Qatar 2022 Cybersecurity Framework

Version 1.0

Document Control

Document Name	Qatar 2022 Cybersecurity Framework
Current Version	1.0
Last Updated	05 August 2018
First Published	05 August 2018
Document Owner	SCDL

Revision Chart

Date	Version	Description of Changes
05 August 2018	1.0	Initial document published

Copyright®

ISBN	Copyright Name	Filing Date	Reg. No.	Reg. Date	Country of Registration - Owner
978 9927 4071 0 9	Security_framework Qatar 2022	Feb 21, 2019	74/2019	March 4, 2019	Qatar – Supreme Committee for Delivery & Legacy

Foreword

As a nation, we are taking progressive strides towards becoming a knowledge-based economy. This major transformation requires that we all recognise the importance of information security as a national priority – in line with the Qatar National Vision 2030 – so we can cultivate an environment where information, ideas and knowledge are protected.

Qatar now proudly stands as the next host of the FIFA World Cup™. We are committed to hosting an event, an event that promises an amazing experience for visitors and guests from all over the world. The 2022 FIFA World Cup™ Qatar™ is our chance to share the beauty of our country with the world. As such, we are planning for our guests to experience Qatar and its advanced capabilities in a new way.

We offer new, inspiring, innovative, resilient, safe and secure digital services to all our guests – services that will make the FIFA World Cup™ in Qatar a truly experience.

With cybersecurity and privacy at the top of the event agenda, the Supreme Committee for Delivery & Legacy issued this cyber framework to set a benchmark for all of us to follow.

This is a national effort that I expect the government, critical sectors and businesses to adopt and implement.

After all, cybersecurity is everyone's responsibility. Through our collective efforts in applying the best practices in this valuable document, we can acquire the cybersecurity capabilities required to succeed as a nation and as a team.

We look forward to delivering amazing.

H.E. the Prime Minister
State of Qatar

Foreword

In this modern, interconnected and digital age, Qatar recognizes the importance of cybersecurity in delivering a secure and safe FIFA World Cup™.

As a result, the Security Committee (under the Supreme Committee for Delivery & Legacy) has progressed with the development of the Qatar 2022 Cybersecurity Framework that you are reading now. It defines the core cyber-competencies and cyber-capabilities needed to safeguard critical national services supporting this prestigious the tournament.

As the 2022 FIFA World Cup™ will be a digitally enabled, smart tournament, we have huge potential to take advantage of innovations such as the internet of things (IoT), machine learning, and artificial intelligence. But doing so does pose additional challenges for security and privacy.

To address those expected challenges, the Security Committee, working closely with our partners, has developed this cybersecurity framework to fulfil our mandate and the promise of a safe and secure event.

We have ensured that the framework is future ready and meets all the global and local standards as well as applicable laws and regulations. Therefore, we are confident of seamless integration with existing cybersecurity programmes.

Developing the cybersecurity framework was a truly collaborative effort. The Security Committee is thankful for and proud of our partners, who contributed to this national effort from all sectors, as well as the multinationals operating in Qatar. The cybersecurity framework truly reflects all our sincere and collective commitment to succeed as one team.

We look forward to delivering amazing.

Colonel Al-Sulaiti

Acknowledgement

This framework was developed with the contributions and comments received from representatives of government and civil society, universities, information security communities, subject matter experts and consultants working in various sectors nationally and internationally. The Supreme Committee for Delivery & Legacy (SC) acknowledges their contributions, especially Hamad International Airport (HIA), whose significant contributions helped in shaping the current framework. Furthermore, SC would like to acknowledge the excellent contribution of EY in developing the cybersecurity framework for the Qatar 2022 world cup as one of the trusted partners in our journey towards hosting a secure and resilient event.


دولة قطر
وزارة الداخلية
دولة قطر
وزارة العدل
Ministry of Justice
دولة قطر
وزارة الطاقة والصناعة
دولة قطر
وزارة المواصلات والاتصالات
مصرف قطر المركزي
Qatar Central Bank
دولة قطر
وزارة الدفاع
دولة قطر
النيابة العامة
الحرس الأميري
AMIRI GUARD
ASHGHAL
قطر تستحق الأفضل
Qatar Deserves The Best
اللجنة العليا
للمشاريع والإرث
Supreme Committee
for Delivery & Legacy
جامعة قطر
QATAR UNIVERSITY
QCRI
معهد قطر لبحوث الحوسبة
Qatar Computing Research Institute
جامعة حمد بن خليفة
HAMAD BIN KHALIFA UNIVERSITY
Carnegie
Mellon
University
Qatar
EY
مطار حمد الدولي
Hamad International Airport
قطر QATAR
قطر للبترول
Qatar Petroleum
QAPCO
شركة قطر للبتروكيماويات
QATAR PETROCHEMICAL COMPANY
وقود
WOQOD
KAHRAMAA
المؤسسة العامة القطرية للكهرباء والماء
كهرماء
Qatar General Electricity & Water Corporation
قطرغاز
QATARGAS
beIN
MEDIA GROUP
QATAR
AIRWAYS
القطرية
ميزة
MEEZA
ooredoo
البنك التجاري
Commercial bank
QDB
بنك قطر للتنمية
QATAR DEVELOPMENT BANK
QIB
المصرف
مصرف الريان
MASRAF AL RAYAN


Microsoft


cisco


RSA

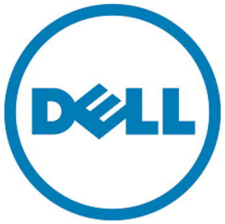

Hewlett Packard
Enterprise


SIEMENS


thinkst
applied research


IBM


BT


DELL


Secureworks


VAUBAN
GROUP


veeAM


FireEye


GE


INFORMATION &
COMMUNICATION
TECHNOLOGY W.L.L

Table of Contents

Figures

Tables

Foreword

The use of Information and communication technologies have become vital to the everyday lifestyle. It is being used to govern societies, public services, support major international sporting events and running everyday businesses. Accordingly, for the functioning of society, nations have also become dependent on these technologies as they are used for running critical information infrastructures. With the ever-changing threats and risks landscape against critical information infrastructures, the availability, integrity and confidentiality must be constantly protected.

In this versatile threat landscape and the various entities involved including supply-chain, the measures and competencies to address cyber threats can be procedural, technological or can involve other disciplines appropriate for mitigating the risks. These competences need to come together to offer appropriate mechanisms capable of strengthening security and resisting threats in harmony.

In 2013, Qatar published its National Cyber Security Strategy which represents a blueprint for moving forward to improve Qatar's national cyber security. This national cyber security strategy has provided fundamental principles and values which helps to derive national cyber security initiatives.

Figure 1: Principles and Values defined in Qatar's National Cyber Security Strategy

The driving principles and values of Qatar's national cybersecurity strategy has acknowledged a fundamental fact that "cybersecurity is a shared responsibility and only collective & collaborative efforts can address its complex challenges".

As the state of Qatar prepares to deliver a successful and secure FIFA World Cup in 2022, a unified system of cybersecurity safeguards is required for the international event where multiple entities are involved to provide world cup services required to execute interdependent activities in a tight eco-system at the national level. This unified system of safeguards is defined in the Cybersecurity Framework.

Structure of the document

This document has been arranged in following sections:

Table 1: Structure of the framework document

Section Name	Description
Introduction	Introduces the world cup ecosystem and capabilities approach to define cybersecurity framework
Cybersecurity Capabilities	Each subsequent chapter defines identified capability 1. Cybersecurity Governance 2. Endpoint Security 3. Application Security 4. Network Security 5. Data Protection 6. Change and Patch Management 7. Security Monitoring and Operations 8. Operations Technology Security Monitoring 9. Incident Handling and Response 10. Recovery and Continuity 11. Data Privacy 12. Identity and Access Management 13. Internet of Things (IoT) 14. Cloud Security
Annexures	i. Security Metrics – these are the measurable parameters to validate effectiveness of activities defined in the capability ii. Glossary iii. References

Each capability chapter has been defined in following structure

Table 2: Structure of each capability chapter

Section heads		Description
What good looks like?	Capability Description	• Description of the capability
	Pre-requisites	• Inputs to this capability • Dependencies, assumptions and requirements which should be completed first & their outputs will be used in this capability
	Service/Process	• Services and/or process(es) defined under this capability • Activities that needs to be conducted in each process phase
	Capability Enterprise Architecture Model	• Simplified version (high level) of capability enterprise architecture to include linkage between people, process and technology
	Information Flow at various level	• What information will flow between Entity to Sector and to National level? • How that information will be passed on to various levels?
How to build one?	Compendium	• It's a collection of various references which provides insights how to build that capability from ground zero • It defines one of many ways for building this capability • Includes some samples based on which the process can be defined such as high-level architecture, major criteria that will be required during the process phases etc. • Skills required by the personnel to carry out capability activities and suggested professional certifications • Required features in the proposed technologies/tools (if applicable) • Mapping to other industry information security standards

How to read this framework

Following is the approach the reader should take to read this framework:

- It is advised that the reader should read first two chapters as requisite which provides a base to work on and fair understanding of this cybersecurity framework requirements and implementation
  - Chapter-1: Introduction – This chapter provides insights how the framework is defined, its foundation and how it can be implemented
  - Chapter-2: Cybersecurity Governance – This chapter is a canopy for all other chapters (i.e. capabilities) defined in the framework
- Choose any of the capability chapter i.e. Chapter 3-15
  - Each capability chapter has been prepared from the perspective to build it from ground zero
  - In case the entity has already implemented the capability, refer to the activities table in each applicable capability to ascertain the cybersecurity requirements from world cup perspective
- Annexure-I: Security Metrics – Once the capability is realized, pick the appropriate security metrics which will help to check the effectiveness of the cybersecurity activities followed

1 Introduction

1. 2022 FIFA World Cup™ Qatar Ecosystem

The 2022 FIFA World Cup Qatar-ecosystem has been defined as:

- Information assets hold valuable information which will be used and processed by world cup services
- Services define the essential activities that will be performed and/or facilities provided to stakeholders
- Entities will contribute in the execution of services for world cup
- These entities are categorized under critical sectors
- SCDL, in cooperation with government will organize the world cup
- The above-mentioned hierarchy is supported with communications, cooperation and collaboration
  - Communication defines information sharing using a medium
  - Cooperation is required among all stakeholders to accomplish individual tasks of an activity
  - Collaboration is required among all stakeholders to accomplish the overall world cup event

1.1 Approach for Defining Cybersecurity Framework

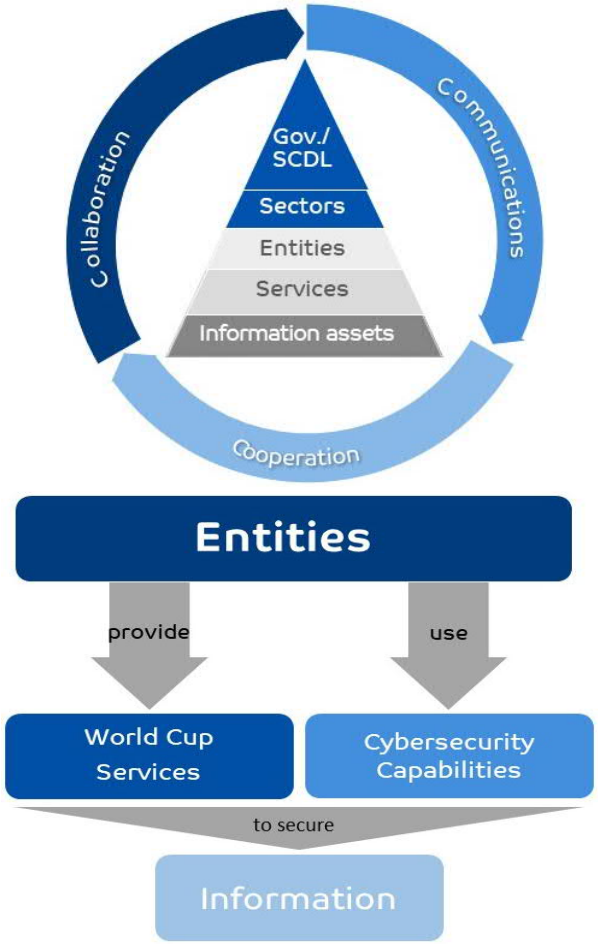
This cybersecurity framework is attempting to take an innovative approach, capability-based approach which is a fit for purpose. It considers security risks identified by the entities as a result of risk management and use it to scope world cup services and associated systems.

The framework is designed to focus on raising and embedding “must have” capabilities and competencies required at all entities that are part of the world cup ecosystem, taking into consideration the current maturity levels of entities in Qatar, the current/future challenges and building on the existing cybersecurity laws, standards and competencies within Qatar.

From the world cup perspective, capabilities have been defined as the cybersecurity competencies expected from entities to secure world cup services and the information used.

In other words, entities will provide world cup services for the event and use cybersecurity capabilities to secure the information.

Figure 2: 2022 FIFA World Cup Qatar

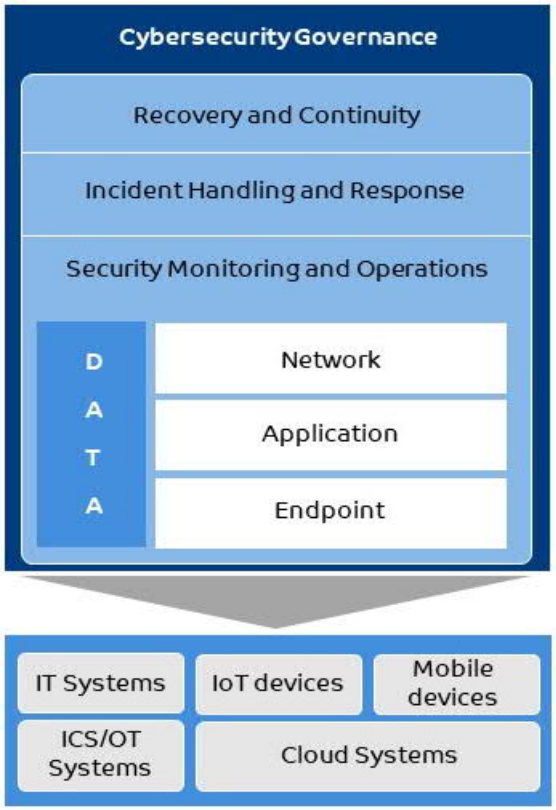


1.2 Approach for Identifying cybersecurity capabilities

To identify which cybersecurity capabilities are required, basic cybersecurity operational activities can be divided into layers that it will be applicable to various systems:

- Data (information) can be:
  - *At rest:* on endpoints like workstations/servers/storage etc.
  - *In use:* while various processing units are processing it
  - *In motion:* when it is being shared among various systems or devices
- From a detection perspective, security monitoring and operations activities are required to identify anomalous activities, i.e.
  - How was the data misused?
  - Who misused it?
  - What was the purpose?
  - When was it misused?
  - How was it accessed?
- Once an anomaly is detected, it must be handled to minimize damage. Hence, Incident Handling & Response and Recovery & Continuity activities are defined to be triggered based on the situation
- All these cybersecurity activities are governed by a governance layer which defines roles and responsibilities of the cybersecurity team
- All above mentioned security layers are applicable to various digital systems like IT systems, ICS/OT systems, IoT devices, mobile devices and cloud systems

Figure 4: Cybersecurity operational activities layers



Based on these cybersecurity operational layers, the following individual capabilities have been identified**:**

Table 3: Cybersecurity capabilities defined

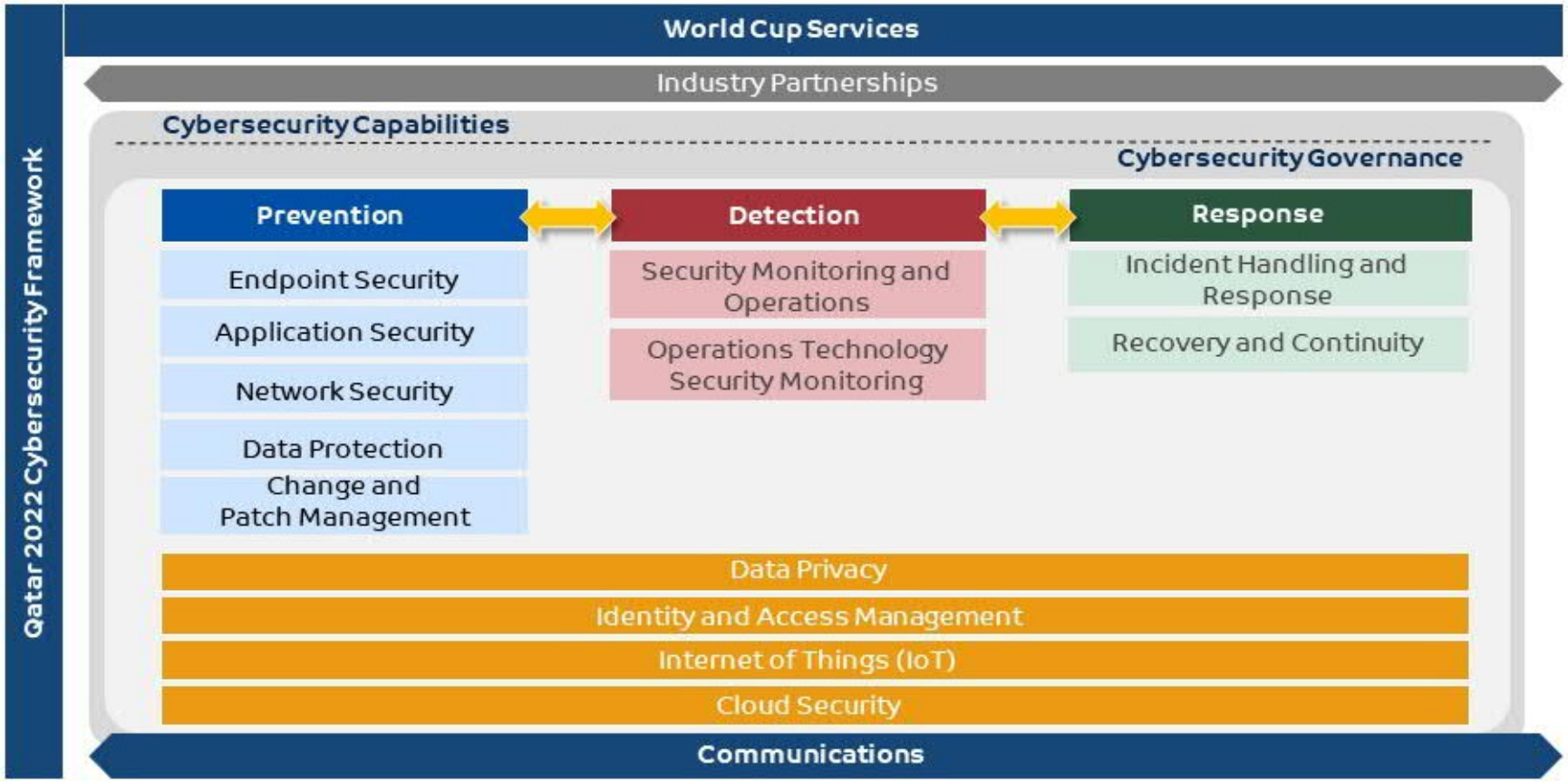
Capability name	Description
Cyber Governance	Used to define standard functions (Risk Assessment, Internal Audit and Training & Awareness) to support the entities with implementation of identified cybersecurity capabilities
Endpoint security	Used to protect all endpoints such as servers, desktops, laptops, wireless devices, mobile devices and other OT/IoT devices connected to the entity's network
Application Security	Used to prevent security weaknesses proactively during the development, acquisition of applications and while using existing applications
Network Security	Used to protect the IT Infrastructure and connected devices internally and externally
Data Protection	Used to detect and prevent confidential information from leaving an entity's boundaries for unauthorized use
Change and Patch Management	Used to ensure required changes affecting assets are deployed in controlled and secure manner
Security Monitoring and Operations	Used to ensure the security posture of mission critical systems (OT/ICS) that help to operate national
Operations Technology Security Monitoring	Used to ensure reliable, safe and secure operations of the Operational Technologies utilized within the national critical infrastructures
Incident Handling and Response	Used to address and manage aftereffects of an attack or anomalous activity
Recovery and Continuity	Used to build appropriate resilience, recovery strategies and tactics
Data Privacy	Used to ensure compliance to legally binding regulation to protect the fundamental rights and freedoms while processing personal data
Identity and Access Management	Used to manage the right individuals to access the right resources at the right times for the right reasons
Internet of Things (IoT)	Used to define secure mechanism of using IoT based devices
Cloud Security	Used to ensure proper hardening of cloud fabric, a model security architecture, as well as the security requirements that should be provided by the cloud service provider (CSP)

1.3 Qatar 2022 cybersecurity framework

These cybersecurity capabilities have been categorized under three distinguished cybersecurity pillars as below:

- Prevention — to reduce attack surface
- Detection — to reduce attackers' presence
- Response — to reduce impact/damage

Figure 5: Qatar 2022 Cybersecurity Framework

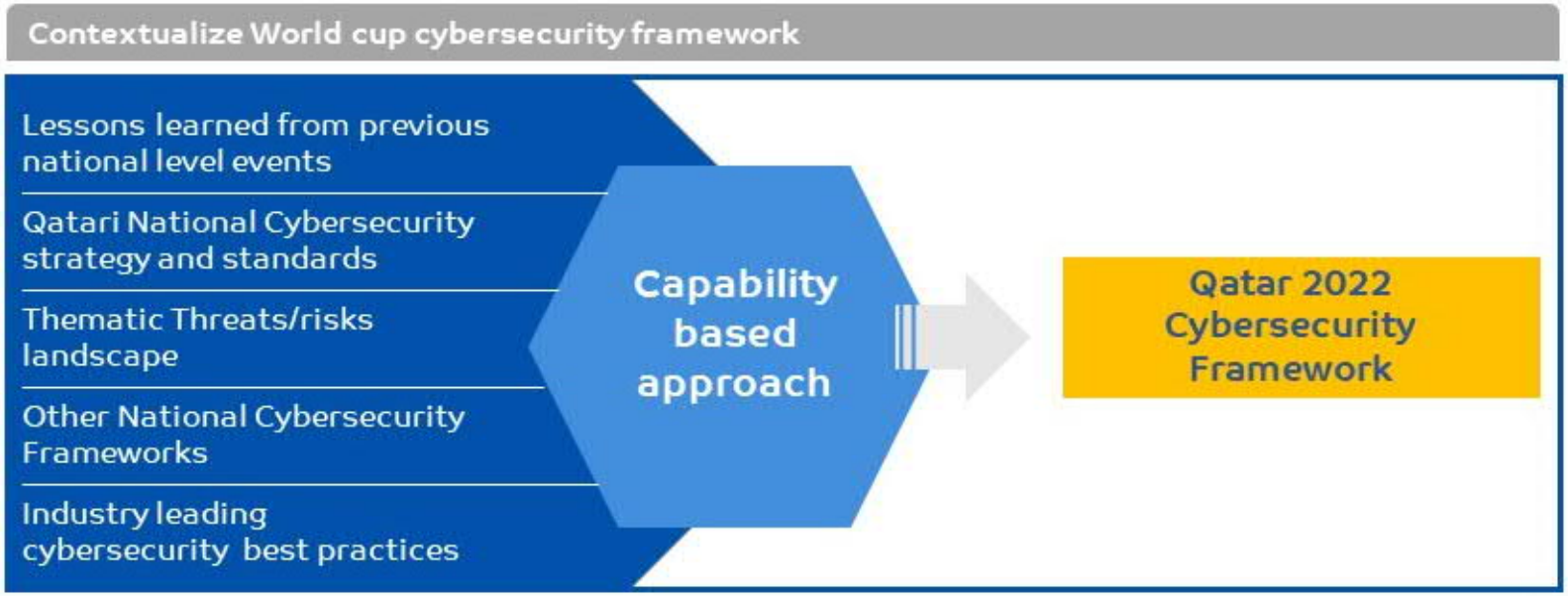


- Cyber security governance is an umbrella to all defined capabilities
- Some of the capabilities which are more of a process or technology centric are horizontally cross-cutting all three pillars
- For all capabilities, a defined industry partnership and sector specific communications are required for properly executing the activities
- From information flow perspective, the information is PROTECTED by prevention capabilities, anomalous activities are DETECTED by detection capabilities and RESPONDED by response capabilities. Therefore;
  - Either 'Security Monitoring and Operations' or 'Operations Technology Security Monitoring' will trigger the process of 'Incident Handling and Response'
  - 'Incident Handling and Response' on requirement basis will trigger the process flow of 'Recover and Continuity'

1.4 FIFA World Cup™ Cybersecurity Framework Contextualization Approach

After defining the core framework, it is paramount that the framework be contextualized within the national laws, regulations and threats & risks more prevalent in the geographical region.

Figure 6: Contextualization approach for world cup cybersecurity framework



For contextualization, the capabilities defined for Qatar 2022 Cybersecurity Framework ***(Qatar 2022 cybersecurity framework)*** assimilated with:

- Lessons learned from previous national level events, which provides insights as to which strategy will be successful at executing national level event activities

- Qatari National Cybersecurity strategy and standards, the cybersecurity principles, values and regulations defined by the Qatari government and are mandated to be followed
- Thematic threats/risks prevalent in geographical region, which provide insights to threats and risks that are currently active within this geographical region
- Other National cybersecurity frameworks, which provide understandings of what strategy worked in other nations while defining national level cybersecurity framework
- Industry leading cybersecurity best practices, that guide tried and tested best practices to thwart cybersecurity incidents

The most important aspect for any entity providing world cup services is to remain in abidance with laws and regulations applicable to them.

With above mentioned contextualization approach, it is believed that as such will address the specific needs and constraints of entities. Concurrently, entities will be following industry leading cybersecurity best practices while implementing and using abreast of new technologies.

Subsequent chapters of this framework document will define each identified capability.

1.5 How to implement the framework

Following figures show the implementation steps for Qatar 2022 Cybersecurity Framework

Figure 7: Implementation steps for Qatar 2022 Cybersecurity Framework– Step1

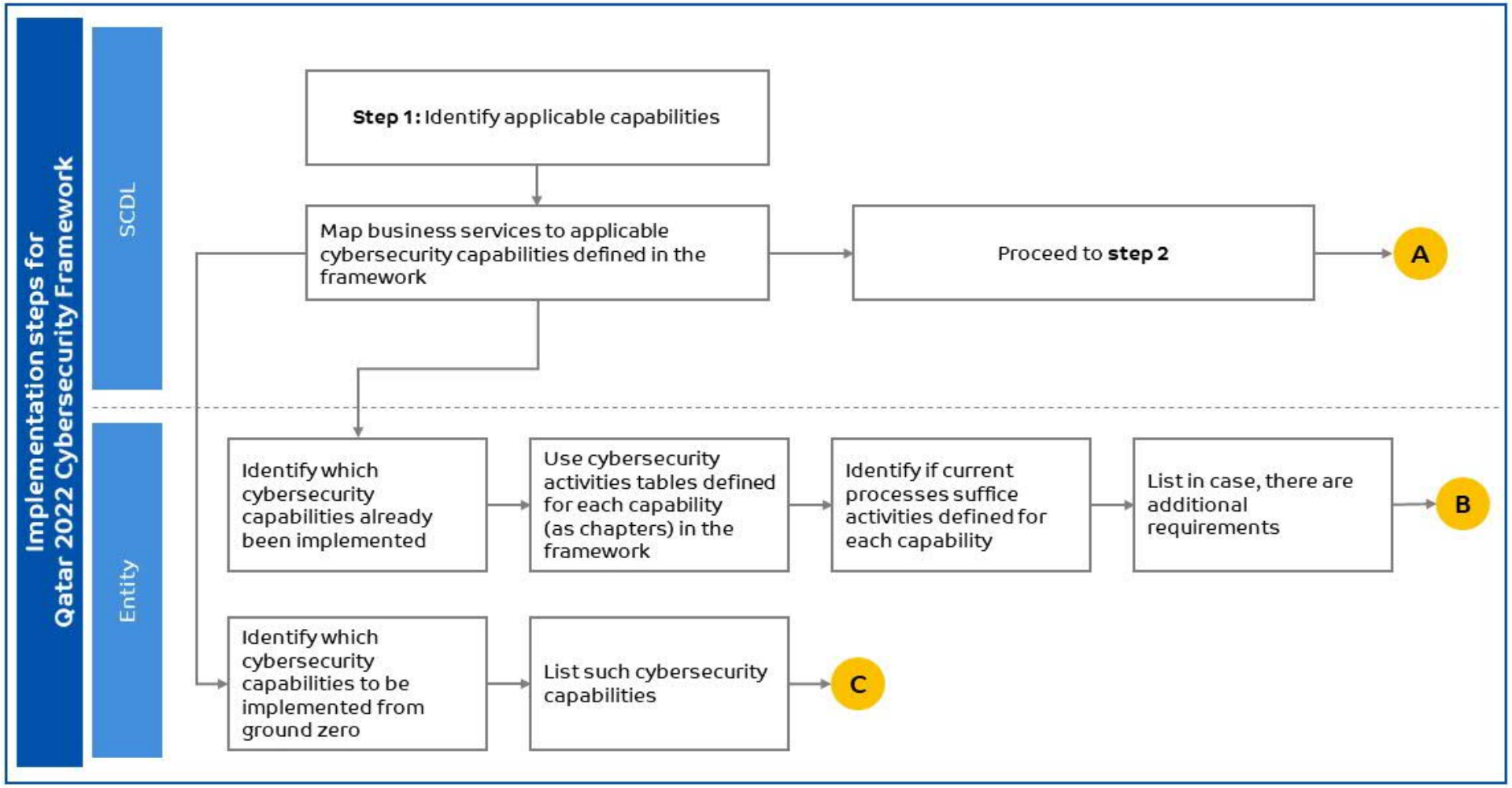
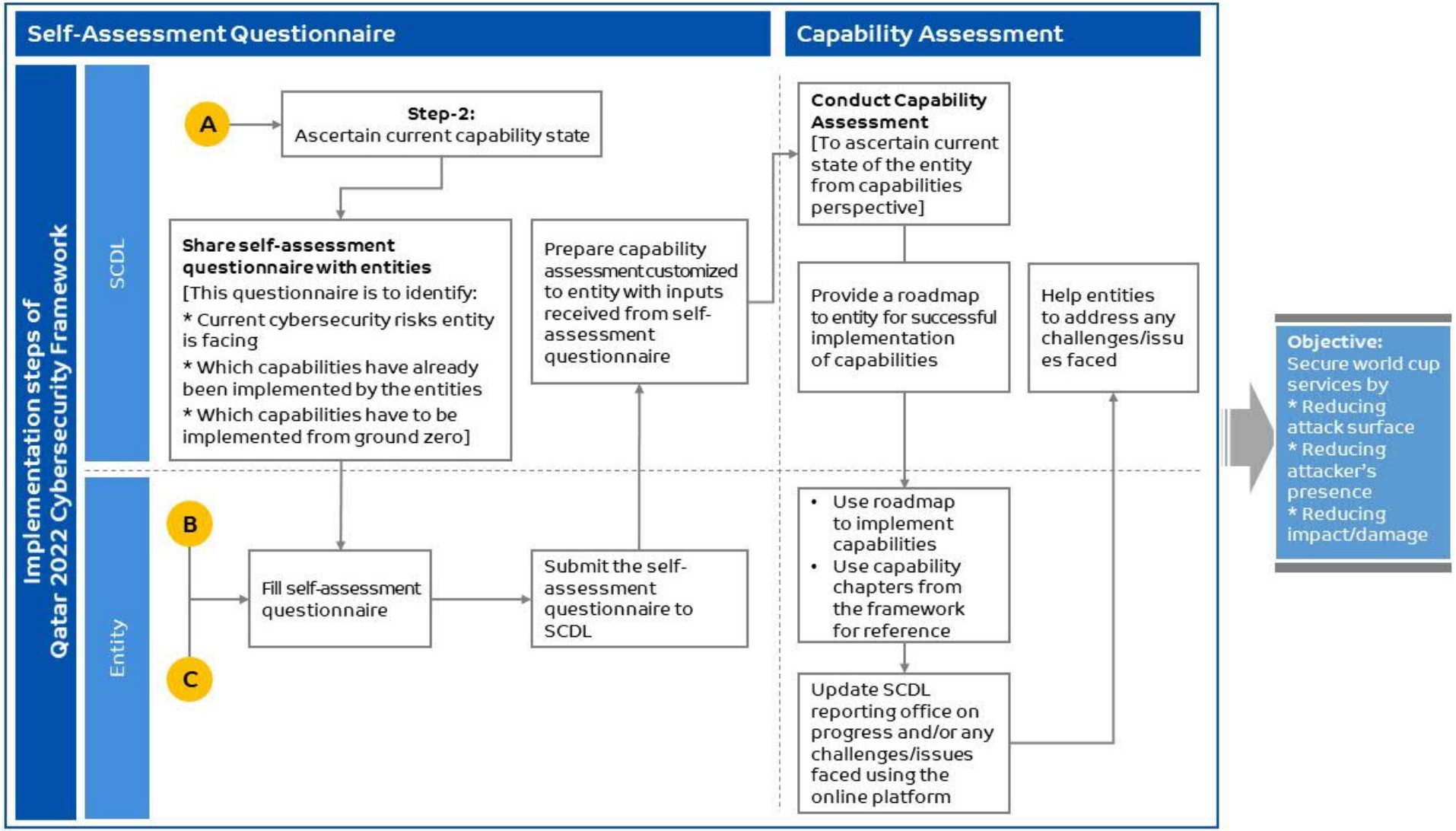


Figure 8: Implementation steps for Qatar 2022 Cybersecurity Framework – Step2



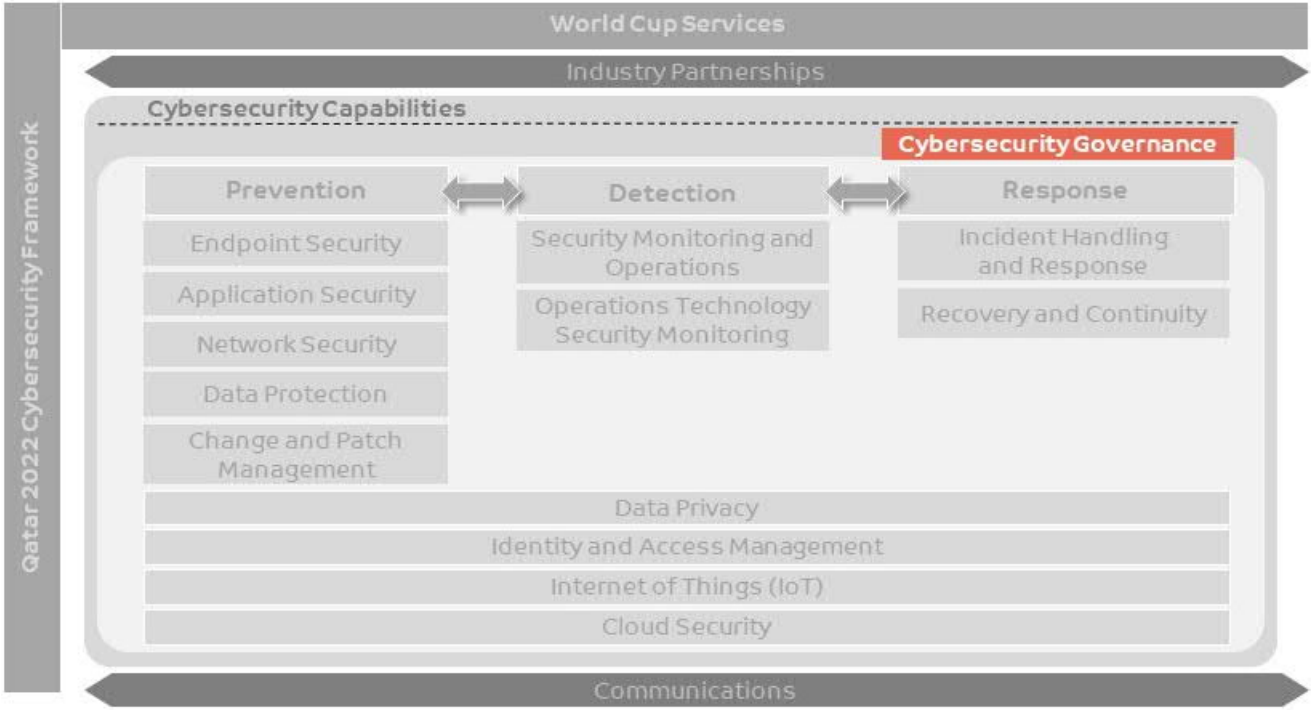
2

Cybersecurity Governance

2. Capability Description — Cybersecurity Governance

This section defines Cybersecurity Governance capability which is an umbrella to all defined capabilities.

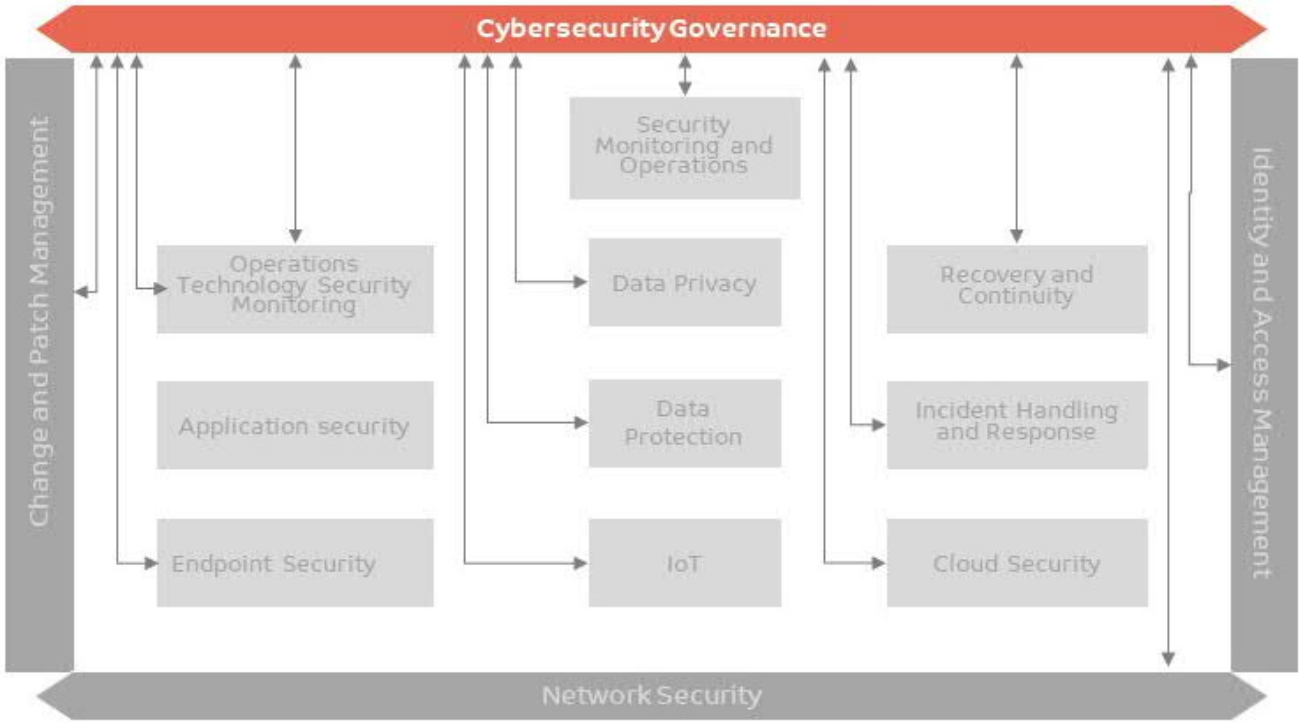
Figure 9: Cybersecurity Governance



Cybersecurity governance refers to the component of enterprise governance that addresses the enterprise's dependence on cyberspace from strategy perspective. Its structure and practices enable consistent and reasonable decision making which in turn regulates the implementation and operation of cybersecurity capabilities defined within the framework.

Following figure depicts the linking of the cybersecurity governance with other cybersecurity capabilities defined in the framework.

Figure 10: Cybersecurity Governance linkage with other capabilities



2.1 Cybersecurity Governance Functions Supporting Cybersecurity Capabilities

There are three cybersecurity governance functions which support the entities with implementation of identified cybersecurity capabilities, namely:

- Cybersecurity Risk Management
- Cybersecurity Internal Audit
- Cybersecurity Training and Awareness

2.2 Cybersecurity Risk Management

The objective of the cybersecurity risk management is to ensure that cybersecurity risks are adequately identified and managed by the entity for each cybersecurity capability (aligned with the bigger enterprise risk) to enable better business resilience and compliance against cybersecurity risks. The risk management function supports each capability to focus on enhancing entity's management and personnel understanding of various cybersecurity risk exposures and their implications to provide a rigorous decision-making process and to make sure that the information systems are adequately protected during the world cup.

2.2.1Prerequisites

Following are the prerequisites which are required to accomplish the Cybersecurity Risk Management:

- National/Sector level cybersecurity Risk Assessment compliance requirements are identified related to World Cup Cybersecurity Capabilities

2.2.2Cybersecurity Risk Assessment Service

The Cybersecurity Risk Management process describes the overall approach to security risk management against World Cup's cybersecurity capabilities. This will help the entity to achieve its strategic cybersecurity objectives by managing and mitigating the various security risks for each capability, which have the potential to affect the achievement of world cup cybersecurity objectives.

From a world cup perspective, following table describes the respective activities that need to be conducted to establish Cybersecurity Risk Management. The cybersecurity risk assessment process shall be followed by each prioritized entity and shall be linked to the entity's own Risk Management cycle.

Table 4: Cybersecurity Risk Management Service

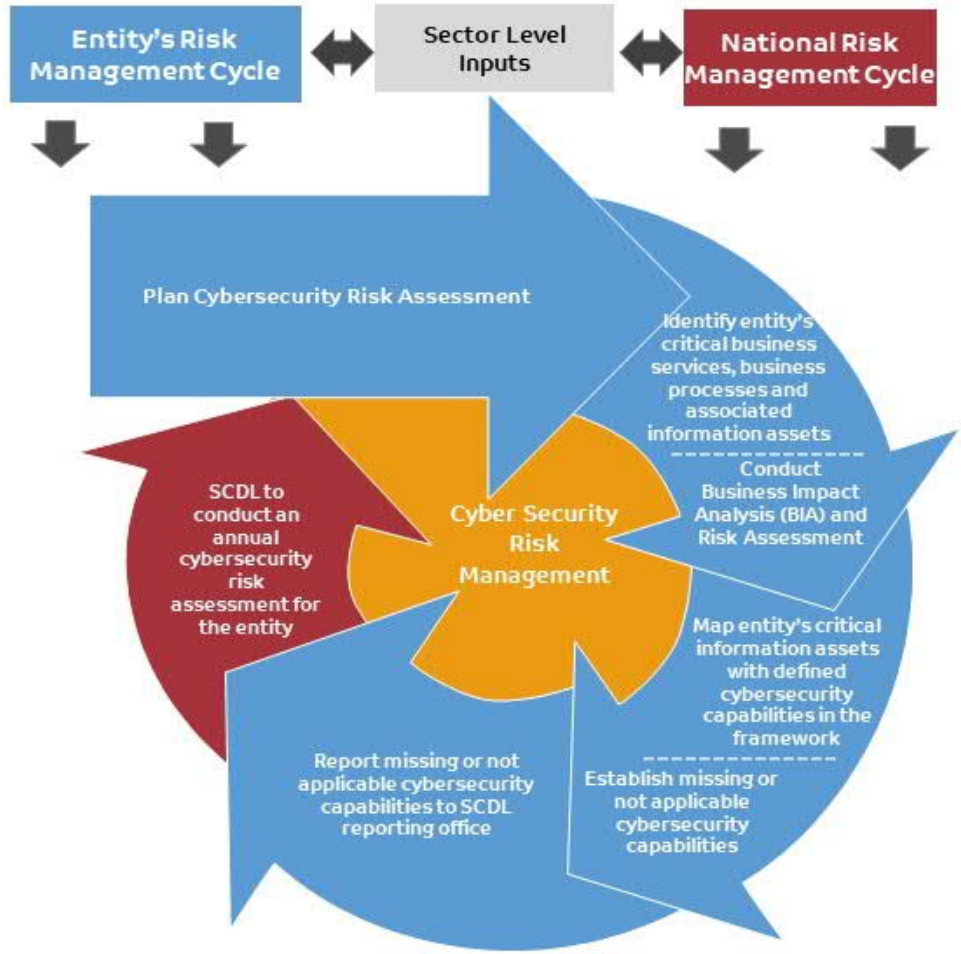
Service Name: Cybersecurity Risk Management	
Description	The Risk Management service describes the overall process to cyber security risk management against World Cup cybersecurity capabilities
Process phases	**Activities/Controls**
Plan Cybersecurity Risk Assessment	• The scope of risk management determined within the context of the entity's business objectives as part of their own Risk Management Cycle • The entity's cybersecurity Risk Management to be aligned to the National Risk Management Cycle for World Cup Cybersecurity Capabilities
Identify entity's critical business services, processes and associated information assets	• Identify entity's critical business services, processes and associated information assets
Conduct Business Impact Analysis (BIA) and Risk Assessment	• Identify magnitude of losses/impacts derived from disruptions and the associated risks that have a potential to impact operations

Service Name: Cybersecurity Risk Management	
Map entity's critical information assets with defined cybersecurity capabilities in the framework	• Map entity's critical information assets with defined cybersecurity capabilities in the framework
Establish missing or not applicable cybersecurity capabilities	• Establish the cybersecurity capabilities which are missing or not applicable to the entity
Report to SCDL reporting Office	• Report the missing or not applicable cybersecurity capabilities to the SCDL reporting Office • SCDL reporting Office will review and confirm the cybersecurity capabilities to be implemented by the entity
Annual Cybersecurity Risk Assessment by SCDL	• SCDL to conduct an annual risk assessment exercise for the entities to assess the current status of cybersecurity capabilities implementation in line with implementation suggestion by SCDL reporting Office

2.2.3Cybersecurity Risk Management Model

Following figure illustrates the risk management model established for Cybersecurity Risk Assessment at Entity level:

Figure 11: Cyber Security Risk Management Model for World Cup Cybersecurity Capabilities



- **Plan Cybersecurity Risk Assessment** — defines the scope for the risk management process for identification of world cup cybersecurity capabilities
- **Identify entity's critical business services and processes and associated information assets —** covers identification of entity's critical business services, processes and associated information assets
- **Conduct Business Impact Analysis (BIA) and Risk Assessment** – to identify magnitude of losses/impacts derived from disruptions and all the risks that have potential to impact the operations
- **Map entity's critical information assets with defined cybersecurity capabilities in the framework —** covers mapping of the entity's critical information assets with defined cybersecurity capabilities in the framework
- **Establish missing or not applicable cybersecurity capabilities —** covers identification of the missing or not applicable cybersecurity capabilities against cybersecurity capabilities defined in the framework
- **Report to SCDL Reporting Office —** covers reporting of missing or not applicable cybersecurity capabilities to SCDL reporting office. SCDL reporting office will review the entity's reported missing or not applicable cybersecurity capabilities and suggest the cybersecurity capabilities to be implemented by the entity
- **Annual Cybersecurity Risk Assessment by SCDL —** covers an annual external cybersecurity risk assessment by SCDL against the world cup cybersecurity capabilities

2.2.4Cybersecurity Risk Management Service Expected at Entity/Sector/National Levels

This cybersecurity risk management is applicable at individual capacity at all levels (i.e. Entity/Sector/National). Following table describes the processes expected at each level of world cup ecosystem:

Table 5: Risk Management Services expected at each level

Entity	Sector	National
• Identify the scope of cybersecurity risk management • Conduct cyber security risk assessment to identify missing or not applicable cybersecurity capabilities • Report risk results - missing or not applicable capabilities to SCDL reporting Office • Conduct an annual cybersecurity risk assessment for World Cup cybersecurity capabilities as part of the Entity's Risk Management Cycle	• Provide support to identify scope of risk management for entities in the sector • Identify / coordinate common critical services for security capabilities relevant to the sector • Collate results of cybersecurity risk assessment from all entities in the sector and communicate those to National Level contacts (SCDL reporting Office)	• Provide support to identify the scope of security risk management for all sectors • Review entity's cybersecurity risk management results missing capabilities • Suggest entities on capabilities to be implemented/enhanced • SCDL to conduct annual risk management as part of the National Risk Management Cycle of the identified sectors and entities against requirements of the National Cybersecurity Risk Management

2.2.5Skills Required for Cybersecurity Risk Assessment Supporting Cybersecurity Capabilities

Following are the skills expected from personnel executing Cybersecurity Risk Assessment activities:

- Experience performing risk and compliance assessments and in-depth knowledge of industry standards and regulatory requirements (e.g., NIAF, ISA, PCI-DSS, HIPAA, HITRUST, HITECH, FISMA, NIST, ISO 3100, ISO 2700X, COBIT, FFIEC, NERC CIP)
- Experience assessing and defining system specifications preferably in relation to compliance, data protection and data privacy regulations such as GDPR
- Understanding of entity's services, processes and controls environments
- Experience with risk assessment techniques and with GRC/ERM tools (e.g. RSA Archer, MetricStream, SAP GRC, Logic manager, etc.)
- Strong background in information security, IT audit or security risk management
- Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity
- Working knowledge of risk and security frameworks, standards, and best practices (e.g. ISO 31000, COBIT, NIST, ISO 27001/2 etc.)
- Suggested professional certifications which can help personnel to attain skills for risk assessment activities
    - Certified Information Systems Auditor (CISA)
    - Certified Information Security Manager (CISM)
    - Certified in Risk and Information Systems Control (CRISC)

2.3 Cybersecurity Internal Audit

The objective of the internal audit function is to assess and report the entities' level of achievement towards the World Cup Cybersecurity framework capabilities and ensure continuous monitoring of the compliance to each cybersecurity capability.

2.3.1Prerequisites

Following are the pre-requisites, which are required to be accomplished for Cybersecurity Internal Audit:

- National cybersecurity Internal Audit compliance requirements are identified related to World Cup Cybersecurity Capabilities
- The internal audit function shall be independent, apply integrity & duty of care and professional ethics

2.3.2Cybersecurity Internal Audit Service

The Cybersecurity Internal Audit process describes the overall approach to self-assessment for each cybersecurity capability. Cybersecurity internal audit process defined here shall be followed for each capability.

Following table describes respective activities that needs to be conducted for Cybersecurity Internal Audit. The cybersecurity internal audit self-assessment process shall be followed by each entity which shall be linked to the entity's own Internal Audit cycle.

Table 6: Cybersecurity Internal Audit Service

Service Name: Cybersecurity Internal Audit	
Description	The Cybersecurity Internal Audit service describes the overall process of entity's self-assessment to assess compliance against World Cup cybersecurity capabilities
Process phases	**Activities/Controls**
Plan	• Plan the internal audit of cybersecurity capabilities • Identify the scope of the cybersecurity capabilities self-assessment to be covered in the assessment/audit exercise that are applicable to the entity • Determine the skillset/competency required for the self-assessment • Confirm the reporting timeline of the overall self-assessment of cybersecurity capabilities

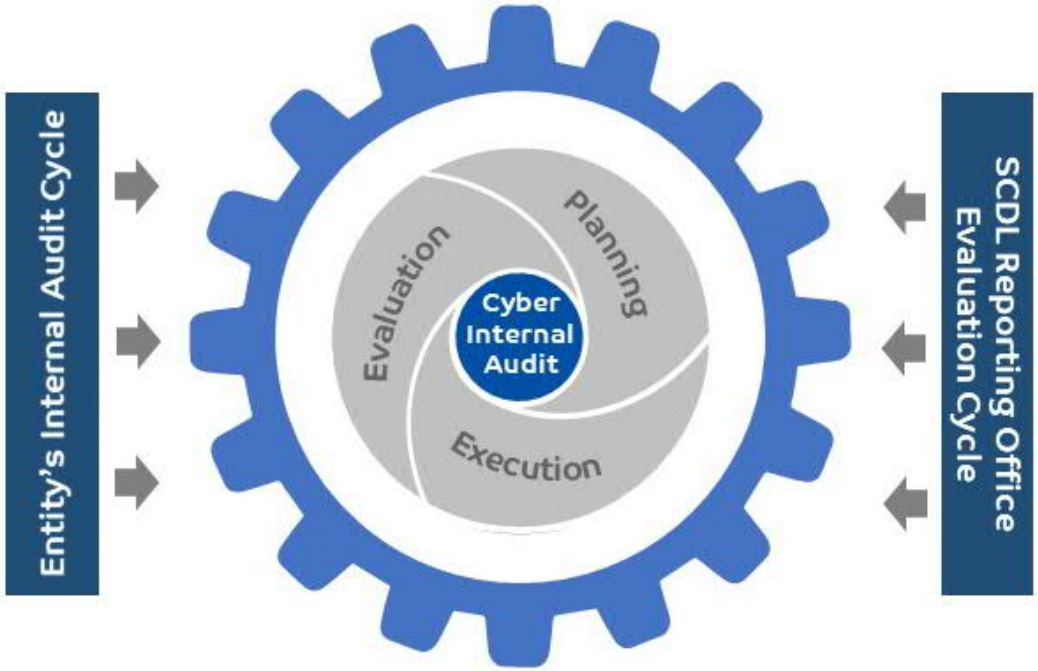
Service Name: Cybersecurity Internal Audit	
	• Select independent parties within the organization to assist in conducting the self-assessment/audit exercise. (E.g. Internal audit senior/manager, Risk officer, conducted by a third-party professional etc.) • Sample evidence: Annual audit plan • Audit plan and scope • Auditor qualifications
Identify	• Determine the required capability section in the pre-defined self-assessment questionnaire/or audit scope • Statement of applicability (SOA)
Execute	• Review the design of entity's cybersecurity capabilities and controls by assessing whether the design of controls is effective to achieve management assertions or policy claims • Determine the validation of the assessment/audit results are reliant on • Ensure that the self-assessment evidences are complete and documented • Audit/Work Programs • Testing sheets • Audit samples
Formalize Findings	• Formalize the self-assessment report for in-scope cybersecurity capabilities • Evaluate the results of the self-assessment exercise in line with requirements of the relevant capabilities • Draft internal audit report • Auditee action plans for remediation planning
Report	• Report the final self-assessment/internal audit report on world cup cybersecurity capabilities to SCDL reporting office (SC-CSU established office) • Report corrective and preventive actions to entity's management
Evaluate and Improve	• SCDL reporting team to conduct an annual external audit of the entity's implemented cybersecurity capabilities to check compliance against world cup cybersecurity requirements • Include lessons learned from previous audits/assessments conducted

2.3.3Cybersecurity Internal Audit Model

Following figure illustrates the internal audit self-assessment process established for Cybersecurity Internal Audit at Entity level:

Figure 12: Cyber Security Internal Audit Model for World Cup Cybersecurity Capabilities

- **Planning —** the Internal Audit process for self-assessment of World Cup Cybersecurity Capabilities. Planning will also cover identification pre-defined self-assessment questionnaires as communicated by SCDL reporting office team for each World Cup cybersecurity capability
- **Execution —** conduct the self-assessment of entity's cybersecurity capabilities and documenting the results of the assessment
- **Evaluation —** covers formalizing the observations of the self-assessment and agreeing on management actions and related timelines. Further, the cybersecurity capabilities self-assessment results will be reported by the entity to the SCDL reporting office for their evaluation



2.3.4 Cybersecurity Internal Audit Service Expected at Entity/Sector/National Levels

This cybersecurity Internal Audit Self-assessment is applicable in individual capacity at all levels (i.e. Entity/Sector/National). Following table describes processes expected at each level of world cup ecosystem:

Table 7: Internal Audit Services expected at each level

Entity	Sector	National
• Identify the scope of cybersecurity capabilities Self-Assessment • Conduct self-assessment based on pre-defined cybersecurity capabilities self-assessment questionnaire • Communicate cyber capabilities self-assessment results to established sector and national level contacts (SCDL reporting office)	• Provide support to identify scope of cybersecurity capabilities self-assessment for entities in the sector • Identify/ coordinate common security capabilities relevant to the sector • Collate results of cybersecurity capabilities self-assessment from all entities in the sector and communicate these to National Level contacts (SCDL reporting office)	• Provide support to identify the scope of security capabilities self-assessment for all sectors • Evaluate entity's cybersecurity self-assessment results • Suggest entities on cybersecurity capabilities to be enhanced. • SCDL reporting team to conduct periodic external audit as part of the identified sectors and entities against requirements of

Entity	Sector	National
• Conduct an annual cybersecurity Internal Audit Self-Assessment as part of the Entity's Internal Audit Cycle		the National Cybersecurity Governance Internal Audit

2.3.5Skills Required for Cybersecurity Internal Audit Supporting Cybersecurity Capabilities

Following are the skills expected from personnel executing Cybersecurity Internal Audit activities:

- Hands-on experience with cybersecurity internal audits and self-assessments
- Understanding of entity's services, processes and controls environments
- Experience performing Cyber Security Audits and compliance assessments and in-depth knowledge of industry standards and regulatory requirements (e.g., HIPAA, HITRUST, HITECH, FISMA, NIST, ISO 2700X, COBIT, FFIEC, NERC CIP, etc.)
- Experience assessing and defining system specifications preferably in relation to compliance, data protection and data privacy regulations such as GDPR
- Strong knowledge of the management of both physical and logical information security systems
- Working knowledge of risk and security frameworks, standards, and best practices (e.g. ISO 31000, COBIT, NIST, ISO 27001/2 etc.)
- Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Internal Auditor (CIA), and other applicable certifications preferred
- Demonstrate functional audit knowledge and ability to apply auditing protocols
- Provide leadership, direction and guidance in assessing and evaluating information security risks and monitor compliance with security standards and appropriate policies

2.4 Cybersecurity Training and Awareness

The objective of the cybersecurity training and awareness is to:

- Improve the entities learning and understanding of cybersecurity capabilities, latest cyber risks, current trends and threat landscape
- Understand the importance of adequate planning and implementation of identified cybersecurity capabilities
- Understand a variety of techniques to identify, assess, manage & monitor World Cup's cybersecurity capabilities

2.4.1Pre-requisites

Following are the pre-requisites, which are required to be accomplished for Cybersecurity Training and Awareness:

- National level and sector level cybersecurity training and awareness requirements are identified related to World Cup Cybersecurity Capabilities

2.4.2Cybersecurity Training and Awareness Service

The Cybersecurity Training and Awareness process describes the overall approach to cybersecurity training and awareness program to assist the entity by training the identified personnel with a solid understanding of requirements for World Cup cybersecurity capabilities and creating awareness for other entity users on latest cybersecurity risks, current trends and threat landscape.

From world cup perspective, following table describes respective activities that needs to be conducted for Cybersecurity Training and Awareness. The cybersecurity training and awareness program shall be followed by each prioritized entity which shall be linked to the entity's own Training and Awareness cycle.

Table 8: Cybersecurity Training and Awareness Service

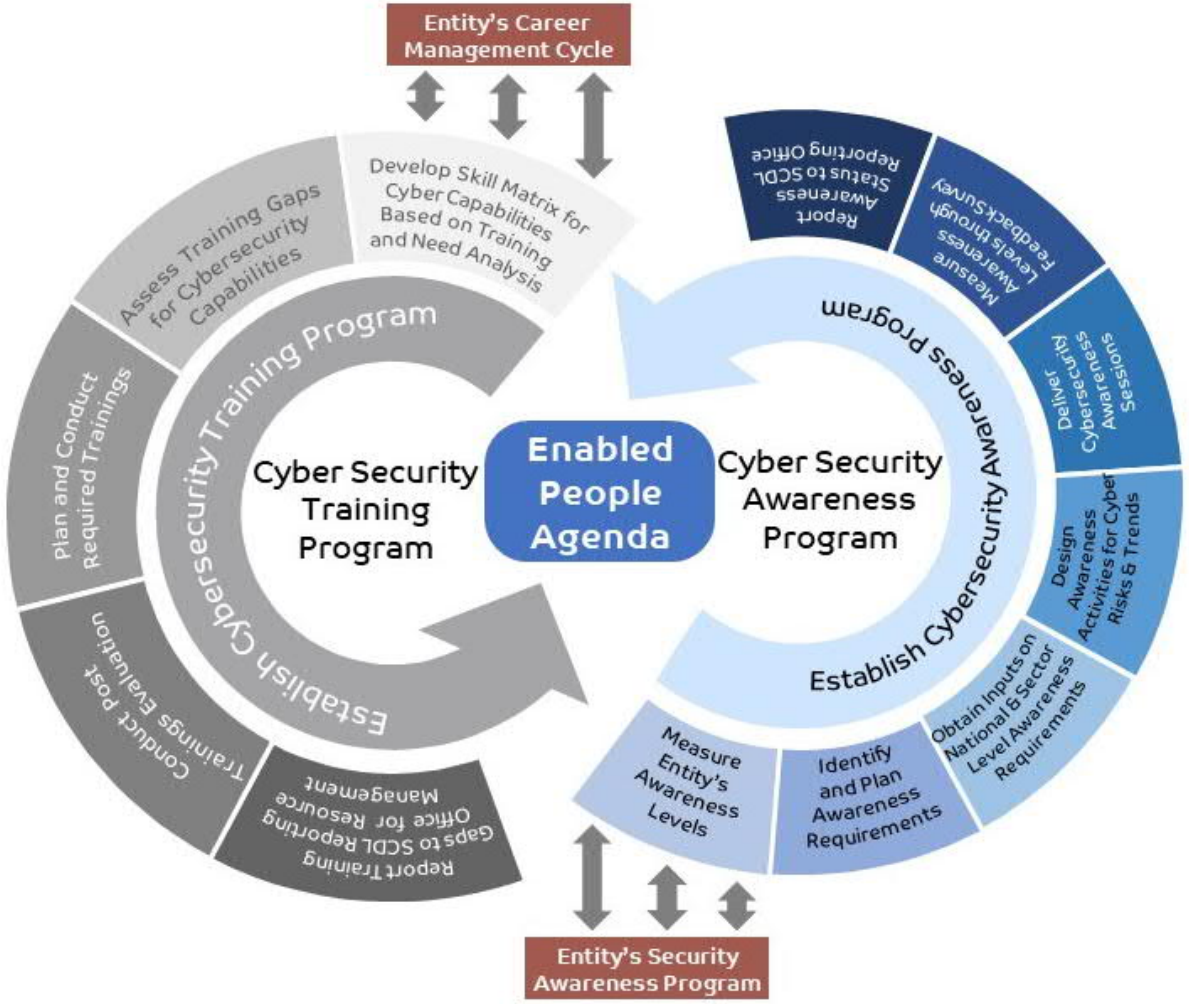
Service Name: Cybersecurity Training and Awareness		
Description	The cybersecurity training and awareness service describes the overall process to cyber security training and awareness against World Cup cybersecurity capabilities and latest cyber risks/trends.	
Process	**Process phases**	**Activities/Controls**
Cybersecurity Training Activities	Training Need Analysis	• Develop skill matrix for cybersecurity capabilities based on training and need analysis
	Assess Training Gaps	• Assess training gaps for cybersecurity capabilities
	Execute Trainings	• Plan and conduct required trainings for cybersecurity capabilities as part of entity's career management cycle
	Post Training Evaluation	• Conduct post trainings evaluation
	Report Gaps to SCDL reporting team	• Report training gaps to SCDL reporting office for assistance with arranging the right training with skilled trainer
Cybersecurity Awareness Activities	Measure Awareness Level	• Measure current cybersecurity awareness levels in the entity
	Plan Awareness Requirements	• Identify and plan cybersecurity awareness requirements
	National/Sector Requirements	• Obtain inputs on national & sector level awareness requirements
	Design Awareness Activities	• Design awareness activities based on latest cyber risks & trends
	Deliver Awareness	• Deliver cybersecurity awareness sessions for entity users
	Measure Awareness	• Measure cybersecurity awareness levels through feedback surveys

Service Name: Cybersecurity Training and Awareness		
	Report Status to SCDL reporting team	• Entity to report cybersecurity awareness status to SCDL reporting office for their evaluation

2.4.3Cybersecurity Training and Awareness Model

Following figure illustrates the process established for cybersecurity training and awareness at entity level:

Figure 13: Cybersecurity training and awareness model for world cup cybersecurity capabilities



2.4.4Cybersecurity Training and Awareness Service Expected at Entity/Sector/National Levels

This cybersecurity training and awareness management is applicable in individual capacity at all levels (i.e. Entity/Sector/National). Following table describes processes expected at each level of world cup ecosystem:

Table 9: Cybersecurity Training and Awareness Services expected at each level

Entity	Sector	National
• Identify and plan the cybersecurity training and awareness requirements by assessing training and awareness gaps • Conduct required trainings cybersecurity capabilities and cybersecurity awareness across the entity • Evaluate trainings and awareness through feedbacks surveys • Communicate training and awareness gaps to established sector and national level contacts (SCDL reporting office) • Conduct annual cybersecurity training and awareness for World Cup cybersecurity capabilities and cyber risks/trends as part of the Entity's training and awareness program	• Provide support to entities in the sector for cybersecurity training and awareness program • Identify/ coordinate common trainings and awareness programs for security capabilities relevant to the sector • Collate results of cybersecurity training gaps and status of cybersecurity awareness program from all entities in the sector and communicate these to National Level contacts (SCDL reporting office)	• Provide support to all sectors for the cybersecurity training and awareness program • Evaluate entity's cybersecurity training and awareness results • Support sectors and entities with resource identification and management where training gaps are because of non-availability of a personnel. • Provide sector and national levels cybersecurity training and awareness requirements.

2.4.5Skills Required for Cybersecurity Training and Awareness Supporting Cybersecurity Capabilities

Following are the skills expected from personnel executing Cybersecurity Training and Awareness activities:

- Experience performing training and awareness of industry standards and regulatory requirements (e.g., HIPAA, HITRUST, HITECH, FISMA, NIST, ISO 2700X, COBIT, FFIEC, NERC CIP, etc.)
- Hands-on experience with cybersecurity training and awareness programs
- Understanding of entity's services, processes and controls environments
- Experience with security training and awareness techniques
- Strong background in information security, IT audit or security risk management
- Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.
- Working knowledge of risk and security frameworks, standards, and best practices (e.g. ISO 31000, COBIT, NIST, ISO 27001/2 etc.)

2.5 Proposed Cyber Organization Structure

Organization structure provides the approaches in which an organization operates and performs. It defines allocation of tasks and responsibilities for various roles which are directed towards the achievement of organizational goals.

This framework supports current organization structure and propose some changes for cybersecurity function. However, it is utmost important that organizations/entities should define their organizational structure as per their organizational goals.

Following table defines broad sub functions identified that are allied to the Qatar 2022 Cybersecurity Framework and proposed roles.

Table 10: Cybersecurity sub functions and their salient activities – Part I

Cybersecurity Function		
Sub function	Salient activities	Roles
Overall cybersecurity portfolio management External relationship	• Manage relationships with third parties (vendors, suppliers, contractors, partners, and critical infrastructure owners/operators) • Manage and liaise with other board members and C-Level executives within the organization • Manage relationships with external stakeholders (for example, National CERT, Regulators, Law and Enforcement, National/Sector cybersecurity forums) • Liaise with Head of Legal for legal matters such as Data Privacy and other legal/regulatory requirements	Chief Information Security Officer/Head of Cybersecurity

Cybersecurity Function		
Personnel management	• Manage the employment lifecycle and performance of personnel in accordance with security requirements (background checks, vetting, transfers, risk designations, succession planning, disciplinary action, and termination) • Manage knowledge, skills, capabilities, and availability of the cybersecurity team	Director – Cybersecurity
Cybersecurity Governance	• Define, implement, and enforce information security policies • Establish an information security risk management strategy, process, and program • Govern/oversee the cybersecurity program and plan • Ensure that controls are adequate to meet legal, regulatory, policy, standards, and security requirements • Conduct internal audits • Implement an enterprise-wide role-based cybersecurity awareness and training program	Manager – Cybersecurity – Governance & Compliance

Table 11: Cybersecurity sub functions and their salient activities – Part II

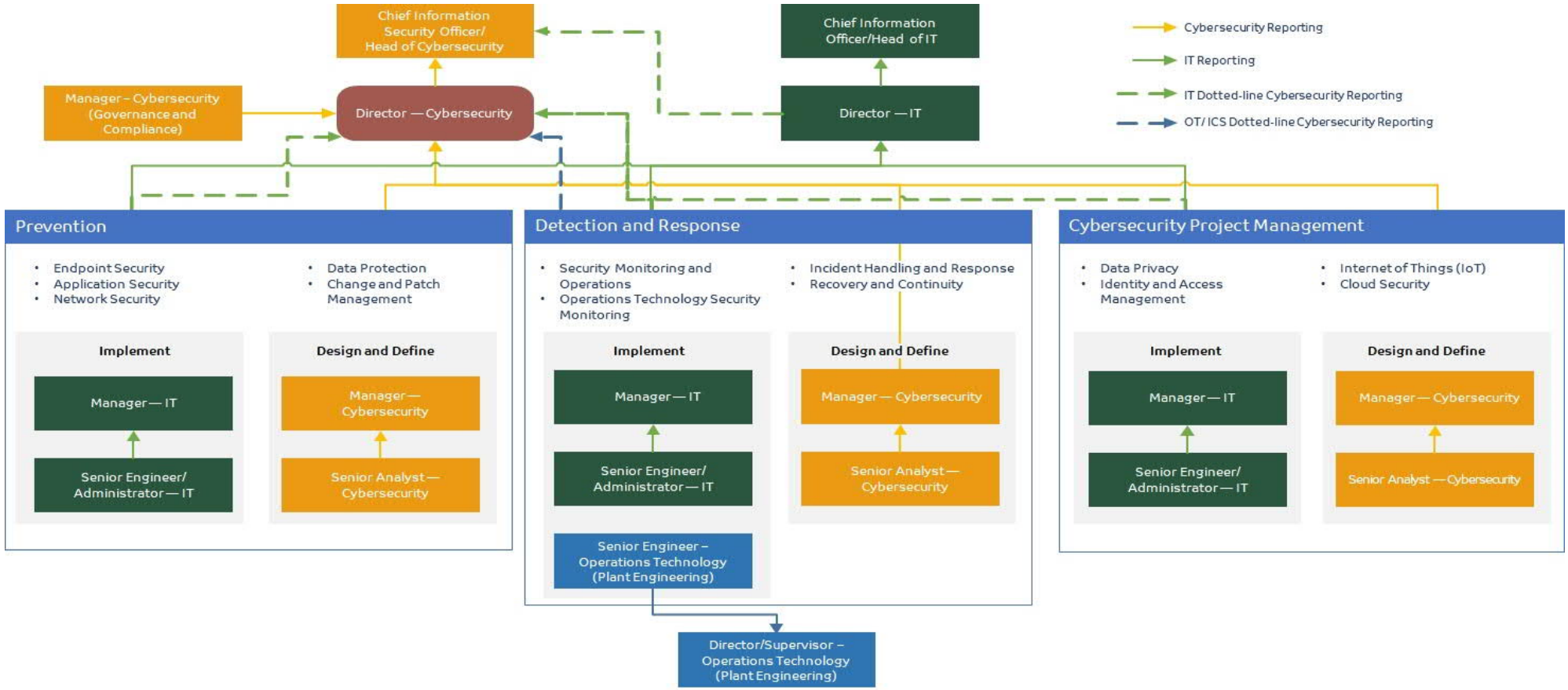
Cybersecurity Function		
Sub function	Salient activities	Roles
Prevention	• Endpoint Security • Application Security • Network Security • Data Protection • Change and Patch Management	Responsible for the implementation of cybersecurity technologies • Manager – IT • Senior Engineer/Administrator
		Responsible for designing and defining cybersecurity technologies • Manager – Cybersecurity • Senior Analyst – Cybersecurity
Detection And	• Security Monitoring and Operations • Operations Technology security monitoring	Responsible for the implementation of cybersecurity technologies • Manager – IT • Senior Engineer/Administrator – IT • Senior Engineer-Operations Technology (Plant Engineering)

Cybersecurity Function		
Response	• Incident Handling and Response • Recovery and Continuity	Responsible for designing and defining cybersecurity technologies • Manager – Cybersecurity • Senior Analyst – Cybersecurity
Cybersecurity Project Management	• Data Privacy (From internal process and technology perspective) • Identity and Access Management • Internet of Things (IoT) • Cloud Security	Responsible for the implementation of cybersecurity technologies • Manager – IT • Senior Engineer/Administrator
		Responsible for designing and defining cybersecurity technologies • Manager – Cybersecurity • Senior Analyst – Cybersecurity

* Refer individual capability chapters for detail on activities defined under each sub function PREVENTION, DETECTION and RESPONSE

Following figure depicts proposed organizational structure for cybersecurity function and its relation to Information Technology (IT) and Operations Technology (OT /ICS)

Figure 14: Proposed Cybersecurity – Organizational Structure



- Dotted-line reporting means that the role has some level of accountability related to cybersecurity but is not a direct report
- Skillsets required to perform activities for each identified capability have been defined in respective chapters under compendium section
- Titles are just indicative and are not compulsory to be followed Organizations/entities should follow the titles as defined in their organizational structure

- Hierarchy levels defined in the organization structure may vary according to the different sectors and the size of the respective organization considering any regulatory or legal requirements. For example: GDPR, PCI-DSS, SOX, HIPPA, Qatar Data privacy law, NIA etc. requires specific roles to be defined
- Number of team members should be defined by size of the organization, world cup services provided by the organization and in-scope applicable capabilities. Ideally it can also be defined by work-load analysis exercise

3

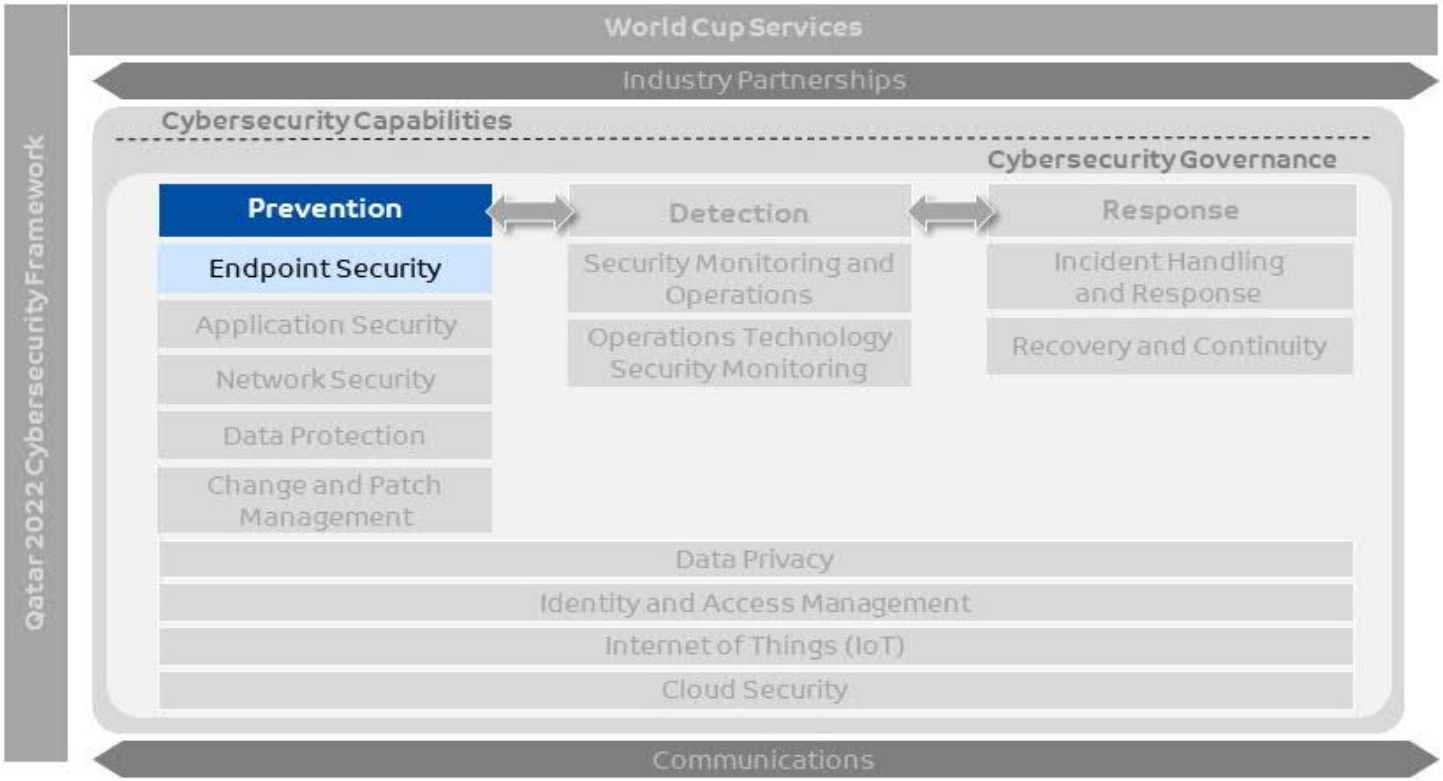
Endpoint Security

3. Capability Description – Endpoint Security

A capability for protecting all endpoints such as servers, desktops, laptops, wireless devices, mobile devices and other OT/IoT devices connected to the network from cyber threats. This capability will implement the processes, controls and technologies required to build a sustainable endpoint protection program aligned to the business and focused on protecting all endpoints that matters most with respect to services provided for the world cup.

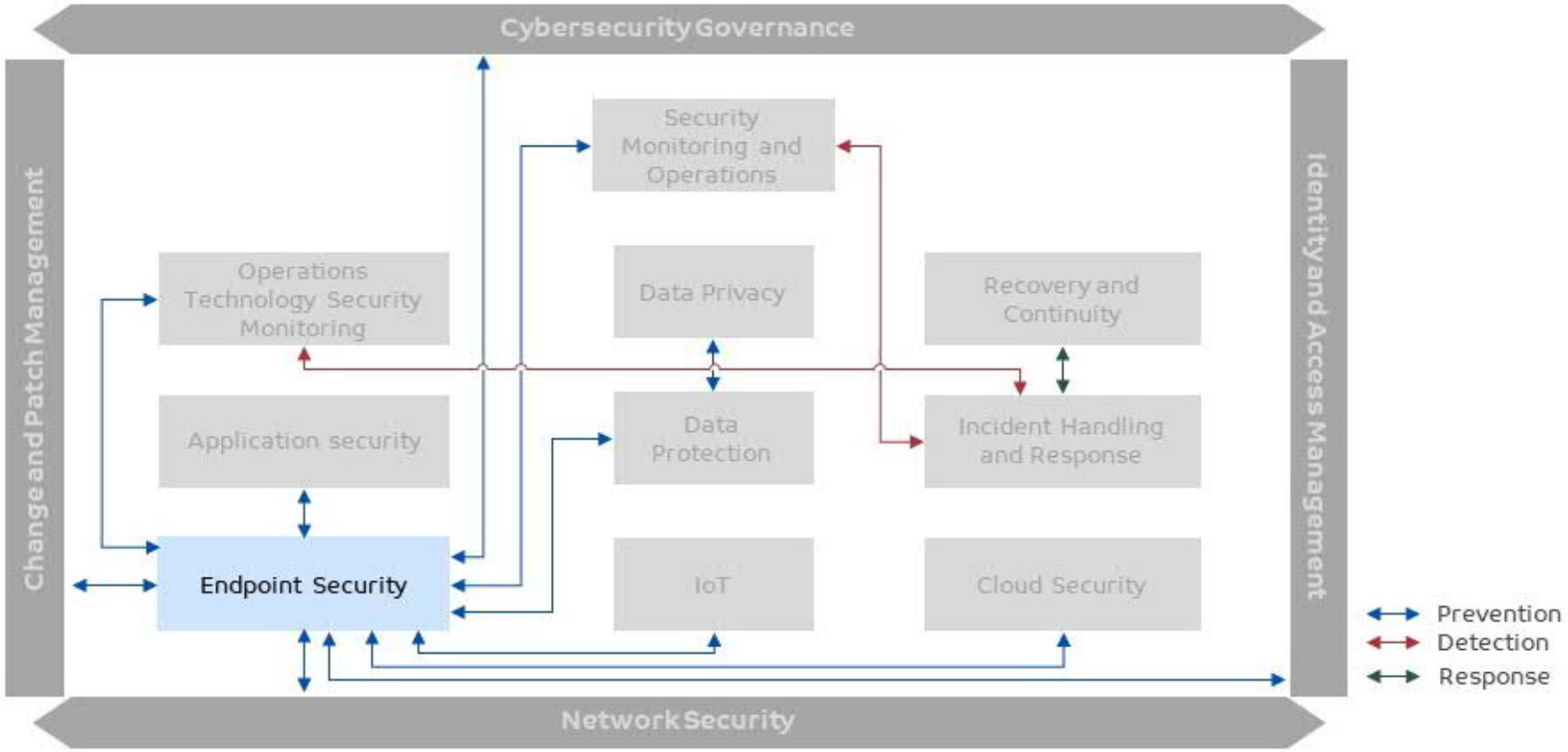
This chapter focuses on ‘Endpoint Security” capability defined under the ‘Prevention’ pillar of world cup cybersecurity capabilities.

Figure 15: Cybersecurity Capabilities – Endpoint Security



Following figure depicts linkage of Endpoint security with other cybersecurity capabilities defined in the framework

Figure 16: Endpoint Security linkage with other capabilities



3.1 Prerequisites

Following are the pre-requisites, which are required to be accomplished for Endpoint Security:

- Security risks identified for the endpoints during the risk assessment have been communicated and considered while defining endpoint security
- Assets to be protected have been identified, managed and inventoried (refer to Cybersecurity Governance capability chapter)
- Appropriate logs and events have been enabled on identified assets for collection. These logs should be forwarded to security monitoring team for analysis (refer to application security, network security, data protection and cloud security capability chapters)
- Information protection regulations and industry compliance requirements are identified
- The Operations team should be notified for any change activities (refer to change and patch management capability chapter)
- The endpoint security tooling should collect and ship logs to a centralized logging server for analysis and monitoring
- Where possible, the access to endpoints should be provided through two-factor authentication

3.2 Endpoint Security Service

From world cup perspective, ***Table 12: Endpoint Security Service*** describes respective activities that needs to be conducted for Endpoint Security service. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal policies, procedures and guidelines
- Define program scope and identify target assets
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define acceptance standards
- Deploy/configure appropriate solutions to align with establish standards
- Deploy and train team members for endpoint security support
- Identify opportunities of automation where applicable
- Define service levels for remediation activities
- Continually improve policy, procedure, and guidelines as per risk levels and lessons learned

Table 12: Endpoint Security Service

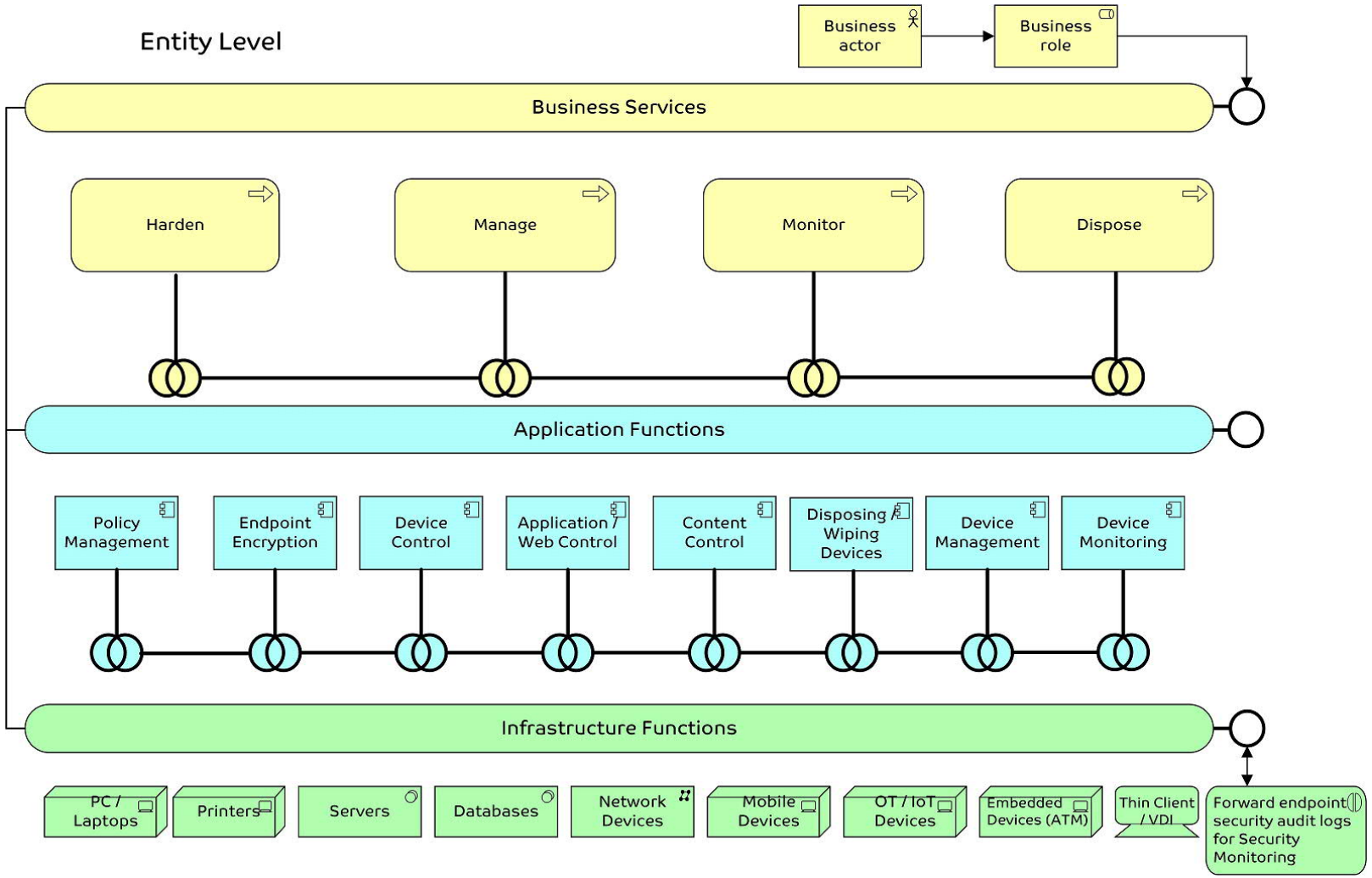
Service Name: Endpoint Security	
Description	Endpoint security is the process of providing protection to those devices connected to the network with the aim of protecting the network and an organization's data. Endpoint security addresses the risks presented by devices connecting to the network
Process Phases	**Activities/Controls**
Harden	• Implement and enforce endpoint security configurations by applying it on operating system, application and network layers

Service Name: Endpoint Security	
	• Define an endpoint security policy that dictates the type of configuration required on endpoint devices by supporting industry leading practices • Ensure that best practice security configurations are applied on endpoints • Ensure that application whitelisting is applied on endpoints
Manage	• Track asset inventory of endpoint devices on asset repository by gathering all the details of hardware, operating systems, and applications changing and configurations • Ensure that endpoint changes, patches and configuration go through a controlled change management process to continuously log and track security requirements • Install security applications on endpoint devices to ensure that right protection is applied • Integrity checking mechanisms are used to verify software, firmware, and information integrity • Manage mobile devices, related applications, and apply security controls on mobiles devices including BYOD (bring your own device) and COPE (corporate-owned, personally enabled) devices
Monitor	• Detect unprotected endpoints via security operation centre • Identify, track and detect abnormal behaviours or malicious activities • Ensure endpoint protection is applied
Dispose	• Manage reuse or final disposition of expired, obsolete devices, and unwanted endpoints in a secure manner • Ensure the information stored on obsolete, expired, and unwanted endpoints storage/media are appropriately sanitized

3.3 Endpoint Security Capability Model

Following figure illustrates an architecture model established for Endpoint Security capability at Entity level:

Figure 17: Endpoint Security Capability Model



Above figure defines the Endpoint Security capability model in layered approach:

- **The Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- **The Applications Functions layer** supports the business layer with application services which are realized by (software) application components.

- **The Infrastructure functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform.

3.4 Information Flow at various levels

Upon analysis and following confirmation that certain threats and risks are targeting the world cup specific services and associated endpoints, this should be shared with the sector/national levels as world cup specific risks and threats via the security monitoring team and utilizing vehicles such as STIX/TAXII/CyboX as mentioned in the security monitoring and operations capability. This will help in implementing unified mitigating/compensating control across the world cup ecosystem.

3.4.1 Services expected at each level

Endpoint Security service will be applicable to all the endpoints used for world cup irrespective of the level (i.e. Entity/Sector/National) it is being used.

3.5 Milestones

Following milestones have been defined for Endpoint Security:

- Hardening of all assets is applied
- Management of all assets is enabled

- Monitoring of all assets is enabled and reported
- Disposal processes are implemented

3.6 Skills required for Endpoint Security

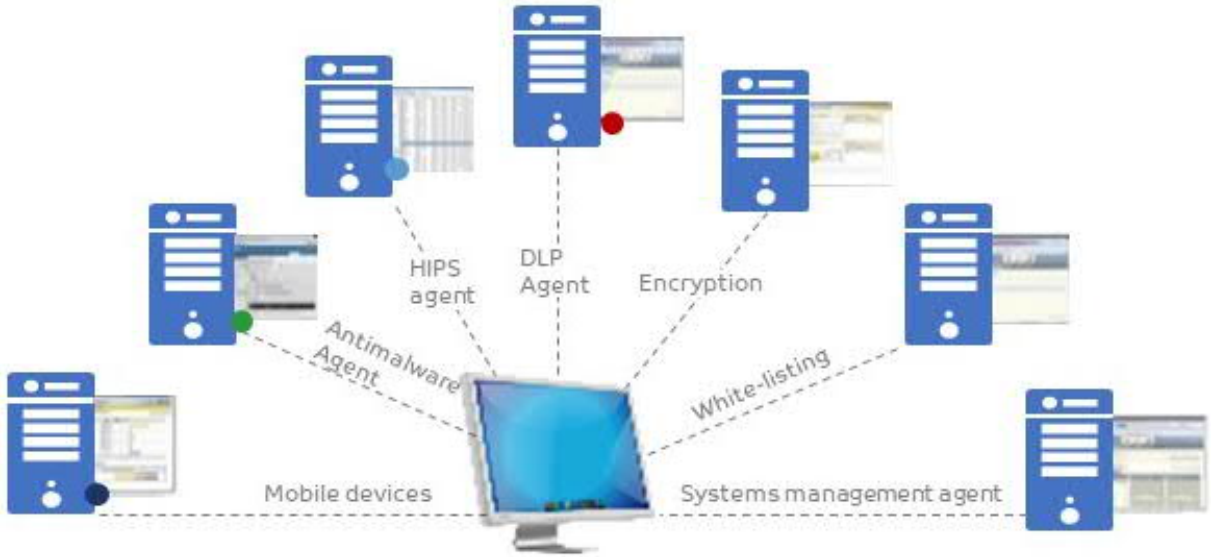
Following are the skills expected from personnel executing Endpoint Security activities:

- Technical hands-on experience with endpoint security
- Understanding of operating system, networking protocols, security and Internet environments
- Experience with common enterprise desktop software deployment methodologies
- Experience installing, configuring and integrating a security environment
- Experience troubleshooting operating system
- Experience with systems installation, configuration and administration of operating systems and applications
- In-depth knowledge of TCP/IP, routing and host-based security technologies
- Experience using application firewalls, SIEM, IDS/IPS
- Suggested certifications which can help personnel to attain skills for the services defined under endpoint security: A+, Network+, SANS GIAC Security Essentials (GSEC), SANS GIAC Certified Enterprise Defender (GCED)

3.7 Technology

Following figure shows the mapping between a device and Endpoint security technologies:

Figure 18: Endpoint Security Technologies-I



The Endpoint security technologies main purpose is to adequately secure devices by ensuring that unauthorized access is blocked, and malicious activities are detected & prevented. Endpoint security technologies may contain the following features:

- Endpoint, file, folder, and E-mail encryption
- Application whitelisting or equivalent applicable control
- Network access control
- Data loss protection
- Insider threat protection
- Endpoint detection and response (EDR)
- Privileged user control
- Logging and monitoring

Endpoint Technologies described in this section are:

- Endpoint Encryption (Hard Disk Encryption)
- File and folder encryption (Removable media, USB, SD Cards)
- File Integrity Monitoring
- Endpoint Security Management
- Mobile Device Management

- Host based Anti-Malware
- Host based IPS (Intrusion Prevention System)
- Endpoint based DLP (Data Loss Protection)
- Endpoint Detection and Response (EDR)
- Sandboxing environment

Figure 19: Endpoint Security Technologies-II

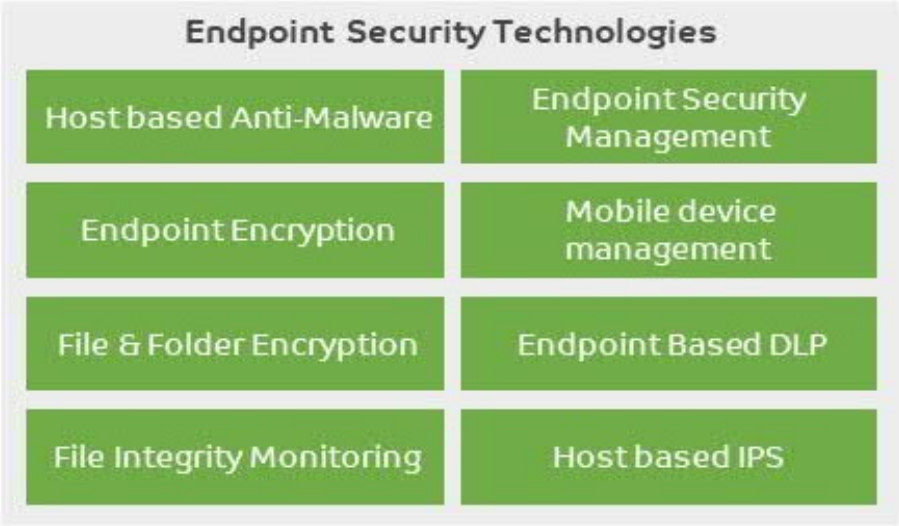


Table 13: Endpoint security Technologies

Technologies	Description
Host based Anti-Malware	Technologies that can detect, prevent, and remove malicious computer viruses/ malwares
Endpoint Encryption	Technologies that are used to provide Full Disk Encryption (FDE) by applying encryption on all disk sectors/clusters.

Technologies	Description
File and Folder Encryption	Technologies used to encrypt user files without affecting the operating system or application files.
File Integrity Monitoring	Technologies used to perform an integrity check on operating systems and application files.
Endpoint Security Management	Technologies that manage compliance on endpoint devices by providing alerts on required updated security patches.
Mobile Device Management	Technologies that secure mobile devices across a range of operating systems and service providers used in an entity.
Host based IPS	Technologies used to block actions and alert users in case of attempted malicious changes to an endpoint device by an attacker.
Endpoint based DLP	Technologies that can detect and prevent defined sensitive data from leakage
Endpoint Detection and Response (EDR)	Technologies that focus on detecting, investigating, and mitigating suspicious activities and issues on hosts and endpoints used to detect and respond to cyber threats and exploits
Sandboxing environment	Technologies used to isolate applications from critical system resources and other programs to mitigate system failures or software vulnerabilities from spreading and prevent malware or harmful applications from negatively affecting the system

3.8 Endpoint Security Hardening Controls

- Maintain documented, standard security configuration standards for all entity's authorized operating systems and software
- Maintain secure images or templates for all systems in the enterprise based on the entities approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates
- Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible
- Consider the role of the server (web server, application server, AD server) when designing the security baselines

- Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals
- Utilize a compliant configuration monitoring system to verify all security configuration elements, catalogue approved exceptions, and alert when unauthorized changes occur
- Utilize an up-to-date compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the entity's systems
- Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested
- Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses (for example a dedicated service accounts should have access to the minimum number of operations required, e.g. Nessus can do with the least number of rights needed to complete comprehensive scans).
- Deploy automated software update tools to ensure that the operating systems are running the most recent OS versions and security patches security updates provided by the software vendor
- Deploy automated software update tools to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor
- Ensure that deploying automated auto software update don’t disrupt legacy systems, automation needs to be carefully planned, scoped and tested before rolling out as some upgrades are subject to change management, testing and control (Please refer to change and patch management capability)
- Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner
- Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities
- Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges
- Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts

- Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities
- Secure virtual endpoints as you secure physical endpoints such as disable unnecessary functions, isolate virtual endpoint networks and strictly control root privileges
- Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system
    - Use multi-factor authentication and encrypted channels for all administrative account access
- Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the entity's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet
- Limit access to scripting tools to only administrative or development users with the need to access those capabilities
- Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges
- Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account
- Ensure that only fully supported web browsers and clients can be used, ideally only using the latest version of the browsers and clients provided by the vendor

- Uninstall or disable any unauthorized browser or client plugins or add-on applications
- Ensure that only authorized scripting languages can run in all web browsers and email clients
- Enforce URL filters that limit a system's ability to connect to websites not approved by the entity. This filtering shall be enforced for each of the entity systems, whether they are physically at an entity facility or not
- Log all URL requests from each of the entity systems, whether onsite or a mobile device, to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems
- Block access to known malicious domains
- Analyse and block all attachments if the file types are unnecessary for the entity's business or with malicious behaviour
- Utilize centrally managed anti-malware software to continuously monitor and defend each of the entity workstations and servers
- Ensure that the entity anti-malware software updates its scanning engine and signature database on a regular basis
- Enable anti-exploitation features such as Data Execution Prevention (DEP) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables
- Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected
- Disable the use of removable media where applicable or configure devices to not auto-run content from removable media.
- Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting
- Ensure that only network ports, protocols and services listening on a system with validated business needs are running on each system
- Perform port scans on a regular basis against all systems including OT, IoT and cloud systems and alert if unauthorized ports are detected on a system
- Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed
- Any unauthorized traffic should be blocked and logged
- Apply appropriate controls for service accounts as applicable to the environment such as restricting interactive logons or automating password management etc.
- Ensure that all remote login access to the entity network to encrypt data in transit and use multi-factor authentication
- Scan all enterprise devices remotely logging into the entity network prior to accessing the network to ensure that each of the entity security policies has been enforced in the same manner as local network devices
- Disable wireless access on devices that do not have a business purpose for wireless access
- Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks
- Disable peer-to-peer (ad-hoc) wireless network capabilities on wireless clients
- Disable wireless peripheral access of devices (Ex. Bluetooth and NFC), unless such access is required for a business purpose
- Ensure that either unauthorized devices are removed from the network or quarantined, the inventory is updated in a timely manner
- Utilize port’s level access control following 802.1x standards, to control which devices can authenticate to the network
- Use client certificates to authenticate hardware assets connecting to the entity's trusted network
- Endpoints which do not comply to the proposed security requirements should be prevented from accessing entity resources

- Ensure that endpoint protection have a capability to receive an automated threat intelligence from Security Monitoring and Operations and Incident Handling and Response capabilities and enforce the required protection to reduce the response time

3.9 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards

Table 14: Endpoint security activities mapping industry cyber security standards – Part I of II

Service Name: Endpoint Security						
Process Phases	**Activities/Controls**	**Controls Reference - NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Harden	Implement and enforce endpoint security configurations by applying it on operating system, application and network layers	AM-1	11.2.2	3, 11, 14	4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8,	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7

Service Name: Endpoint Security						
Process Phases	**Activities/Controls**	**Controls Reference - NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
					4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4	
Harden	Define an endpoint security policy that dictates the type of configuration required on endpoint devices by supporting industry leading practices		6.6.7, 6.6.15, 6.6.17, 7.4.1, 7.4.1	12	4.3.3.6.6	SR 1.13, SR 2.6
Harden	Ensure that best practice security configurations are applied on endpoints		11.2.6		4.3.4.4.4	
Manage	Track asset inventory of endpoint devices on asset repository by gathering all the details of hardware, operating systems, and applications changing and configurations			4, 20	4.2.3.1, 4.2.3.7	
Manage	Ensure that endpoint changes, patches and configuration go through a controlled change management process to continuously log and track security requirements	IE-11, GS-17	11.2.1	2, 3		SR 3.1, SR 3.3, SR 3.4, SR 3.8
Manage	Install security applications on endpoint devices to ensure adequate protection is applied			4, 7, 8, 12	4.3.4.3.8	SR 3.2

Service Name: Endpoint Security						
Process Phases	**Activities/Controls**	**Controls Reference - NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Manage	Manage mobile devices, related applications, and apply security policies on endpoint devices including BYOD (bring your own device) and COPE (corporate-owned, personally enabled) devices	AM-1	11.2.2	3, 11, 14	4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
Monitor	Detect unprotected endpoints via security operation centre					
Monitor	Identify, track and detect abnormal behaviours or malicious activities through incident handling			7, 8		SR 2.4
Monitor	Ensure endpoint protection is applied on hardware and software			1, 2, 3, 5, 9, 12, 13, 15, 16		
Dispose	Manage reuse or final disposition of expired, obsolete		6.7.1, 6.7.2, 6.8.3	1	4.3.3.3.9, 4.3.4.4.1	SR 4.2

Service Name: Endpoint Security						
Process Phases	**Activities/Controls**	**Controls Reference - NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
	devices, and unwanted endpoints in a safe manner					
Dispose	Ensure the information stored on obsolete, expired, and unwanted endpoints storage/media are appropriately sanitized		6.3.1, 6.3.2		4.3.3.3.7	

Table 15: Endpoint security activities mapping industry information security standards – Part II of II

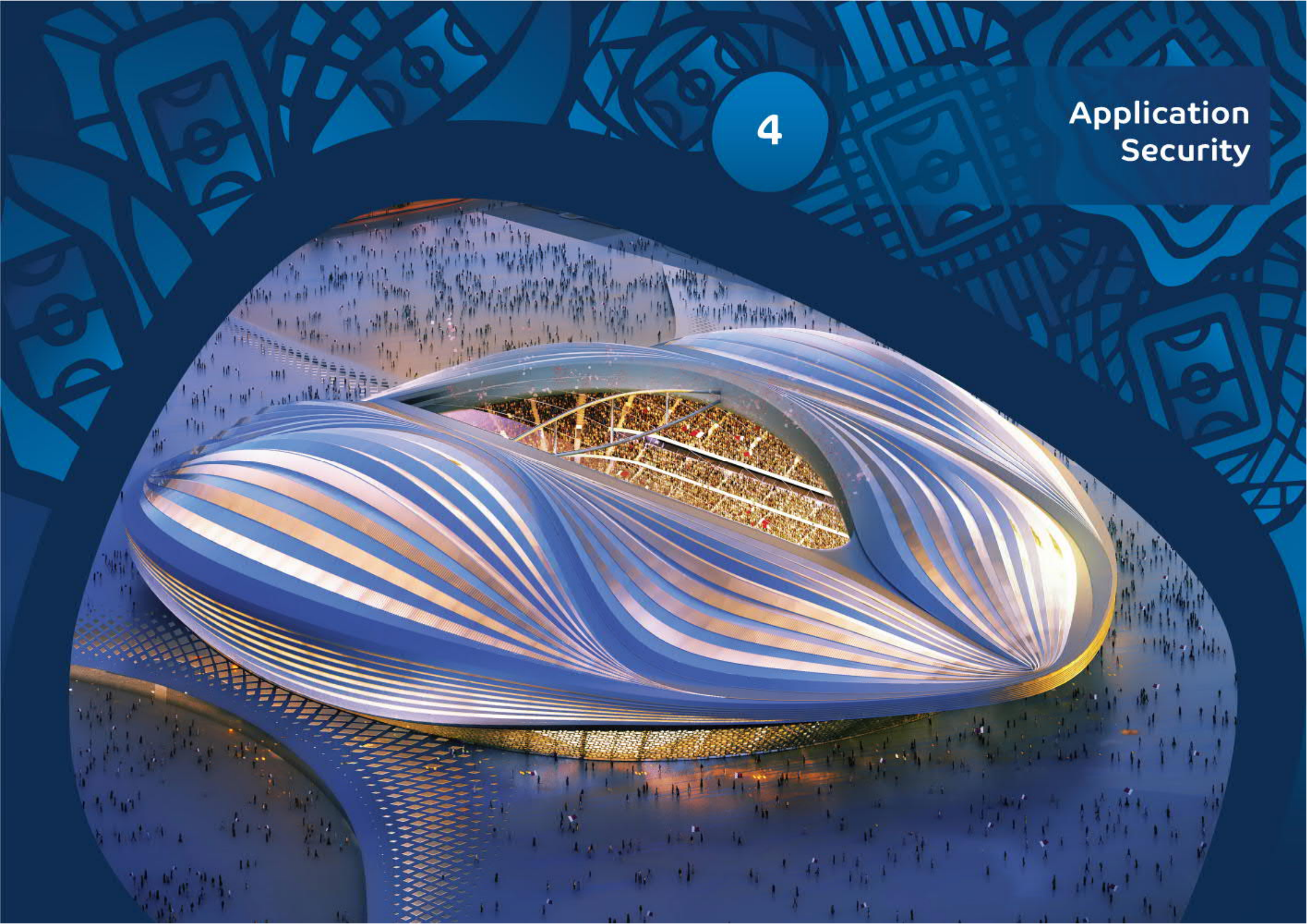
Service Name: Endpoint Security							
Process Phases	**Activities/Controls**	**Controls Reference —ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference - Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Harden	Implement and enforce endpoint security configurations by applying it on operating system, application and network layers.	A.9.1.2	AC-3, CM-7	2.2 (all), 7.1, 7.2, 9.3	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iv)		
Harden	Define an endpoint security policy that dictates the type of configuration required on endpoint devices by supporting industry leading practices	A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1	AC-1, AC-17, AC-19, AC-20, SC-15	AC-3, CM-7	164.308(a)(4)(i) 164.308(b)(1) 164.308(b)(3) 164.310(b) 164.312(e)(1) 164.312(e)(2)(ii)	IAM-09, IAM-12	
Harden	Ensure that best practice security configurations are applied on endpoints	A.11.2.4	SA-10, SI-7				
Manage	Track asset inventory of endpoint devices on asset repository by gathering all the details of hardware, operating systems, and applications changing and configurations	A.12.6.1	RA-5	11.2	164.308(a)(1)(i) 164.308(a)(8)	CCC-04, DCS-05	
Manage	Ensure that endpoint changes, patches and configuration go through a controlled change	A.12.2.1, A.12.5.1, A.14.1.2,	SC-16, SI-7	10.5, 11.5	164.308(a)(1)(ii)(D) 164.312(b) 164.312(c)(1)		

Service Name: Endpoint Security							
Process Phases	**Activities/Controls**	**Controls Reference —ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference - Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
	management process to continuously log and track security requirements	A.14.1.3, A.14.2.4			164.312(c)(2) 164.312(e)(2)(i)		
Manage	Install security applications on endpoint devices to ensure adequate protection is applied	A.12.2.1	SI-3, SI-8	5 (all)	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)	BCR-10, TVM-02	
Manage	Manage mobile devices, related applications, and apply security policies on endpoint devices including BYOD (bring your own device) and COPE (corporate-owned, personally enabled) devices	A.9.1.2	AC-3, CM-7	2.2 (all), 7.1, 7.2, 9.3	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iv)		
Monitor	Detect unprotected endpoints via security operation centre						
Monitor	Identify, track and detect abnormal behaviours or malicious activities through incident handling	A.12.5.1, A.12.6.2	SC-18, SI-4, SC-44	5 (all)	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)	BCR-10, CCC-04, CCC-05, IAM-06	

Service Name: Endpoint Security							
Process Phases	**Activities/Controls**	**Controls Reference —ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference - Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Monitor	Ensure endpoint protection is applied on hardware and software	A.12.4.1, A.14.2.7, A.15.2.1	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	10.1, 10.6.1, 11.1, 11.4, 11.5, 12.10.5	164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.310(d)(1) 164.310(d)(2)(iii) 164.312(b) 164.314(b)(2)(i)	CCC-04, IAM-03, IAM-13	
Dispose	Manage reuse or final disposition of expired, obsolete devices, and unwanted endpoints in a safe manner	A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7	CM-8, MP-6, PE-16	2.4, 9.5, 9.6, 9.7, 9.8, 9.9, 11.1.1	164.308(a)(1)(ii)(A) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv) 164.310(d)(1) 164.310(d)(2)		
Dispose	Ensure the information stored on obsolete, expired, and unwanted endpoints storage/media are appropriately sanitized	A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6	MA-2, MA-3, MA-5, MA-6	6.2	164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	DCS-04, DCS-08, GRM-06, GRM-09, AAC-03	

4

Application Security

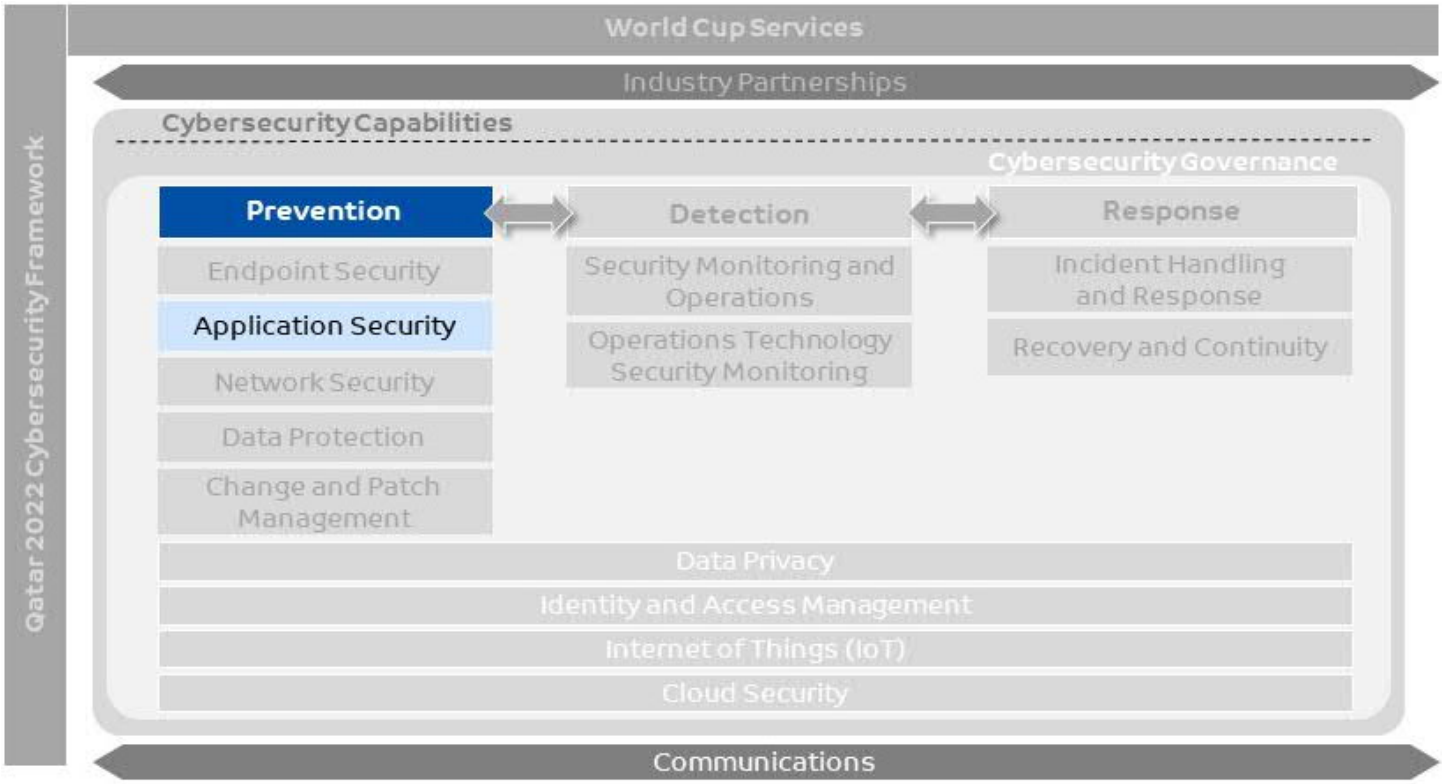


4. Capability Description – Application Security

Application Security capability is the processes use to prevent/detect/correct security weaknesses during the development, acquisition of applications and while using existing applications. Thereby reducing the application vulnerabilities before they are deployed and reduce the likelihood of successful exploitation.

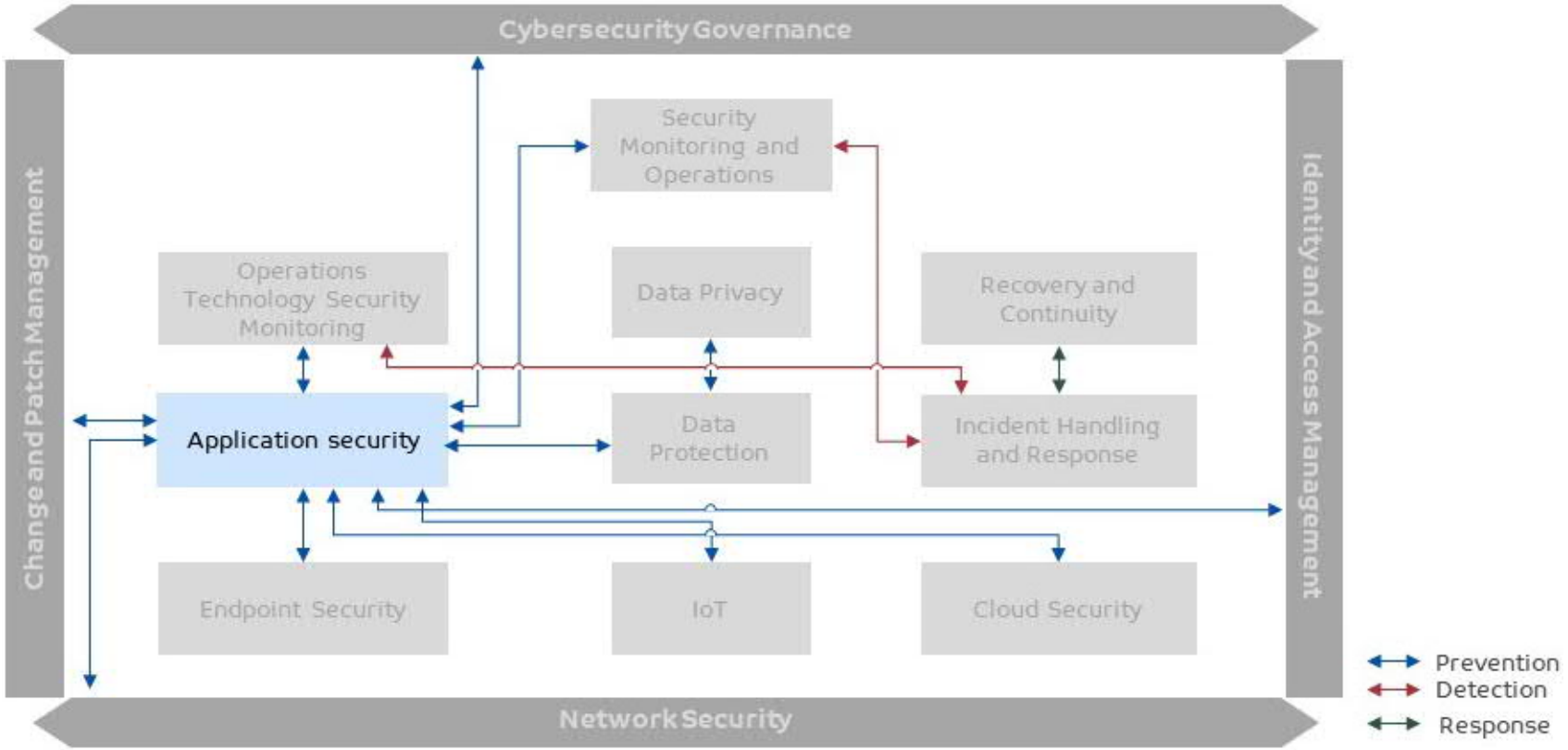
This chapter focuses on 'Application Security' capability defined under the 'Prevention' pillar of world cup cybersecurity capabilities.

Figure 20: Cybersecurity capabilities – Application Security



Following figure depicts linkage of Application security with other cybersecurity capabilities defined in the framework

Figure 21: Application Security linkage with other capabilities



4.1 Pre-requisites

Following are the pre-requisites which are required to be accomplished for application security:

- Development of application(s) has followed secure development lifecycle
- Security requirements (functional, technical and assurance requirements) has been defined before the application development commences
- Applications connected to entity's environment should use identity and access management technology, where applicable, for defined roles (refer Identity and Access Management capability chapter)
- Underlying operating system and infrastructure are hardened (refer endpoint security and network security capability chapters)
- All changes in application including patching go through change management process (refer Change and patch management capability chapter)
- Appropriate backup plans are in place for taking backups of applications which includes the configuration and required data
- Recovery and continuity for identified critical applications have been defined and tested (refer Recovery and Continuity capability chapter)
- Appropriate application security audit logs have been enabled and collected on central logging server
- Collected logs have been monitored and analysed regularly
- Events are monitored & analysed to understand attack targets and methods including external vendors, partners and service provider activity
- Application code is appropriately classified as per data classification defined and stored (refer data protection capability chapter)
- SLAs have been defined with third-party vendors from service availability and support management perspective which includes provision of security patches and updates
- Third-party vendors or application developers have provided reports for all application security testing they conducted during the secure development lifecycle of the application. This report should also include the application security processes they followed, and tools used for conducting various tests
- Entity has software escrow agreement in place with third-party vendors or application developers where applicable and required
- Application acquired and/or developed complies with all legal requirements including license, copyrights, IPR etc.
- Security risks identified for the application during the risk assessment have been communicated and considered while defining application security

4.2 Application Security Service

Following table describes service established for Application Security capability. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal policies, procedures and guidelines
- Define program scope and identify target applications
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define severity classification and acceptance standards
- Deploy/configure appropriate solutions to align with establish standards
- Deploy and train team members to support
- Identify opportunities of automation where applicable
- Define services levels for remediation activity

- Define rules of engagement which will be followed
- Continually improve policy, procedure and guidelines with changing risks and lessons learned

Table 16: Application Security Services

<table>
<tr><th colspan="2">Service Name — Application Security</th></tr>
<tr><td>Description</td><td>Application Security capability is the processes use to prevent/detect/correct security weaknesses during the development, acquisition of applications and while using existing applications. Thereby reducing the application vulnerabilities before they are deployed and reduce the likelihood of successful exploitation</td></tr>
<tr><th>Process Phases</th><th>Activities/Controls</th></tr>
<tr><td>Identify</td><td>• Software platforms and applications within the organization are inventoried
• Identify in which of the following application lifecycle phases the application is:
- Development
- Implementation</td></tr>
<tr><td>Qualify</td><td>Select appropriate application security method based on the phase the application is
<table><tr><th>Application lifecycle phase</th><th>Application Security Method</th></tr><tr><td>Development</td><td>• Secure Coding
• Threat Modelling
• Design Review</td></tr><tr><td>Implementation</td><td>• SAST
• DAST
• Application – level vulnerability shielding</td></tr></table></td></tr>
<tr><td>Test</td><td>• Test the application with the selected application security method</td></tr>
<tr><td>Treat</td><td>• The development and testing environments are separate from the production environment
• Determine and document remediation of issues
• Schedule treatment activity based on defined service levels
• Apply remediation steps, adhering to established procedure
• Track all changes made to the application</td></tr>
</table>

4.2.1 Application lifecycle phases

Following are the broad application lifecycle phases which is applicable to all types of applications:

- Development: In this phase, the application is designed, components are coded, application is built and tested
- Implementation: In this phase, the application is tested for functionality, performance and security. It is further distributed in following sub-phases:
  - User Acceptance Testing (UAT)
  - Production

4.2.2 Application Security Testing Methods

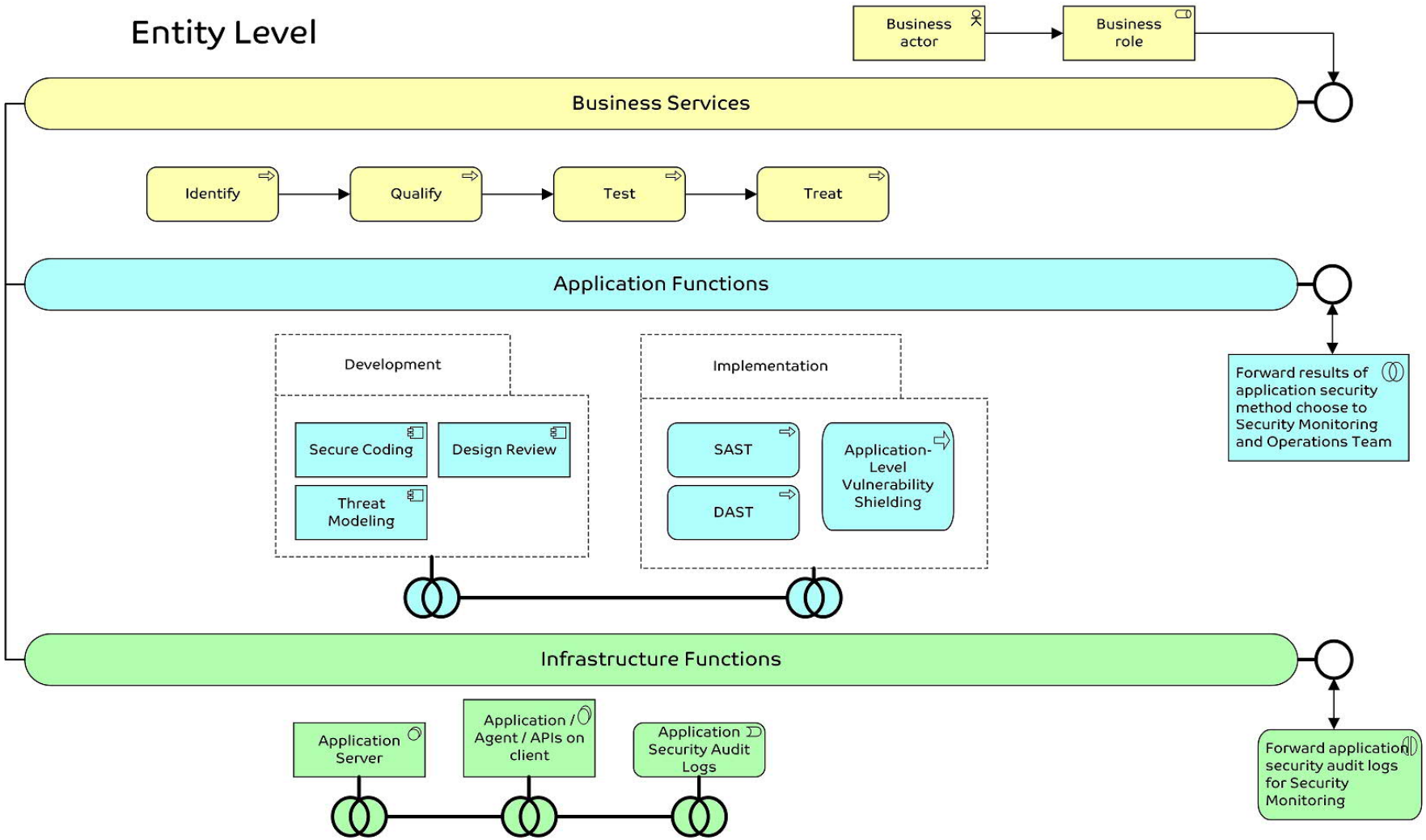
Following are the application security testing methods used during the application lifecycle as defined in section above

- **Secure Coding:** It defines a practice using which most common software/application vulnerabilities can be mitigated (refer ***Secure Coding*** in Compendium section)
- **Threat Modelling**: It is a structured approach for analysing the security of an application and enables to identify, quantify and address the security risks associated with an application (refer ***Threat*** in Compendium section)
- **Design Review:** It is focused on assessment of application design and architecture for security-related issues. This allows to detect architecture-level issues early in application development (refer ***Design Review*** in Compendium section)
- **SAST:** It defines detecting and correcting vulnerabilities in individual components of an application at the source, at object code or at binary level (refer *Error! Reference source not found.* in Compendium section)
- **DAST**: It defines detecting vulnerabilities using penetration-testing techniques at the “black box” level during implementation and during operational use (refer *Error! Reference source not found.* in Compendium section)
- **Application-level Vulnerability Shielding:** It is a practice of deploying and managing technologies to prevent the exploitation of vulnerabilities in operational applications before patches or updates can be applied (refer Error! Reference source not found. in Compendium section)

4.3 Application Security Capability Model

Following figure illustrates an architecture model of processes established for Application Security capability at entity level:

Figure 22: Application Security Capability Model



Above figure defines the Application Security capability model in layered approach:

- **The Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- **The Applications Functions layer** supports the business layer with application services which are realized by (software) application components.

- **The Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform.

4.4 Information Flow at various levels

Upon analysis and following confirmation that certain threats and risks are targeting the world cup specific services and associated applications, this should be shared with the sector/national levels as world cup specific risks and threats via the security monitoring team and utilizing vehicles such as STIX/TAXII as mentioned in the security monitoring and operations capability. This will help in implementing unified mitigating/compensating control across the world cup ecosystem.

4.4.1 Services expected at each level

Application Security service will be applicable to all the applications used for world cup irrespective of the level (i.e. Entity/Sector/National) it is being used.

4.5 Milestones

Following milestones have been defined for security monitoring and operations:

- All world cup applications go through applicable application security method defined
- Identified application weaknesses communicated to sector and national level

4.6 Application Security Methods

4.6.1Secure Coding

Secure coding is a practice using which most common software/application vulnerabilities can be mitigated

Use the OWASP Secure Coding Practices Quick Reference Guide which is a technology agnostic set of general software security coding practices, in a comprehensive checklist format, that can be integrated into the development lifecycle. This guide focuses on:

- Secure coding requirements, rather than on vulnerabilities and exploits
- Technical controls specific to mitigate the occurrence of common software/application vulnerabilities

At minimum following Top 10 Secure Coding practices needs to be followed:

1. **Validate input —** Validate input from all untrusted data sources. Proper input validation can eliminate most software vulnerabilities. Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user-controlled files
2. **Heed compiler warnings —** Compile code using the highest warning level available for compiler used and eliminate warnings by modifying the code. Use static and dynamic analysis tools to detect and eliminate additional security flaws
3. **Architect and design for security policies —** Create a software architecture and design the software/application to implement and enforce security policies. For example, if application system requires different privileges at different times, consider dividing the system into distinct intercommunicating subsystems, each with an appropriate privilege set
4. **Keep it simple —** Keep the design as simple and small as possible. Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use. Additionally, the effort required to achieve an appropriate level of assurance increases dramatically as security mechanisms become more complex
5. **Default deny —** Base access decisions on permission rather than exclusion. This means that, by default, access is denied, and the protection scheme identifies conditions under which access is permitted
6. **Adhere to the principle of least privilege —** Every process should execute with the least set of privileges necessary to complete the job. Any elevated permission should be held for a minimum time. This approach reduces the opportunities an attacker must execute arbitrary code with elevated privileges
7. **Sanitize data sent to other systems —** Sanitize all data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components. Attackers may be able to invoke unused functionality in these components using SQL, command, or other injection attacks. This is not necessarily an input validation problem because the complex subsystem being invoked does not understand the context in which the call is made. Because the calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem
8. **Practice defence in depth —** Manage risk with multiple defensive strategies, so that if one layer of defence turns out to be inadequate, another layer of defence can prevent a security flaw from becoming an exploitable vulnerability and/or limit the consequences of a successful exploit. For example, combining secure programming techniques with secure runtime environments should reduce the likelihood that vulnerabilities remaining in the code at deployment time can be exploited in the operational environment

9. **Use effective quality assurance techniques —** Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Fuzz testing, penetration testing, and source code audits should all be incorporated as part of an effective quality assurance program. Independent security reviews can lead to more secure systems. External reviewers bring an independent perspective; for example, in identifying and correcting invalid assumptions
10. **Adopt a secure coding standard —** Develop and/or apply a secure coding standard for target development language and platform

4.6.2Threat Modelling

Threat modelling is a structured approach for analysing the security of an application and enables to identify, quantify, and address the security risks associated with an application

From details about threats and likely attacks against each application, the organization operates more effectively through better decisions about prioritization of initiatives for security. Additionally, decisions for risk acceptance are more informed, therefore better aligned to the business.

The objective to conduct threat modelling is to investigate following:

1. The trust boundaries to and within the application
2. The actors that interact within and outside of the trust boundaries
3. Information flows within and to and from the trust boundaries
4. Information persistence within and out of trust boundaries
5. Threats to transgression of trust boundaries by actors and for information flow and persistence
6. Vulnerabilities at trust boundaries as accessed by actors and for information flow and persistence
7. Threat agents that can exploit the vulnerabilities
8. Impact of exploitation of vulnerability by a threat agent
9. Decision tree to treat the risk

4.6.3Design Review

The Design Review is focused on assessment of application design and architecture for security-related problems. This allows an organization to detect architecture-level issues early in application development and thereby avoid potentially large costs from refactoring later due to security concerns.

Following table is the checklist that should be used for design review, it should be improved as per security requirement of the application.

Table 17: Application architecture and design considerations

Application Architecture and Design Considerations	
Input Validation	• All entry points and trust boundaries are identified by the design • Input validation is applied whenever input is received from outside the current trust boundary • The design assumes that user input is malicious • Centralized input validation is used where appropriate • The input validation strategy that the application adopted is modular and consistent

Application Architecture and Design Considerations	
	• The validation approach is to constrain, reject, and then sanitize input • (Looking for known, valid, and safe input is much easier than looking for known malicious or dangerous input) • Data is validated for type, length, format, and range • The design addresses potential canonicalization issues • Input file names and file paths are avoided where possible • The design addresses potential SQL injection issues • The design addresses potential cross-site scripting issues • The design does not rely on client-side validation • The design applies defence in depth to the input validation strategy by providing input validation across tiers • Output that contains input is encoded using HtmlEncode and UrltEncode
Authentication	• Application trust boundaries are identified by the design • The design identifies the identities that are used to access resources across the trust boundaries • The design partitions the Web site into public and restricted areas using separate folders • The design identifies service account requirements • The design identifies secure storage of credentials that are accepted from users • The design identifies the mechanisms to protect the credentials over the wire (SSL, IPSec, encryption etc.) • Account management policies are taken into consideration by the design • The design ensure that minimum error information is returned in the event of authentication failure • The identity that is used to authenticate with the database is identified by the design • If SQL authentication is used, credentials are adequately secured over the wire (SSL or IPSec) and in storage (DPAPI) • The design adopts a policy of using least-privileged accounts • Password digests (with salt) are stored in the user store for verification • Strong passwords are used • Authentication tickets (cookies) are not transmitted over non-encrypted connections
Authorization	• The role design offers enough separation of privileges (the design considers authorization granularity) • Multiple gatekeepers are used for defence in depth • The application's login is restricted in the database to access-specific stored procedures • The application's login does not have permissions to access tables directly • Access to system level resources is restricted • The design identifies code access security requirements. Privileged resources and privileged operations are identified • All identities that are used by the application are identified and the resources accessed by each identity are known
Configuration Management	• Administration interfaces are secured (strong authentication and authorization is used) • Remote administration channels are secured

Application Architecture and Design Considerations	
	• Configuration stores are secured • Configuration secrets are not held in plain text in configuration files • Administrator privileges are separated based on roles (for example, site content developer or system administrator) • Least-privileged process accounts and service accounts are used
Sensitive Data	• Secrets are not stored unless necessary. (Alternate methods have been explored at design time) • Secrets are not stored in code • Database connections, passwords, keys, or other secrets are not stored in plain text • The design identifies the methodology to store secrets securely. (Appropriate algorithms and key sizes are used for encryption. It is preferable that DPAPI is used to store configuration data to avoid key management) • Sensitive data is not logged in clear text by the application • The design identifies protection mechanisms for sensitive data that is sent over the network • Sensitive data is not stored in persistent cookies • Sensitive data is not transmitted with the GET protocol
Session Management	• SSL is used to protect authentication cookies • The contents of authentication cookies are encrypted • Session lifetime is limited • Session state is protected from unauthorized access • Session identifiers are not passed in query strings
Cryptography	• Platform-level cryptography is used, and it has no custom implementations • The design identifies the correct cryptographic algorithm (and key size) for the application's data encryption requirements • The methodology to secure the encryption keys is identified • The design identifies the key recycle policy for the application • Encryption keys are secured • DPAPI is used where possible to avoid key management issues • Keys are periodically recycled
Parameter Manipulation	• All input parameters are validated (including form fields, query strings, cookies, and HTTP headers) • Cookies with sensitive data are encrypted • Sensitive data is not passed in query strings or form fields • HTTP header information is not relied on to make security decisions • View state is protected using machine authentication code (MAC)
Exception Management	• The design outlines a standardized approach to structured exception handling across the application • Application exception handling minimizes the information disclosure in case of an exception • The design identifies generic error messages that are returned to the client

Application Architecture and Design Considerations	
	• Application errors are logged to the error log • Private data (for example, passwords) is not logged
Auditing and Logging	• The design identifies the level of auditing and logging necessary for the application and identifies the key parameters to be logged and audited • The design considers how to flow caller identity across multiple tiers (at the operating system or application level) for auditing • The design identifies the storage, security, and analysis of the application log files
Database Security	• Secure credentials should be created for database access, a limit should be set for the use of privileged accounts • Implement a white list (allowed characters/input) and black list (disallowed characters/input) approach for input validation within the database components • Strongly typed variables should be allowed in the DB components • The application should use the lowest possible level of privilege when accessing the database • Use stored procedures to abstract data access and allow for the removal of permissions to the base tables in the database
Deployment and Infrastructure Considerations	• Deployment and Infrastructure Considerations • The design identifies, understands, and accommodates the company security policy • Restrictions imposed by infrastructure security (including available services, protocols, and firewall restrictions) are identified • The design recognizes and accommodates restrictions imposed by hosting environments (including application isolation requirements) • The target environment code-access-security trust level is known • The design identifies the deployment infrastructure requirements and the deployment configuration of the application • Domain structures, remote application servers, and database servers are identified • The design identifies clustering requirements • The design identifies the application configuration maintenance points (such as what needs to be configured and what tools are available for an IDC admin) • Secure communication features provided by the platform and the application are known • The design addresses Web farm considerations (including session state management, machine specific encryption keys, Secure Sockets Layer (SSL), certificate deployment issues, and roaming profiles) • The design identifies the certificate authority (CA) to be used by the site to support SSL • The design addresses the required scalability and performance criteria

4.6.4Application Security Testing

Application security testing (AST) is the process of evaluating the security of a computer system or network by methodically verifying and validating the effectiveness of application security controls.

- Verify means that the software product meets the stated requirements; this can be done by inspection as well as by automated tests
- Validate means that the product meets those requirements by exercising the product, including negative testing, to identify security vulnerabilities that may be present but are not accounted for in the defined security requirements

Following are two major types of application security testing:

- **Static Application Security Testing (SAST):** It is a set of technologies designed to analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyse an application from the "inside out" in a non-running state.
- **Dynamic application security testing (DAST):** These technologies are designed to detect conditions indicative of a security vulnerability in an application in its running state.

Table 18: SAST vs DAST

	SAST	DAST
Testing Method	• SAST, also known as white box testing or developer viewpoint • Perform code analysis, including source, binary and intermediate builds • Verifies the application from an inside viewpoint • Exposes security flaws in code, rather than exploitable vulnerabilities	• DAST, also known as black box testing or hacker viewpoint • Test application components or full applications when the internal working of the component or app is not required • Validates the application from an outside viewpoint • Exposes actual exploits and behaviour of applications responding to those exploits • Popular with security auditors and penetration testers
Strengths	• Finds vulnerabilities early in the development phase, thereby allowing remediation earlier • Supports all software methods and architectures	• Easily automated, efficient, flexible and scalable • Allows continuity of application security from UAT deployment to production • Finds runtime vulnerabilities • Integrates easily into organization security strategy; findings map directly to risk and prioritization • Can quickly be deployed by the security team
Weaknesses	• No evaluation of runtime vulnerabilities, as application is not tested under production conditions, where insecure server configuration may introduce serious vulnerabilities • No evaluation of how components interact	• Prone to false positives and negatives, especially for fully automated solutions • May not catch all vulnerabilities • Oriented toward latter phases (Deploy and Maintain) • Effectiveness limited to web applications and web services

4.6.5Most Common Application Security Risks

While conducting the application security testing, the objective is to identify most significant application security risks and apply mitigating/compensatory controls to avoid their exploitation. Following are the most prevalent application security lists which are followed during application security testing:

- OWASP Top 10
- CWE/SANS Top 25 most dangerous software errors

Above mentioned both lists are updated regularly based on application attack patterns, thus it is recommended to follow most recent one.

Following table describes OWASP TOP 10 application security risks

Table 19: OWASP Top 10 Application Security Risks

OWASP TOP 10 Application Security Risks	
A1:2017-Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization
A2:2017-Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently
A3:2017-Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser
A4:2017-XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks

OWASP TOP 10 Application Security Risks	
A5:2017-Broken Access Control	Restrictions on what authenticated users can do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion
A7:2017-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites
A8:2017- Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks
A9:2017-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defences and enable various attacks and impacts
A10:2017-Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring

Following table describes CWE/SANS Top 25 most dangerous software errors:

Table 20: CWE/SANS Top 25 most dangerous software errors

CWE/SANS Top 25 most dangerous software errors	
Insecure Interaction Between Components These weaknesses are related to insecure ways in which data is sent and received between separate components, modules, programs, processes, threads, or systems	
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
Risky Resource Management	

CWE/SANS Top 25 most dangerous software errors	
The weaknesses in this category are related to ways in which software does not properly manage the creation, usage, transfer, or destruction of important system resources.	
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-494	Download of Code Without Integrity Check
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-676	Use of Potentially Dangerous Function
CWE-131	Incorrect Calculation of Buffer Size
CWE-134	Uncontrolled Format String
CWE-190	Integer Overflow or Wraparound
Porous Defence's The weaknesses in this category are related to defensive techniques that are often misused, abused, or just plain ignored	
CWE-306	Missing Authentication for Critical Function
CWE-862	Missing Authorization
CWE-798	Use of Hard-coded Credentials
CWE-311	Missing Encryption of Sensitive Data
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-250	Execution with Unnecessary Privileges
CWE-863	Incorrect Authorization
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-759	Use of a One-Way Hash without a Salt

4.6.6 Application-Level Vulnerability Shielding

It's a practice of deploying and managing technologies to prevent the exploitation of vulnerabilities in operational applications before patches or updates can be applied. Following are the two most prevalent technologies which are used to shield application-level vulnerabilities:

- Web Application Firewall (WAF)
- Run time self-protection (RASP)

4.6.6.1 Web Application Firewall (WAF)

Web Application Firewalls (WAFs) are designed to protect web applications. It's a shielding safeguard intended to defend applications accessed via the HTTP. They can prevent attacks that network firewalls or IPS cannot. In general, WAF is placed in front of a web application, monitor application activity and alert on or block traffic that is malicious or that does not comply with defined rules. The objective is to catch application level attacks, such as SQL injection and cross-site scripting, along with attempts to manipulate web application behaviour.

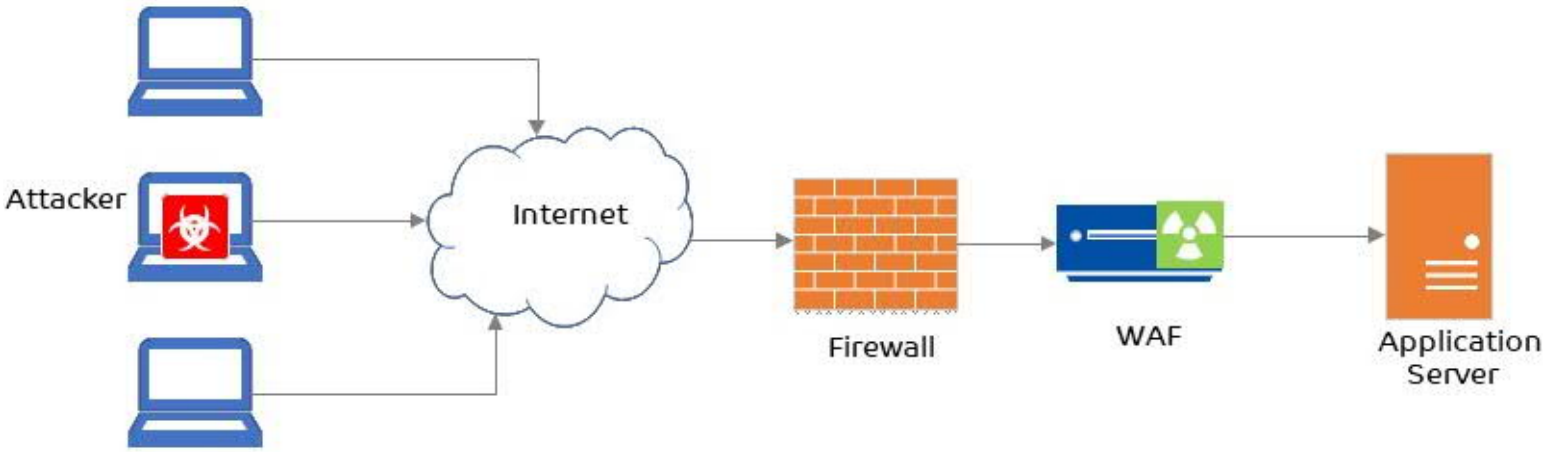
This shielding technology does not require modification of the application source code. WAFs can reduce application security risk without fixing the underlying technology, this feature is known as virtual patching. In cases where it might take a long time or it is infeasible to fix the application level vulnerability in code, a WAF is useful in protecting against attacks targeting the vulnerability.

For example, when new web application vulnerabilities are found, virtual patching quickly remediates the risk without needing to change the application's source code. For production applications that will take time to fix, utilizing a web application firewall to deploy a virtual patch will require the least amount of effort for the desired security posture. For a legacy or COTS application, it could be the only mitigating control available.

Virtual patching can help in reducing the exploit window but should not be used as the only solution. It should be noted that the actual patch should be implemented as soon as it is available and tested.

WAF have several architectures and operating modes which vary in ease of deployment and resulting WAF functionality. However, in general it is deployed in reverse proxy mode. In this mode, the WAF is placed inline, all incoming connections to the application are sent to the WAF, which makes a separate request to the web server. Encrypted connections are terminated at Layer 7 (OSI Model) letting the WAF decrypt and analyse all the web traffic. This allows for a more feature rich WAF deployment as it gives the WAF complete control over the traffic enabling it to rewrite content and inject security mechanisms per policy. Following figure shows reverse proxy implementation of WAF.

Figure 23: WAF Deployment in reverse proxy mode



4.6.6.2 Runtime application self-protection (RASP)

Runtime application self-protection (RASP) is a security technology that is built or linked into an application or application runtime environment and is capable of controlling application execution and detecting and preventing real-time attacks.

RASP incorporates security into a running application wherever it resides on a server. It intercepts all calls from the application to a system, making sure they are secure, and validates data requests directly inside the application. RASP can protect web and non-web applications. The technology does not affect the design of the application because RASP's detection and protection features operate on the server where the application is running on.

When a security event occurs in application, RASP takes control of the application and addresses the problem. In diagnostic mode, RASP will alert that something is detected. In protection mode, it will try to stop it by taking either of actions like terminating a user's session, stopping an application's execution, or alerting security monitoring team.

Developers can implement RASP in following ways:

- Access the technology through function calls included in an application's source code. This approach is more precise because developers can make specific decisions about what they want protected in the app, such as logins, database queries, and administrative functions
- Take a completed application and put it in a wrapper that allows the application to be secured with a single button push

Whichever method is used with RASP, the result is bundling a web application firewall with the application's runtime context

4.7 Skills required for Application Security

Following are the skills expected from personnel executing application security activities:

- Analyse and specify the security requirements for secure development at all phases of SDLC
- Provide Application security training to developers, architects, testers and administrators
- Perform risk assessment of Application Design to identify security bugs at the design stage of SDLC
- Ensure security and privacy requirements are met before the application development
- Provide security architecture and advice in support of application development, infrastructure, and technology projects.
- Define, document and implement the application security guidelines for development, testing and deployment
- Identify architectural and other security risks associated with the solution, and compensating controls where necessary
- Knowledge of Secure Development of technologies and platform used in the application
- Perform Static and Dynamic Security testing of the application code
- Regular Application Security testing and consistently to make sure that appropriate security measures have been added.
- Remediation and tracking of the security issues identified within the application
- Ensure security tools and technologies are deployed in the current environment in line with architectural requirements.

- Perform security hardening of application environment, web server, application server, operating system and network components deployed
- Manages the system vulnerabilities by establishing and running the patch management process and conducting network scans
- Monitoring anomalous behaviour in the application
- Suggested professional certifications which can help personnel to attain skills for the services defined under security monitoring and operations:
    - SANS GIAC Certified Web Application Defender (GWEB)
    - SANS GIAC Certified Secure Software Programmer-Java (GSSP-Java)
    - SANS GIAC Certified Secure Software Programmer- .NET (GSSP-.NET)
    - ISC2 Certified Secure Software Lifecycle Professional (CSSLP)
    - EC-COUNCIL Certified Secure Programmer (ECSP)

4.8 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards

Table 21: Application security activities mapping industry information security standards – Part I of II

Service Name: Application Security						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identify	Software platforms and applications within the organization are inventoried	SS9		2	4.2.3.4	SR 7.8
Identify	Identify in which of the following application lifecycle phases the application is: o Development o Implementation					
Qualify	Select appropriate application security method based on the phase the application is * Development: Secure Coding/Threat Modelling /Design Review * Implementation: SAST/DAST/Application — level vulnerability Shielding					
Test	Test the application with the selected application security method	SS6 SS7 SS22 SS23 SS24 SS25 SS26 SS27 SS28 SS29 SS30 SS31 SS32		18		

Service Name: Application Security						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Treat	The development and testing environments are separate from the production environment	SS4 SS5 SS7				
Treat	Determine and document remediation of issues					
Treat	Schedule treatment activity based on defined service levels					
Treat	Apply remediation steps, adhering to established procedure	SS5 SS7				
Treat	Track all changes made to the application	SS18				

Table 22: Application security activities mapping industry information security standards – Part II of II

Service Name: Application Security							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference —PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference —GDPR**
Identify	Software platforms and applications within the organization are inventoried	A.13.2.1 A.13.2.2	AC-4 CA-3 CA-9 PL-8	2.4	164.308(a)(1)(ii)(A) 164.308(a)(7)(ii) €		
Identify	Identify in which of the following application lifecycle phases the application is: * Development * Implementation						
Qualify	Select appropriate application security method based on the phase the application is * Development: Secure Coding/Threat Modelling/Design Review * Implementation: SAST/DAST/Application - level vulnerability Shielding						
Test	Test the application with the selected application security method		SA-11 SA-15 SA-17	6.2 6.3 6.5 6.6 6.7		AIS-01 AIS-02 AIS-03 AIS-04	
Treat	The development and testing environments are separate from the production environment			6.4		IVS-08	
Treat	Determine and document remediation of issues						

Service Name: Application Security							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference —PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference —GDPR**
Treat	Schedule treatment activity based on defined service levels						
Treat	Apply remediation steps, adhering to established procedure						
Treat	Track all changes made to the application		SA-10	6.4		CCC-01 CCC-02	

5

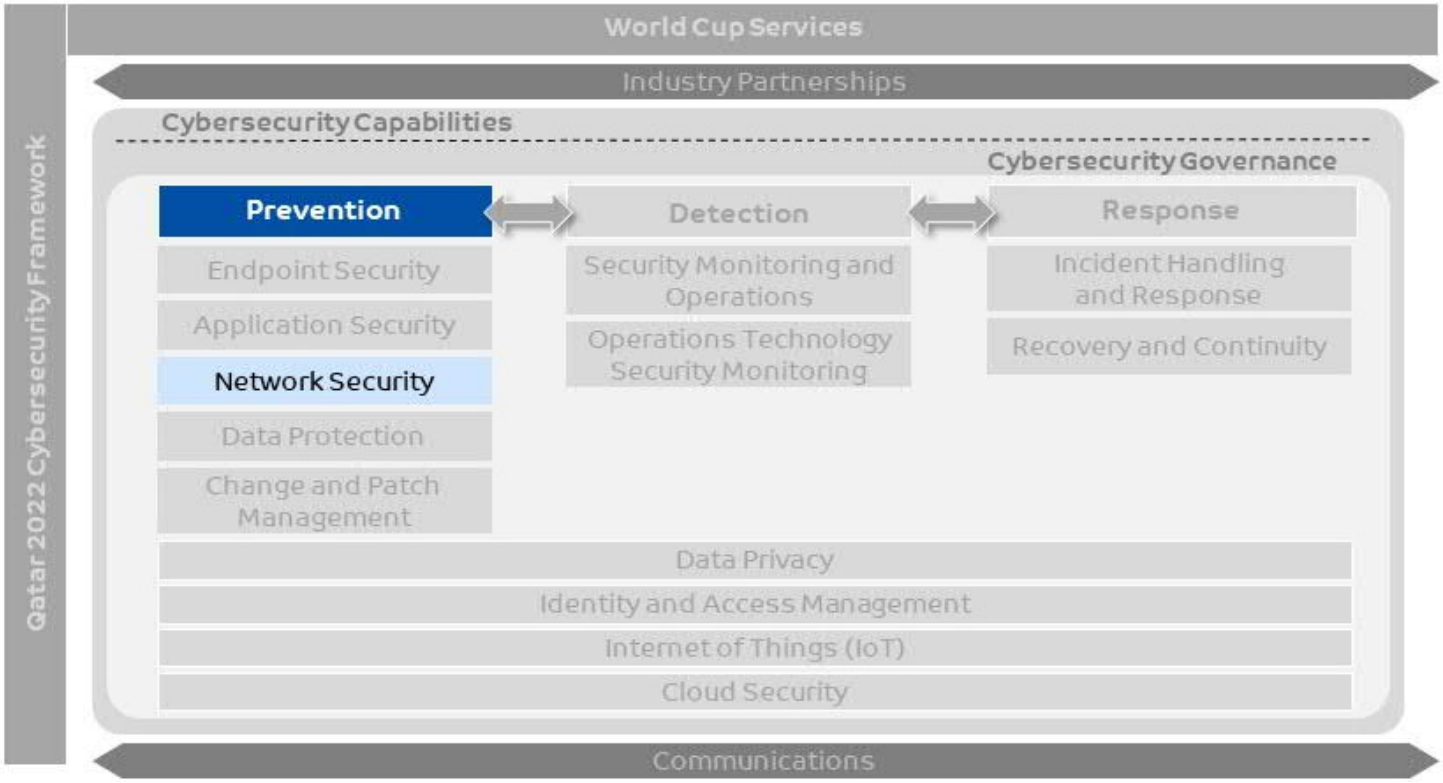
Network Security

5. Capability Description – Network Security

A critical capability for protecting the Infrastructure and hardware used to interconnect devices and systems for communication internally and externally. This capability will implement the processes, controls and technologies required to build an effective Network Security program that is aligned to the business and focused on protecting all systems that matters most with respect to services provided in world cup.

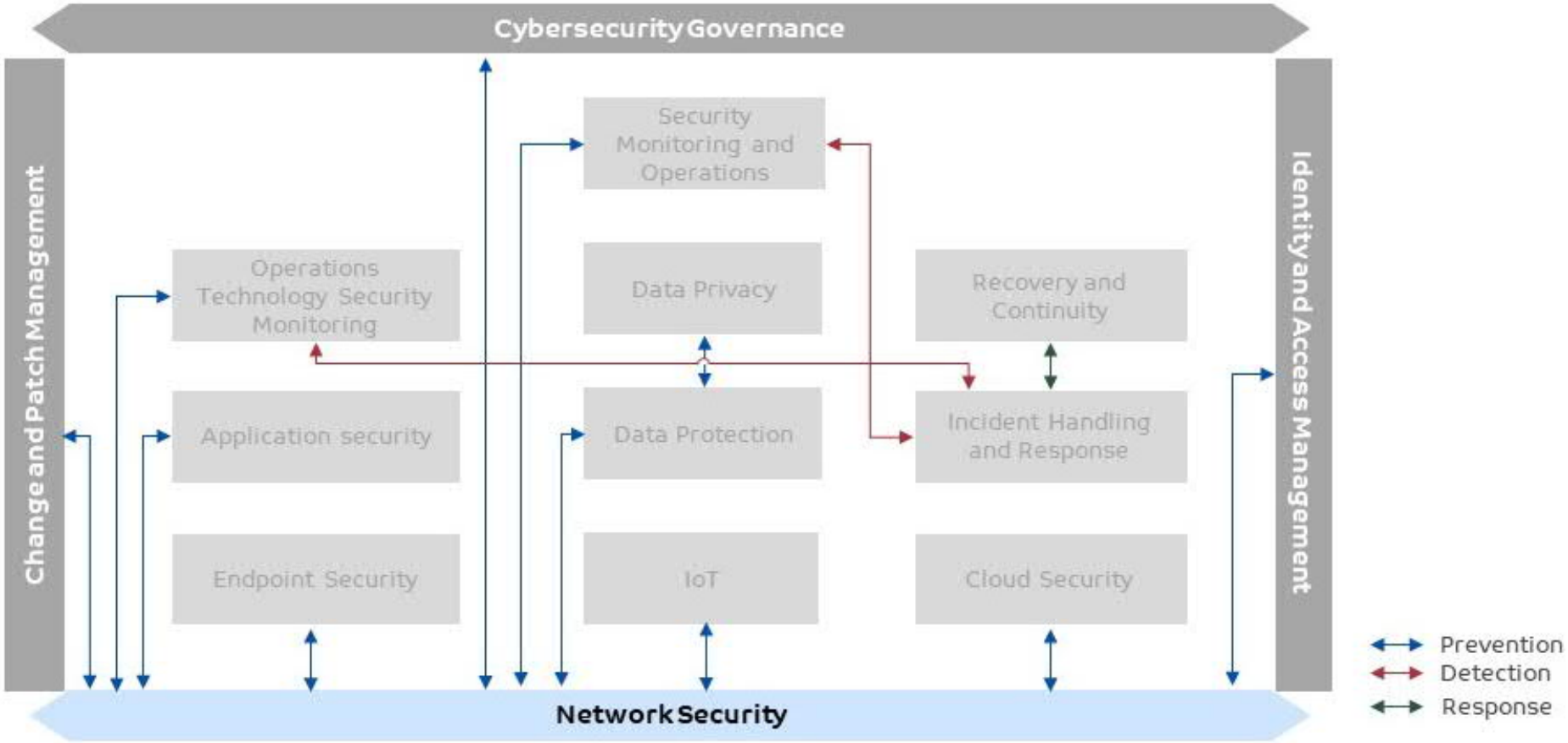
This chapter focuses on 'Network Security' capability defined under the 'Prevention' pillar of world cup cybersecurity capabilities.

Figure 24: Cybersecurity capabilities – Network Security



Following figure depicts linkage of Network security with other cybersecurity capabilities defined in the framework

Figure 25: Network Security linkage with other capabilities



5.1 Prerequisites

Following are the pre-requisites, which are required to be accomplished for Network Security capability:

- Security risks are identified for the network and infrastructure during the risk assessment, which has been communicated and considered while implementing network security
- Assets and network infrastructure to be protected have been identified (refer to other capability chapters cybersecurity governance, data protection, application security, data privacy and cloud security)
- Assets connected to the corporate network, managed and information security policies are applied
- Appropriate logs and events have been enabled on identified assets for collection and analysis (refer to other capability chapters application security, data protection and cloud security)
- Information protection regulations and industry compliance requirements are identified
- All changes on the network should be authorized through change and patch management (refer Change and Patch management capability chapter)

5.2 Various services under Network Security capability

From world cup perspective, following sections describes network security services that have been defined under this capability and respective activities that needs to be conducted for each service. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal policies, procedures and guidelines
- Define program scope and identify target assets
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define availability criteria and acceptance standards
- Deploy/configure appropriate solutions to align with establish standards
- Deploy and train team members to support
- Identify opportunities of automation where applicable
- Define services levels for remediation activity
- Define rules of engagement which will be followed
- Continually improve policy, procedure & guidelines with changing risks and lessons learned

5.2.1 Network Configuration Management Service

Following table describes service established for Network Configuration Management:

Table 23: Network Configuration Management Service

Service Name: Network Configuration Management Service	
Description	Network Security Configuration Management is the process, in which the secure configuration baseline of network components is formalized and subsequently verified against the actual state.
Process Phases	**Activities/Controls**
Prepare	• Network infrastructure devices within the organization are inventoried • Organizational communication and data flows within the system and between interconnected systems are mapped
Implement	• A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) • Network integrity is protected (e.g. network segregation, network segmentation) • Configuration change control and patch processes are in place and followed through change and patch management (refer change and patch management capability chapter) • Communications and control networks are protected • Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
Maintain	• A baseline of network operations and expected data flows for users and systems is established and managed • Vulnerability scans are performed in collaboration with Security Monitoring and Operations (refer Security Monitoring and Operations capability chapter)
Review	• Management and dashboard reporting of identified Security Configuration • Deviations. • Event detection information is communicated to appropriate parties - In case of Alert, Network Security Team will execute response actions - In case of Incident/Breach, Incident Response Team will execute response actions

5.2.2Network Access Control Management Service

Following table describes service established for Network Access Control Management:

Table 24: Network Access Control Management Service

Service Name: Network Access Control Management Service	
Description	Network Access Control Management is the process to control – who (user) or what (devices) has authorized permission to access the network.

Service Name: Network Access Control Management Service	
Process Phases	**Activities/Controls**
Prepare	• Physical devices and systems within the organization are inventoried • Organizational communication and data flows within the system and between interconnected systems are mapped • Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
Provision	• Physical and network access to assets is managed and protected • Remote access of users and devices are managed • Network integrity is protected (e.g., network segregation, network segmentation) • Data-at-rest is protected (refer Data Protection capability chapter) • Data-in-transit is protected (refer Data Protection capability chapter) • Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access • Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks) • Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties • Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
Maintain	• A baseline of network operations and expected data flows for users and systems is established and managed • Vulnerability scans are performed in collaboration with team responsible for Security Monitoring and Operations (refer Security Monitoring and Operations capability chapter)
Review	• Management and dashboard reporting of identified Network Access Control deviations. • Event detection information is communicated to appropriate parties - In case of Alert, Network Security Team will execute response actions - In case of Incident/Breach, Incident Response Team will execute response actions

5.2.3Network Monitoring Management Service

The Network Monitoring Management is to maintain infrastructure availability and performance as defined and manage alerts/incidents in a way that reduces downtime. It focuses to handle issues such as:

- DDoS Attacks, power outages, network failures;
- Remote hands support, the configuration of hardware (such as firewalls and routers) routing black-holes;
- Port management (Opening and closing ports on the firewall to allow the network to communicate with outside servers);
- Communications with network users when a major incident occurs, impacting network services; and
- First level triage of network change requests; once validated, then forward to appropriate stakeholders.

Following table describes service established for Network Monitoring Management service:

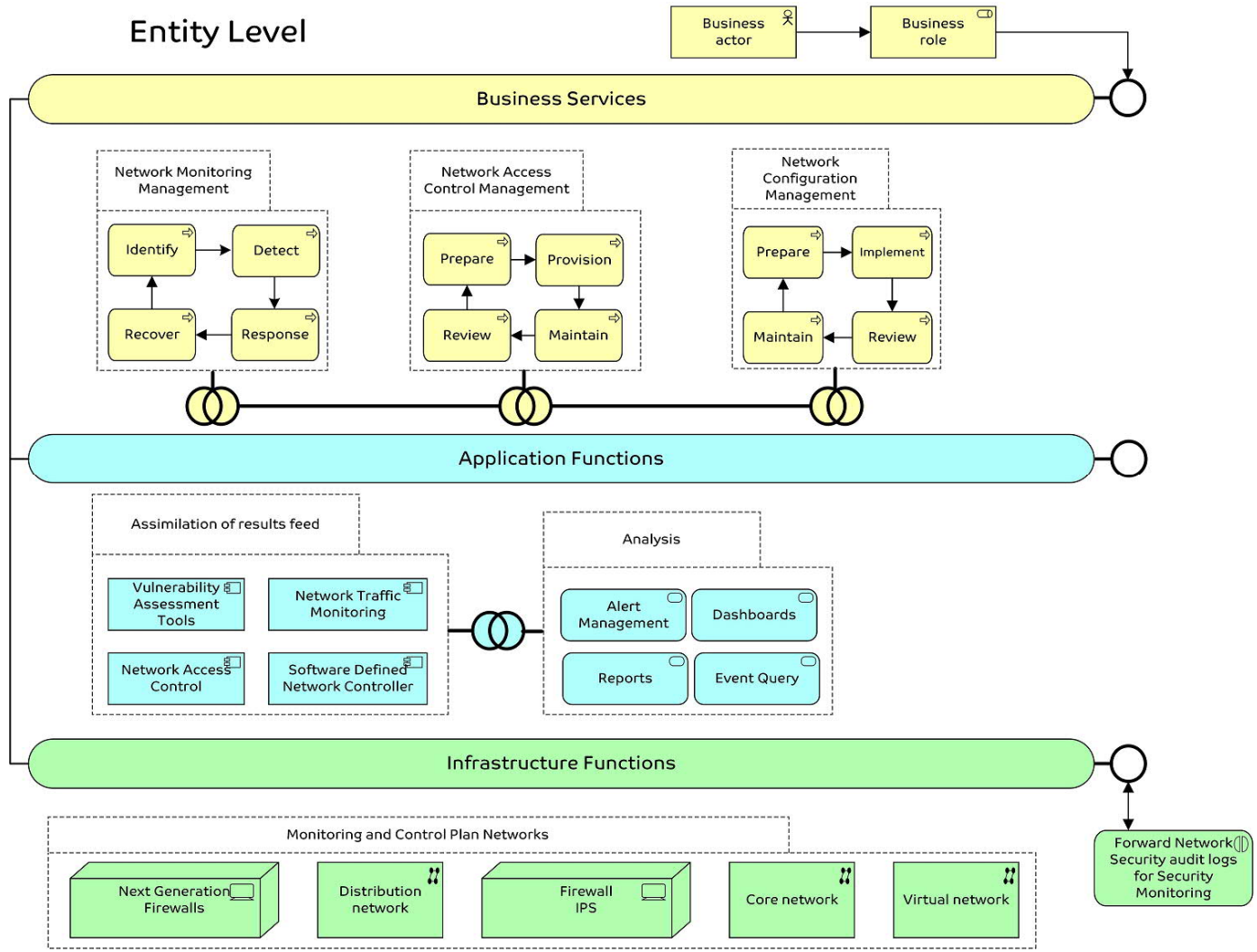
Table 25: Network Monitoring Management Service

Service Name: Network Monitoring Management Service	
Description	Network Monitoring Management, part of Network Operations Centre (NOC), is a process to handle incidents and alerts that affect performance and availability of the network.
Process Phases	**Activities/Controls**
Identify	• Physical devices and systems within the organization are inventoried • Organizational communication and data flows within the system and between interconnected systems are mapped • External network systems are catalogued • Adequate capacity to ensure availability is maintained
Detect	• Detected events are analysed to understand attack targets and methods • Event data are collected and correlated from multiple sources and sensors • Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools • Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access • Network Vulnerability scans are performed in collaboration with team responsible for Security Monitoring and Operations (refer Security Monitoring and Operations capability chapter) • Network Monitoring processes are tested • Network Audit/log records are determined, documented, implemented, and reviewed
Response	• Notifications from detection systems are investigated • Coordination with internal and external stakeholders occurs consistent with response/escalation plans • Event detection information is communicated to appropriate parties - In case of Alert, Network Security Team will execute response actions - In case of Incident/Breach, Incident Response Team will execute response actions
Recover	In collaboration with Teams responsible for Security Monitoring and Operation and Incident Handling and Response • Recovery plan is executed during or after a cybersecurity incident • Incidents are contained • Incidents are mitigated • Newly identified vulnerabilities are mitigated or documented

5.3 Network Security Capability Model

Following figure illustrates an architecture model of various functions established for Network Security:

Figure 26: Network Security Capability Model



Above figure defines the Network Security capability model in layered approach:

- **The Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- **The Applications Functions layer** supports the business layer with application services which are realized by (software) application components.

- **The Infrastructure functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform.

5.4 Information Flow at various levels

Upon analysis and following confirmation that certain threats and risks are targeting the world cup specific services and associated network or network appliances, this should be shared with the sector/national levels as world cup specific risks and threats via the security monitoring team and utilizing vehicles such as STIX/TAXII as mentioned in the security monitoring capability. This will help in implementing unified mitigating/compensating control across the world cup ecosystem. Services expected at each level.

5.4.1 Services expected at each level

Network Security service will be applicable to all the networks used for world cup irrespective of the level (i.e. Entity/Sector/National) it is being used.

5.5 Criteria to categorise Event in Alert/Incident/Breach

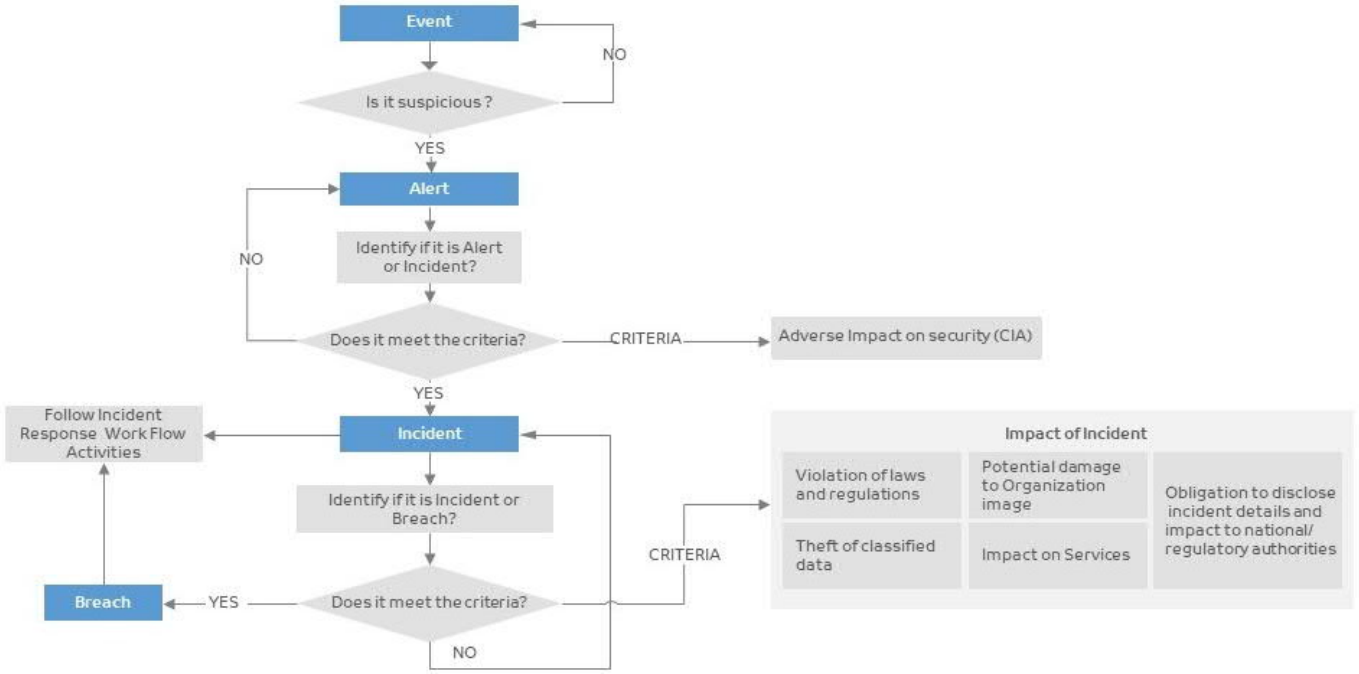
Following are some the important definitions that needs to be considered while defining the categorization criteria:

- **Event:** An action marked, logged to a point in time that may require additional assessment
- **Alert:** a notification that change is observed to the normal behaviour of a system/environment/process/ workflow

- **Incident:** an adverse event that compromises Confidentiality, Integrity or Availability of an information asset, and has been verified as a potential threat.
- **Breach:** an incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party.

Following figure defines the criteria that needs to be followed for categorization among alert/event/incident/breach.

Figure 27: Criteria to categorize Event and Incident



5.6 Skills required

- Solid Knowledge of the IT Network Security domains and corresponding solutions
- Capable of evaluating the cyber risks related to networks to the IT /OT environment
- Knowledge of the TCP/IP stack, OSI model, Network hierarchy models, security zones, VLANs, Network access controls, Intranet/Extranet Edge gateway, remote access, QoS, firewalls, configuring rules, routing & switching, ACLs, scripting etc.
- Knowledge of SIEM, security events logging and monitoring technologies
- Awareness of Network monitoring technology platforms
- Solid understanding of applicable best practices and security standards such as NIST 800-53, SABSA, Qatar's National ICS security standard, etc.

- Suggested vendor provided certifications (CCIE, CCSP, CCNP, etc.)

5.7 Technology

The following contains a detailed Network Security Capability for:

- Enterprise Network Security used for E-commerce including Online booking platforms (i.e. Aviation, Tourism and Hospitality)
- Payment Network Security used by Finance and Banking Sectors
- Telecommunications Network Security
- Healthcare Data Network Security used for used by Healthcare sector
- Industrial Control System (ICS) Network Security used by Energy and Utility sector
- Government Network Security

5.7.1 Network Security Architecture

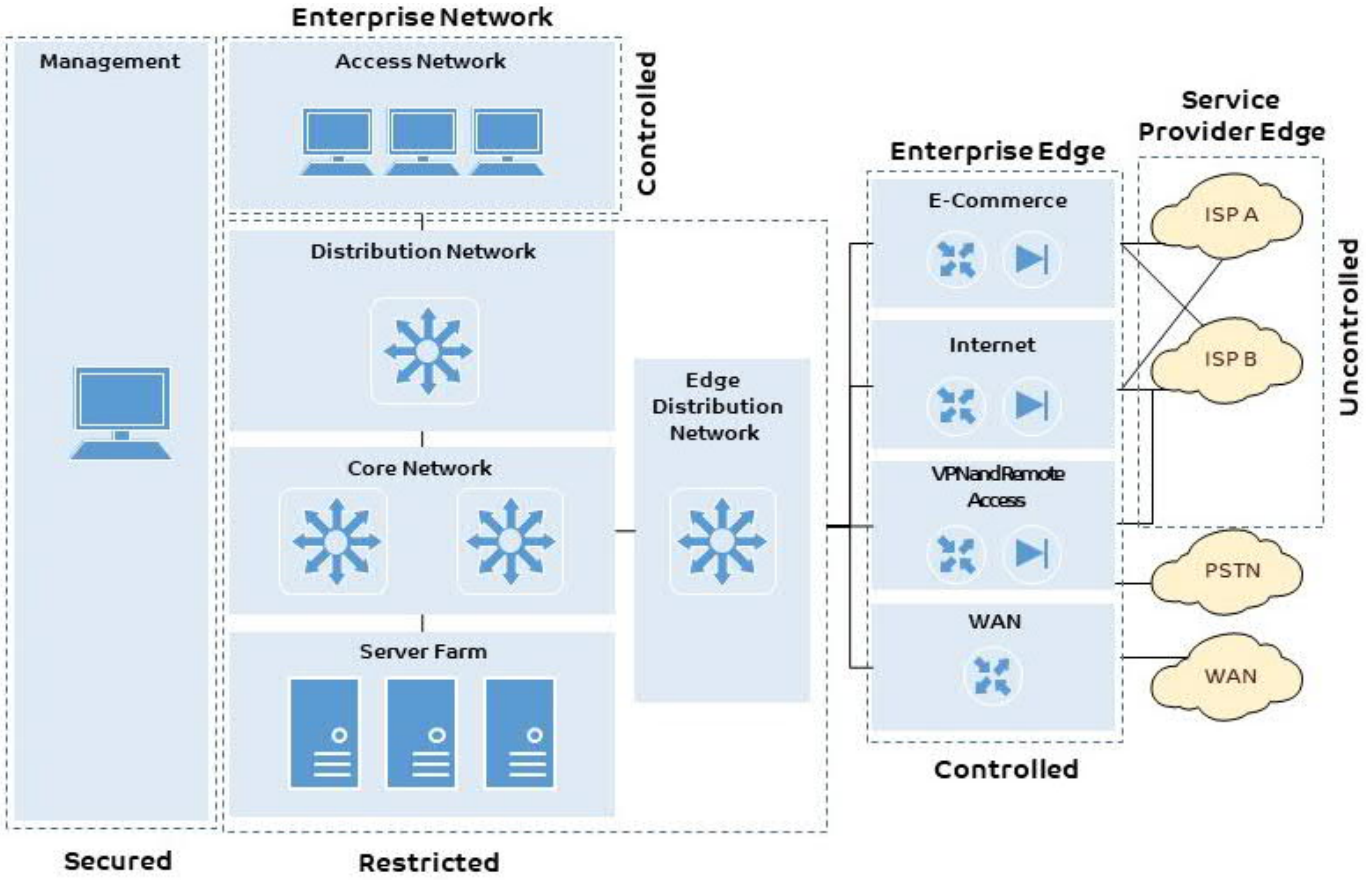
The network security architecture uses a modular approach that has two main advantages allowing:

- The architecture to address the security relationship between the various functional blocks of the network
- The designers to evaluate and implement security on a module by module basis, instead of attempting the complete architecture in a single phase

This approach provides a guide for implementing different security functions throughout the network. Though most enterprise networks evolve with the growing IT requirements of the entity, the Network Security architecture for an enterprise uses a modular approach.

As shown in Figure 28: An enterprise network architecture model, an enterprise network architecture model separates the enterprise network into functional areas that are referred to as modules. These modules perform specific roles in the network and have specific security requirements, but their sizes are not meant to reflect their scale in a real network

Figure 28: An enterprise network architecture model



The following are the primary an enterprise network Architecture module:

Enterprise network: consists of sub modules to provide high availability through a resilient hierarchical network design, redundant features, and automatic procedures for reconfiguring network paths when failures occur. Network security is integrated to protect against and mitigates the impact of attacks on the network.

Enterprise edge module: functions as a liaison between the enterprise network module and the other modules. Also, it provides connectivity for voice, video, and data services outside the enterprise. This module consists of sub modules providing the following:

- E-commerce sub module enables enterprises to support e-commerce applications through the Internet
- Internet connectivity provides internal users with secure connectivity to Internet services such as public servers, email, and DNS. Connectivity to one or several Internet service providers (ISPs) is also provided
- Remote access and VPN access provides remote-access termination services, including authentication for remote users and sites
- WAN site-to-site VPN access uses various WAN technologies for routing traffic between remote sites and the central site

Server Provider Edge sub module is provided by service providers (SPs) to link to other sites. Also, the Internet service provider (ISP) module is not implemented by the enterprise but is included to the extent that specific security features should be requested of an ISP to mitigate against certain attacks.

Note: An enterprise may use multiple remote data centres with all the same functional options as a main data centre. This provides an added layer of security as the offsite data centre can provide disaster recovery and business continuance services for the enterprise.

5.7.2Common Network Security

Zone segmentation

The network model introduces different network zones to allow the placement of IT/OT components according to their risk and security classifications. The breaks between each network zone indicate the use of either a firewall, network IPS, or both, that clearly delineates each perimeter from the others. The following are zone categories:

- **Uncontrolled** - Refers to anything outside the control of an entity
- **Controlled** - Restricts access between uncontrolled and restricted zones
- **Restricted** - Access is restricted and controlled for authorized individuals to gain access.
- **Secured** - Access is available only to a small group of highly trusted users
- **External controlled** - An external zone in which data is stored by business partners external to the systems, where there is limited trust in the protection of data

Network Routing Security

Routing security is a critical element in network security deployment, where it controls access from every network to every network. Routers advertise networks and filter and are potentially vulnerable. By their nature, routers provide access and, therefore, entities should secure them to reduce the likelihood that they are directly compromised. Entity may refer to other documents that have been written about router security.

Entities should take the following precautions router security:

- Locking down telnet access to a router
- Locking down Simple Network Management Protocol (SNMP) access to a router
- Controlling access to a router

- Turning off unneeded services
- Logging at appropriate levels
- Authentication of routing updates

Network Switching Security

Like routers, switches (both Layer 2 and Layer 3) have their own set of security considerations. Most of the security techniques detailed in the preceding section.

Entities should take the following precautions:

- Ports without any need to trunk, should have any trunk settings set to off, as opposed to auto. This prevents a host from becoming a trunk port and receiving all traffic that would normally reside on a trunk port
- Make sure that trunk ports use a virtual LAN (VLAN) number not used anywhere else in the switch. This prevents packets tagged with the same VLAN as the trunk port from reaching another VLAN without crossing Layer 3 devices
- Set all unused ports on a switch to a VLAN that has no Layer 3 connectivity. Better yet, disable any port that is not needed. This prevents hackers from plugging in to unused ports and communicating with the rest of the network
- Avoid using VLANs as the sole method of securing access between two subnets. The capability for human error, combined with understanding that VLANs and VLAN tagging protocols were not designed with security in mind, makes their use in sensitive environments inadvisable. When VLANs are needed in security deployments, be sure to pay close attention to the configurations and guidelines mentioned above
- Within an existing VLAN, private VLANs provide some added security to specific network applications. Private VLANs work by limiting which ports within a VLAN can communicate with other ports in the same VLAN
- Isolated ports within a VLAN can communicate only with promiscuous ports. Community ports can communicate only with other members of the same community and promiscuous ports. Promiscuous ports can communicate with any port. This is an effective way to mitigate the effects of a single compromised host
- If private VLANs are deployed, once one system is compromised, it cannot communicate with the other systems

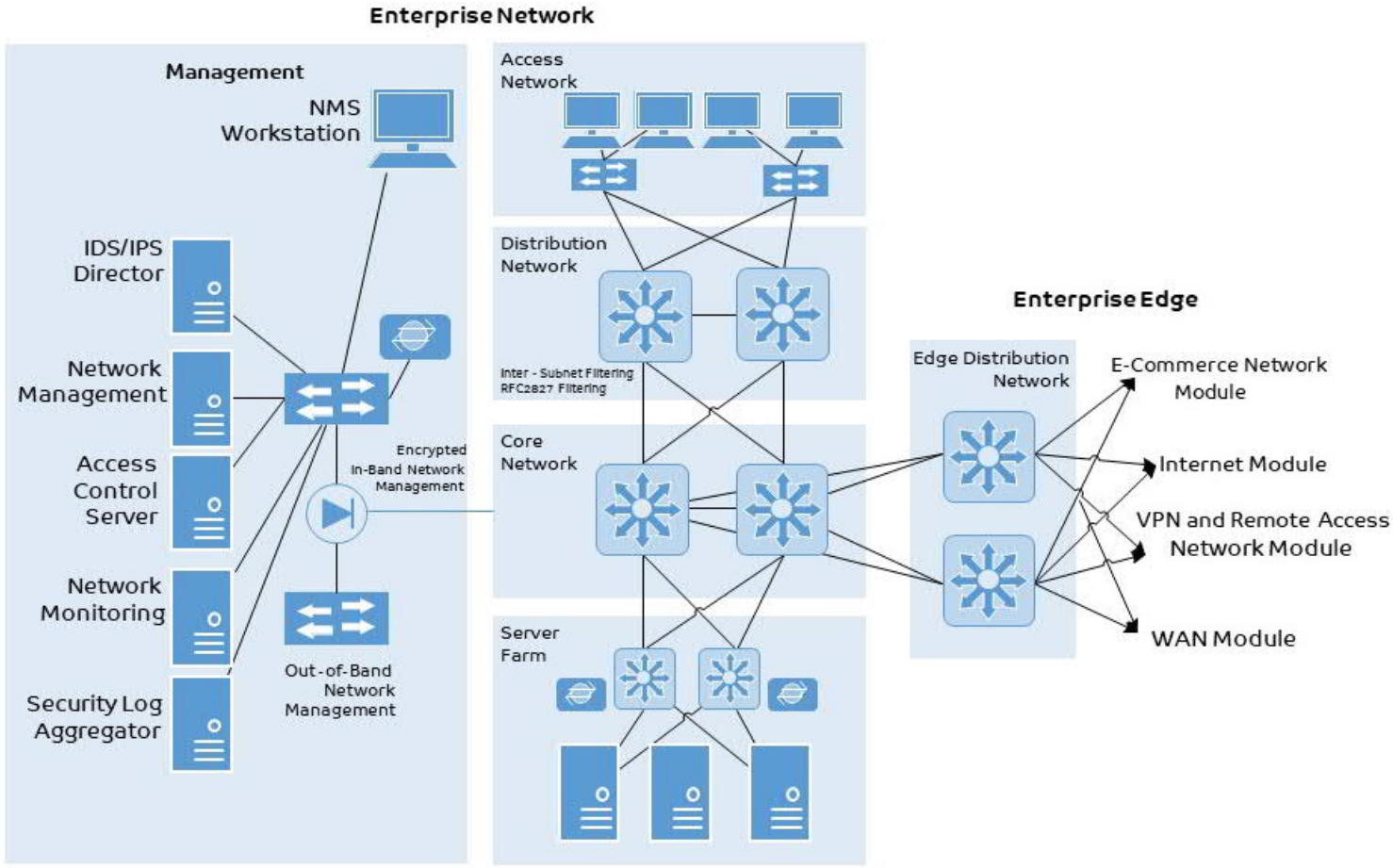
Secure Management and Reporting

From an architectural design point of view, providing out-of-band management of network systems is the recommended practice. Out-of-band (OOB), as its name implies, refers to a network on which no production traffic resides. Devices should have a direct local connection to such a network where possible, and where impossible, (due to geographic, or system-related issues) the device should connect via a private encrypted tunnel over the production network. Such a tunnel should be preconfigured to communicate only across the specific ports required for management and reporting. The tunnel should also be locked down so that only appropriate hosts can initiate and terminate tunnels. Be sure that the out-of-band network does not itself create security issues.

5.7.3Management Module

The primary goal of the management module is to facilitate the secure management of all devices and hosts within the enterprise Network Security architecture. Logging and reporting information flow from the devices through to the management hosts, while content, configurations, and new software flow to the devices from the management hosts.

Figure 29: Management Network



Key Devices

- **Network Management Server (NMS)** – provides SNMP management for devices
- **Security Log Aggregator** – aggregates log information for Firewall and Security appliances
- **Access Control Server** – delivers one-time, two-factor authentication services to the network devices
- **System Admin host** – provides configuration, software, and content changes on devices

- **NIDS/IPS appliance** – provides Layer 4 to Layer 7 monitoring of key network segments in the module
- **Management Zone Firewall** – allows granular control for traffic flows between the management hosts and the managed devices
- **Management switch** (with private VLAN support) – ensures data from managed devices can only cross directly to the firewall

Threats Mitigated

- **Unauthorized Access** – filtering at the firewall stops most unauthorized traffic in both directions
- **Man-in-the-Middle Attacks** – management data is crossing a private network making man-in-the-middle attacks difficult
- **Network Reconnaissance** – because all management traffic crosses this network, it does not cross the production network where it could be intercepted
- **Password Attacks** – the access control server allows for strong two-factor authentication at each device
- **IP Spoofing** – spoofed traffic is stopped in both directions at the management zone firewall Packet Sniffers – a switched infrastructure limits the effectiveness of sniffing
- **Trust Exploitation** – private VLANs prevent a compromised device from masquerading as a management host

Design Considerations

- Enterprise management network has two network segments that are separated by a secure firewall that acts as VPN termination device
  - The segment outside the firewall connects to all the devices that require management
  - The segment inside the firewall contains the management hosts themselves that act as terminal servers.
  - The remaining interface connects to the production network but only for IPSec-protected management traffic from predetermined hosts
  - Both management subnets operate under an address space that is separate from the rest of the production network. This ensures that the management network will not be advertised by any routing protocols.
- The management module provides configuration management for all devices in the network. More advance management features (software changes, content updates, log and alarm aggregation, and SNMP management) are provided through the dedicated management network segment
- Unmanaged devices and hosts are managed through IPSec tunnels that originate from the management network.
- Network management network has administrative access to nearly every area of the network.
- From a security perspective, syslog provides important information regarding security violations and configuration changes. Therefore, a proper aggregation and analysis system for the syslog information is critical to the proper management of a network
- All configurations were done on a standalone Network Management Workstation using management applications and the command-line interface (CLI)
- Complete out-of-band management is not always possible because some devices might not support it or there might be geographic differences that dictate in-band management. When in-band management is required, more emphasis needs to be placed on securing the transport of the management protocols
- All firewall policies should by default be configured to LOG and sent as a SYSLOG to the SIEM tool. Unless a firewall policy is generating excessive LOGs and through a risk assessment is observed that logging is not required then it may be removed.
- All NIDS/IPS policies should by default be configured to LOG and sent as a SYSLOG to the SIEM tool. Unless an IPS policy is generating excessive LOGs and through a risk assessment is observed that logging is not required then it may be removed. However, logging on IPS policies is implicitly enabled

- The Firewall should be configured in Active/Passive Cluster configuration with all interfaces being monitored for failover. Session-pick-up should be enabled for stateful-failover
- Firewall should have a dedicated in-band management
- Firewall should have a dedicated out-of-band management interface (MGMT) that is part of the OOB network
- Firewall admin authentication should be performed using Radius/TACACs+ and RBAC must be enforced
- Firewall must not have any management protocols (SSH, HTTPS) exposed on ANY interfaces except for the in-band and out-of-band management interfaces
- Firewall must be centrally integrated with NMS, NTP and other network services

5.8 Enterprise Network

5.8.1Core Module

The core module provides fast routing and switching traffic as fast from one network to another.

Key Devices

- **Layer 3 switching** – route and switch production network data from one module to another

Threats Mitigated

- Packet Sniffers – a switched infrastructure limits the effectiveness of sniffing

Design Considerations

Standard implementation guidelines should be followed in accordance with the “core, distribution, and access layer” deployments commonly

5.8.2Distribution module

The goal of this module is to provide distribution layer services that includes routing, quality of service (QoS), and access control to the building switches.

Key Devices

- **Layer 3 switches** – aggregate Layer 2 switches in building module and provide advanced services

Threats Mitigated

- Unauthorized Access – attacks against server module resources are limited by Layer 3 filtering of specific subnets
- IP Spoofing – RFC 2827 filtering stops most spoofing attempts
- Packet Sniffers – a switched infrastructure limits the effectiveness of sniffing

Design Considerations

- Depending on the size and performance requirements of the network, the distribution layer can be combined with the core layer to reduce the number of devices required in the environment
- For performance reasons, it is important that this access control be implemented on a hardware platform that can deliver filtered traffic at near wire rates. This generally dictates the use of Layer 3 switching as opposed to more traditional dedicated routing devices
- The access control should also prevent local source-address spoofing using RFC 2827 filtering.
- This module should provide subnet isolation used to route voice-over-IP (VoIP) traffic to the call manager and any associated gateways. This prevents VoIP traffic from crossing the same segments that all other data traffic crosses, reducing the likelihood of sniffing voice communications, and allows a smoother implementation of QoS

5.8.3Access Module

Key Devices

- **Layer 2 switch** – provides Layer 2 services to phones and user workstations
- **User workstation** – provides data services to authorized users on the network
- **VoIP phone** – provides IP telephony services to users on the network

Threats Mitigated

- Packet sniffers – a switched infrastructure and default VLAN services limit the effectiveness of sniffing
- Virus and Trojan horse applications – host-based virus scanning prevents most viruses and many Trojan horses

Design Considerations

- This module should provide most of the access control that is enforced at the end-user level. This is because the Layer 2 switch that the workstations and phones connect to have no capability for Layer 3 access control
- In addition to the network security hardening guidelines for the Network Switching Security, End-point security capability is implemented at the workstation level

5.8.4Server Farm Module

The server farm module's primary goal is to provide application services to end users and devices. Traffic flows on the server module are inspected by on-board intrusion detection within the Layer 3 switches.

Key Devices

- **Layer 3 Switch** – provides layer three services to the servers and inspects data crossing the server module with NIDS
- **Voice and Video Services (Call Switching) and Gateways** – performs call routing functions for IP telephony devices in the enterprise
- **Corporate and Department Servers** – delivers file, print, and DNS services to workstations in the building module
- **E-Mail Server** – provide SMTP and POP3 services to internal users
- **ICT Sub-System Services** - Messaging, Conferencing and Collaboration Services

Threats Mitigated

- Unauthorized Access – mitigated using host-based intrusion detection and access control
- Application Layer Attacks – operating systems, devices, and applications are kept up to date with the latest security fixes and protected by host-based IDS
- IP Spoofing – RFC 2827 filtering prevents source address spoofing
- Packet Sniffers – a switched infrastructure limits the effectiveness of sniffing
- Trust Exploitation – trust arrangements are very explicit, private VLANs prevent hosts on the same subnet from communicating unless necessary
- Port Redirection – host-based IDS prevent port redirection agents from being installed

Design Considerations

- Using host and network-based IDS, private VLANs, access control, and good system administration practices (such as keeping systems up to date with the latest patches), provides a much more comprehensive response to attacks
- Because the NIDS system is limited in the amount of traffic it can analyse, it is important to send it attack-sensitive traffic only. This varies from network to network, but should likely include SMTP, Telnet, FTP, and WWW.
- The switch-based NIDS was chosen because of its ability to look only at interesting traffic across all VLANs as defined by the security policy. Once properly tuned, this IDS can be set up in a restrictive manner, because required traffic streams should be well known

5.8.4.1 Edge Distribution Module

The goal of Edge Distribution Module is to aggregate the connectivity from the various elements at the edge. Traffic is filtered and routed from the edge modules and routed into the core. The edge distribution module provides the last line of defence for all traffic destined to the enterprise network module from the edge module.

Key Devices

- **Layer 3 switches** - aggregate edge connectivity and provide advanced services

Threats Mitigated

- Unauthorized Access – filtering provides granular control over specific edge subnets and their ability to reach areas within the enterprise network
- IP Spoofing – RFC 2827 filtering limits locally initiated spoof attacks
- Network Reconnaissance – filtering limits nonessential traffic from entering the campus limiting a hacker’s ability to perform network recon
- Packet Sniffers – a switched infrastructure limits the effectiveness of sniffing

Design Considerations

- The edge distribution should use access control to filter traffic, although the edge distribution module can rely somewhat on the entire edge functional area to perform additional security functions
- The edge distribution module can add additional security functions for added performance requirements and for mitigation of spoofed packets, erroneous routing updates, and provisions for network layer access control

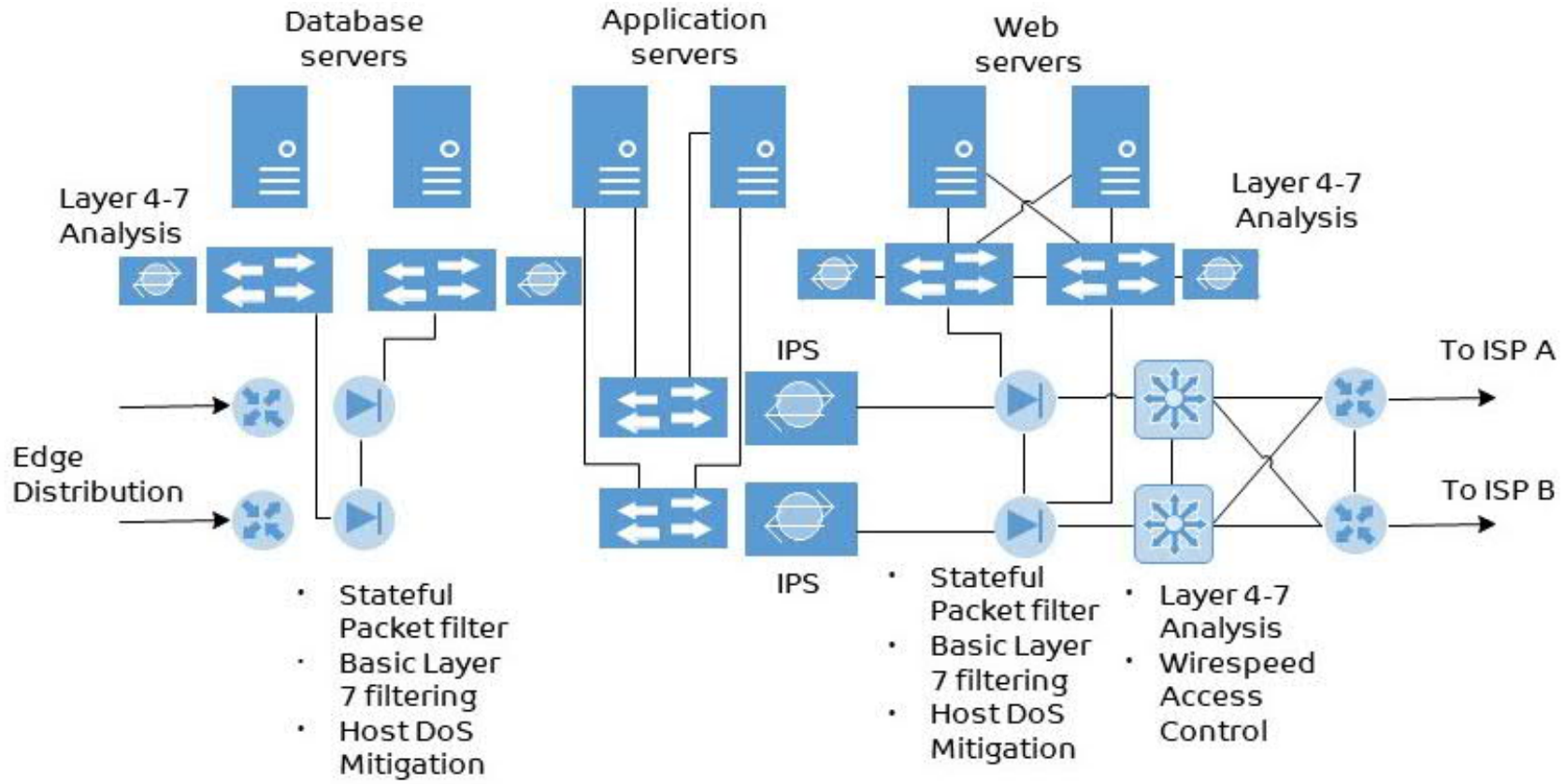
- Like the server and enterprise distribution modules, the edge distribution module can be combined with the core module if performance requirements. NIDS/IPS is not present in this module, but could be placed between the modules using IDS line cards in Layer 3 switches

5.8.5Edge Network

5.8.5.1 Ecommerce Module

Splitting the e-commerce into three components allows the architecture to provide various levels of security without impeding access.

Figure 30: E-Commerce Network



Key Devices

- Web Front server – acts as the primary presentation layer for the e-commerce applications
- Application server – hosted e-commerce applications
- Database server – acts as persistence layer the critical information that is used of the e-commerce business implementation
- Firewall – used various levels of security and segregation between different layers
- NIDS/IPS appliance – provides monitoring protection of key network segments
- Layer 3 switch with IDS module – network components which integrated security monitoring

Threats Mitigated

- Unauthorized Access – stateful firewalling and ACLs limit exposure to specific protocols
- Application Layer Attacks – attacks are mitigated using IDS and Web Application Firewall (WAF)
- Denial of Service – ISP filtering and rate-limiting reduce (D)DoS potential
- IP Spoofing – RFC 2827 and 1918 prevent locally originated spoofed packets and limit remote spoof attempts
- Packet Sniffers – a switched infrastructure and HIDS limits the effectiveness of sniffing
- Network Reconnaissance – ports are limited to only what is necessary, ICMP is restricted
- Trust Exploitation – firewalls ensure communication flows only in the proper direction on the proper service
- Port Redirection – HIDS and firewall filtering limit exposure to these attacks

Design Considerations

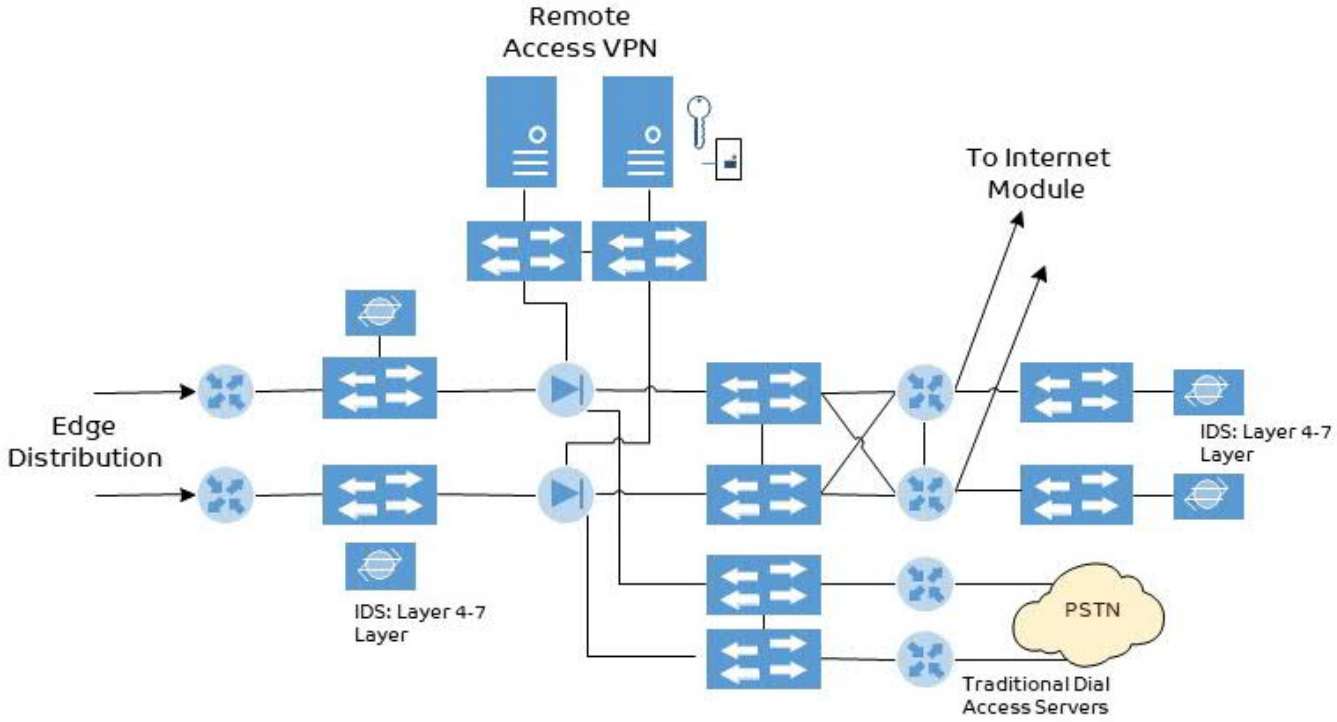
The design consideration for each of these services are addressed below:

- A network security zoning architecture must be followed as below;
  - Mapping of VM workloads (application-group-type) to security zones
  - Security Zones are to be clearly defined as part of the High-Level Design (HLD) and Low-Level Design(/LLD) that are based on security trust levels (DMZ, Internal)
- North to South traffic flow i.e. untrusted security zone such as Web server in DMZ communicating to a trusted security zone such as App server in Internal Application zone must be secured through the firewall with IPS profiles applied where applicable
- IPS profiles must be implemented on security policies (zone to zone) that are applicable.
- Security policies on the respective Firewall must be explicit in nature and be restrictive enough to allow communication flow on a need to know basis
- Gateway Anti-Virus should only be implemented where applicable (i.e. protocol that supports AV) and on the ingress traffic where it is needed - such as FTP upload and HTTP download. It is important to consider pass-through options if file-size limitation exist

5.8.5.2 VPN and Remote Access Module

This module is used for terminating VPN traffic from remote sites, and users. All the traffic forwarded to the edge distribution is from remote corporate users that are before being allowed through the firewall.

Figure 31: Network security details for VPN and Remote Access



Key Devices

- VPN Concentrator – authenticate individual remote users using Extended Authentication (XAUTH) and terminate their IPSec tunnels
- VPN Router – authenticate trusted remote sites and provide connectivity using GRE/IPSec tunnels
- Dial-In Server – authenticate individual remote users using TACACS+ and terminate their analog connections
- Firewall – provide differentiated security for the three different types of remote access
- NIDS appliance – provide Layer 4 to Layer 7 monitoring of key network segments in the module

Design Considerations

The design consideration for each of these services are addressed below:

- For Remote-Access VPN, the traffic is forwarded from the corporate Internet module access routers, where it is first filtered at the egress point to the specific IP addresses and protocols that are part of the VPN services
- Remote-access VPNs can use several different tunnelling and security protocols. Although IPSec is the tunnelling protocol of choice, many organizations choose Point-to-Point Tunnelling Protocol (PPTP) and Layer 2 Tunnelling Protocol (L2TP) because they are natively supported by popular desktop operating systems
- IPsec is chosen because the clients require minimal configuration and at the same time provide good security
- The remote-access VPN traffic will be addressed to one specific public address using the IKE (UDP 500) protocol. Because the IKE connection is not completed until the correct authentication information is provided, this provides a level of deterrence for the potential hacker
- XAUTH provides an additional user authentication mechanism before the remote user is assigned any IP parameters
- The VPN concentrator is “connected” to the access control server on the management subnet via its management interface
- Aside from an IP address and the location of name servers (DNS and WINS), MODCFG also provides authorization services to control the access of the remote user
- Users are prevented from enabling split tunnelling, thereby forcing the user to access the Internet via the corporate connection
- The IPSec parameters that uses stronger encryption algorithms
- For scalable deployment of thousands of remote users, a hardware encryption module in the VPN concentrator
- Following termination of the VPN tunnel, traffic is sent through a firewall to ensure that VPN users are appropriately filtered
- Site-to-site VPN, the VPN traffic associated with site-to-site connections with tunnels protected by an IPSec protocol in transport mode using Encapsulated Security Payload (ESP)
- A pair of NIDS appliances are positioned at the public side of the module to detect any network “reconnaissance” activity targeted at the VPN termination devices

5.8.5.3 WAN Module

Key Devices

- Router – using routing, access-control, QoS mechanisms

Threats Mitigated

- IP Spoofing – mitigated through L3 filtering
- Unauthorized Access – simple access control on the router can limit the types of protocols to which branches have access

Design Considerations

- The resilience is provided by the dual connection from the service provider, through the routers, and to the edge distribution module
- Security is provided by using router security features. Input access-lists are used to block all unwanted traffic from the remote branch
- Some organizations that are very concerned about information privacy encrypt highly confidential traffic on their WAN links using site-to-site VPNs to achieve this information privacy

5.8.5.4 Internet Module

Key Devices

- Router – using routing, access-control, QoS mechanisms

Threats Mitigated

- IP Spoofing – mitigated through L3 filtering
- Unauthorized Access – simple access control on the router can limit the types of protocols to which branches have access

Design Considerations

- The resilience is provided by the dual connection from the service provider, through the routers, and to the edge distribution module.
- Security is provided by using router security features. Input access-lists are used to block all unwanted traffic from the remote branch.
- Some organizations that are very concerned about information privacy encrypt highly confidential traffic on their WAN links using site-to-site VPNs to achieve this information privacy
- As a compensating control for a forward proxy requirement - it would be recommended to have the firewall work as an explicit proxy within the where all browsing to the internet is performed. Direct access to the internet must not be permitted. Restricted access to the internet should be enabled by locking down the relevant ports that are required for internet connectivity for business use
- In case of Next Generation firewall, it must be enabled to provide threat intelligence and dynamic groups such as malware, bad domains, rogue IPs that can be used within firewall policies
- The Firewall shall have the ability to enable on-demand GEO-IP based filtering and blocking of traffic into the network environment (i.e. block country X)
- The Firewall interfaces that connect to the Internet should have IPS DoS features enabled to protect against L3 and L4 attacks
- IPS must inspect traffic for ALL services which are exposed on the Internet. All inbound traffic from the Internet to the various other security zones must have IPS policies enabled.
- IPS policy me be implemented to prevent attacks against SSL/TLS traffic protocols, E.g.-attacks such as SSL Renegotiation Denial of Service
- IPS inspection must be performed on unencrypted traffic flow therefore ingress traffic post SSL offload on the Load balancer is the recommended approach for IPS inspection

- At minimum IPS must have policies enabled for the following attack categories- Exploit, Malware, Policy violation, Reconnaissance, DoS and DDoS, Multi Sensor correlation, Protocol discovery, Multi method Correlation, Flow correlation, Application anomaly, Volume DoS, Spoof detection
- At minimum IPS must have policies enabled for the following sub-attack categories- Arbitrary Command execution, Backdoor, Bots, Brute Force, Buffer Overflow, Code/Script Execution, Command Shell, Covert Channel, Custom Fingerprinting (Hash values), DDoS Agent Activity, DoS, Evasion Attempt, File Mismatch, OS Fingerprinting, GTI File Reputation or Vendor Intelligence feeds, Host Sweep, Malicious Flash Analysis Engine, Malware Being re-downloaded, Multi-Attack Correlation, Multi-Attack Known Bot, Multi-Attack Heuristic Bot, Non-standard Port, Over Threshold, Port Scan, Probes, Protocol Violation, Potentially Unwanted Program, Service Sweep, Shellcode Execution, Statistical Deviation, Trojan, Unauthorized IP, Malware
- Packets must be available for the malicious traffic that can be prevented/detected by IPS for Incident/alert analysis
- IPS must inspect network traffic flowing between VMs, including VM's on same host
- Static IP must be used across the infrastructure for fixed services. The use of IP addresses must be recorded in detail with the relevant asset list updated accordingly
- DDoS mitigation solution must protect the external Internet facing services from Volumetric and Application based DDoS attacks across both data centres

5.8.5.5 Wireless Network Security

Key Devices

- Wireless access switches
- Access points (AP)
- **WIDPS** - Wireless Intrusion Detection and Prevention System

Threats Mitigated

- Passive attack
  - Eavesdropping - Unauthorized device monitors WLAN data transmissions
  - Analysis - Unauthorized device gains intelligence by monitoring the transmissions for patterns of communication
- Active attack
  - Masquerading – Unauthorized device impersonates an authorized user
  - Replay - Unauthorized device monitors transmissions
  - Message modification – Unauthorized device alters legitimate messages
  - Denial of service (DoS)

Design Considerations

- The perimeter firewalls should have installed between all wireless networks and enterprise network, and are these firewalls configured to deny or accept, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the enterprise network
- The firmware on wireless devices should be updated to support strong encryption for authentication and transmission over wireless networks

- The industry leading practices should be used to implement strong encryption for authentication and transmission for wireless networks transmitting critical data or connected to the critical services
- Entity should implement processes for detection and identification of both authorized and unauthorized wireless access points and methodology detect and identify any unauthorized wireless access points
- An inventory of authorized wireless access points maintained, and a business justification documented for all authorized wireless access points.
- Wireless intrusion detection and prevention system (WIDPS) may be used for WLAN security monitoring and placed at designated locations within an organization's facilities
- Entity should do largely the same vulnerability monitoring for WLAN components identifying patches and applying them, and verifying security configuration settings and adjusting them as needed

5.8.5.6 Virtual Network Security

Key Devices

- Distributed Virtual Switches
- Software Defined Network (SDN) controllers
- Virtual IDPS – Intrusion Detection and Prevention System

Threats Mitigated

- Unauthorized Access – mitigated using virtual intrusion detection and access control
- IP Spoofing – RFC 2827 filtering prevents source address spoofing
- Packet Sniffers – a switched infrastructure limits the effectiveness of sniffing
- Trust Exploitation – trust arrangements are very explicit, private VLANs prevent hosts on the same subnet from communicating unless necessary
- Port Redirection – virtual appliance -based IDS prevents port redirection agents from being installed

Design Considerations

Network Segmentation:

- In environments using virtual switches for network segmentation, it is strongly recommended that distributed virtual switches are used instead of standalone virtual switches for the following reasons:
  - To ensure consistency of configuration across virtualized hosts and reduce chances of configuration errors, and
  - To eliminate constraints on VM migration, since a distributed virtual switch (defined for a sensitivity level) spans multiple virtualized hosts
- Isolation of the hypervisor's management network using virtual switches needs special configuration. In addition to dedicated virtual switches, the management traffic pathway should have separate physical Network Interface Controllers (pNICs) and separate physical network connections (besides the traffic itself being encrypted)
- Also, it is preferable that the dedicated virtual switch is a standalone virtual switch (so that it can be configured at the virtualized host level) instead of a distributed virtual switch. This is due to the close dependency between distributed virtual switches and the centralized virtualization management servers

- Distributed virtual switches can only be configured using a virtualization management server (requiring high availability for these servers), and in some situations bringing up a virtualization management server may require distributed virtual switch modification
- In all VLAN deployments, the switch (physical switch connecting to virtualized host) port configuration should be VLAN aware – i.e., its configuration should reflect the VLAN profile of the connected virtualized host
- Large data centre networks with hundreds of virtualized hosts and thousands of VMs and requiring many segments should deploy overlay-based virtual networking because of scalability (Large Namespace) and virtual/physical network independence.
- It is highly advisable that the overall traffic generated by overlay-based network segmentation technique (e.g., VXLAN network traffic) is isolated on the physical network using a technique such as VLAN to maintain segmentation guarantees
- Large overlay-based virtual networking deployments should always include either centralized or federated SDN controllers using standard protocols for configuration of overlay modules in various hypervisor platforms

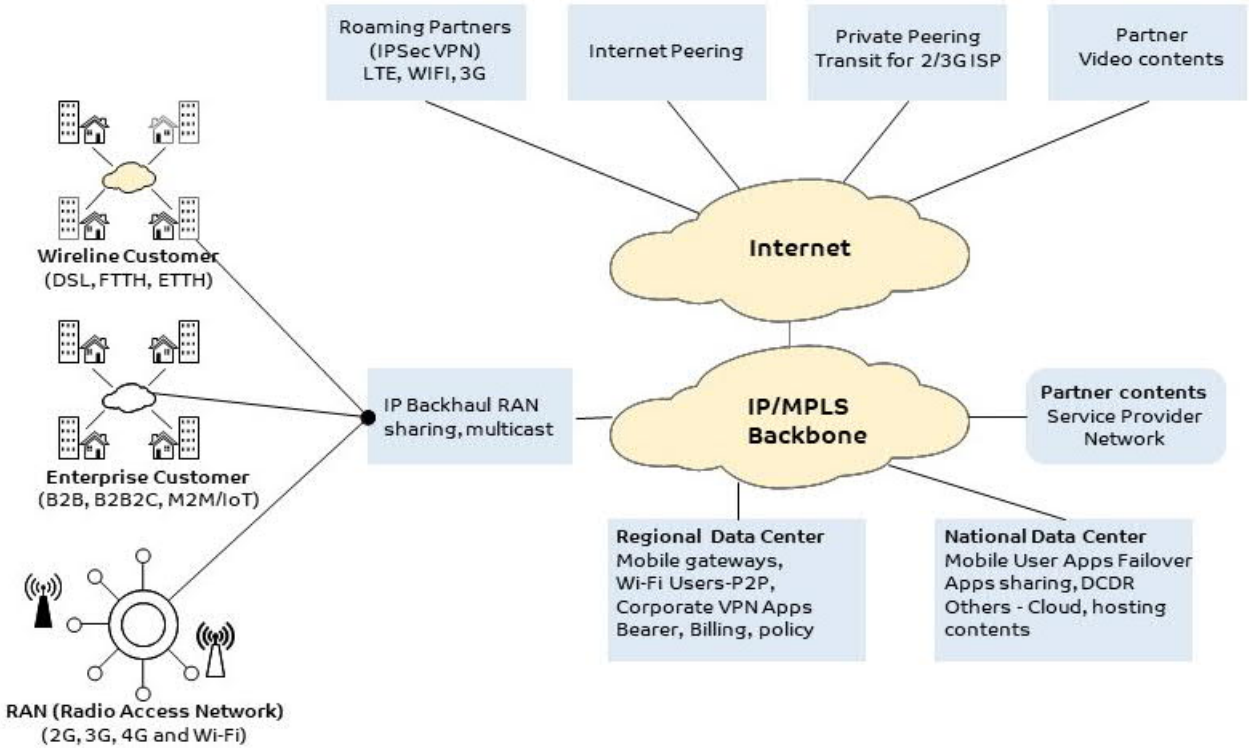
Network Path Redundancy:

- It is preferable to use pNICs that use different drivers in the NIC team. The failure of one driver will only affect one member of the NIC team, and traffic will keep flowing through the other members
- If multiple PCI buses are available in the virtualized host, each pNIC in the NIC team should be placed on a separate PCI bus. This provides fault tolerance against PCI bus failure in the virtualized host
- The network path redundancy created within the virtual network of the virtualized host should also be extended to the immediate physical network links emanating from the virtualized host. This can be achieved by having the individual members of the NIC team (i.e., the two or more pNICs) connected to different physical switches
- In virtualized environments with VMs running delay-sensitive applications, virtual firewalls should be deployed for traffic flow control instead of physical firewalls, because in the latter case, there is latency involved in routing the virtual network traffic outside the virtualized host and back into the virtual network
- In virtualized environments with VMs running I/O intensive applications, kernel-based virtual firewalls should be deployed instead of subnet-level virtual firewalls, since kernel-based virtual firewalls perform packet processing in the kernel of the hypervisor at native hardware speeds
- For both subnet-level and kernel-based virtual firewalls, it is preferable if the firewall is integrated with a virtualization management platform rather than being accessible only through a standalone console. The former will enable easier provisioning of uniform firewall rules to multiple firewall instances, thus reducing the chances of configuration errors
- For both subnet-level and kernel-based virtual firewalls, it is preferable that the firewall supports rules using higher-level components or abstractions (e.g., security group) in addition to the basic 5-tuple (source/destination IP address, source/destination ports, protocol)

5.8.6Telecommunication Network Security

Telecommunication networks have evolved from circuit switching voice to digital voice, and now routinely include data services and streaming digital video, all delivered to the mobile device or user equipment over a common IP network core, as shown in ***Figure 32: Common Telecommunication Network Architecture***

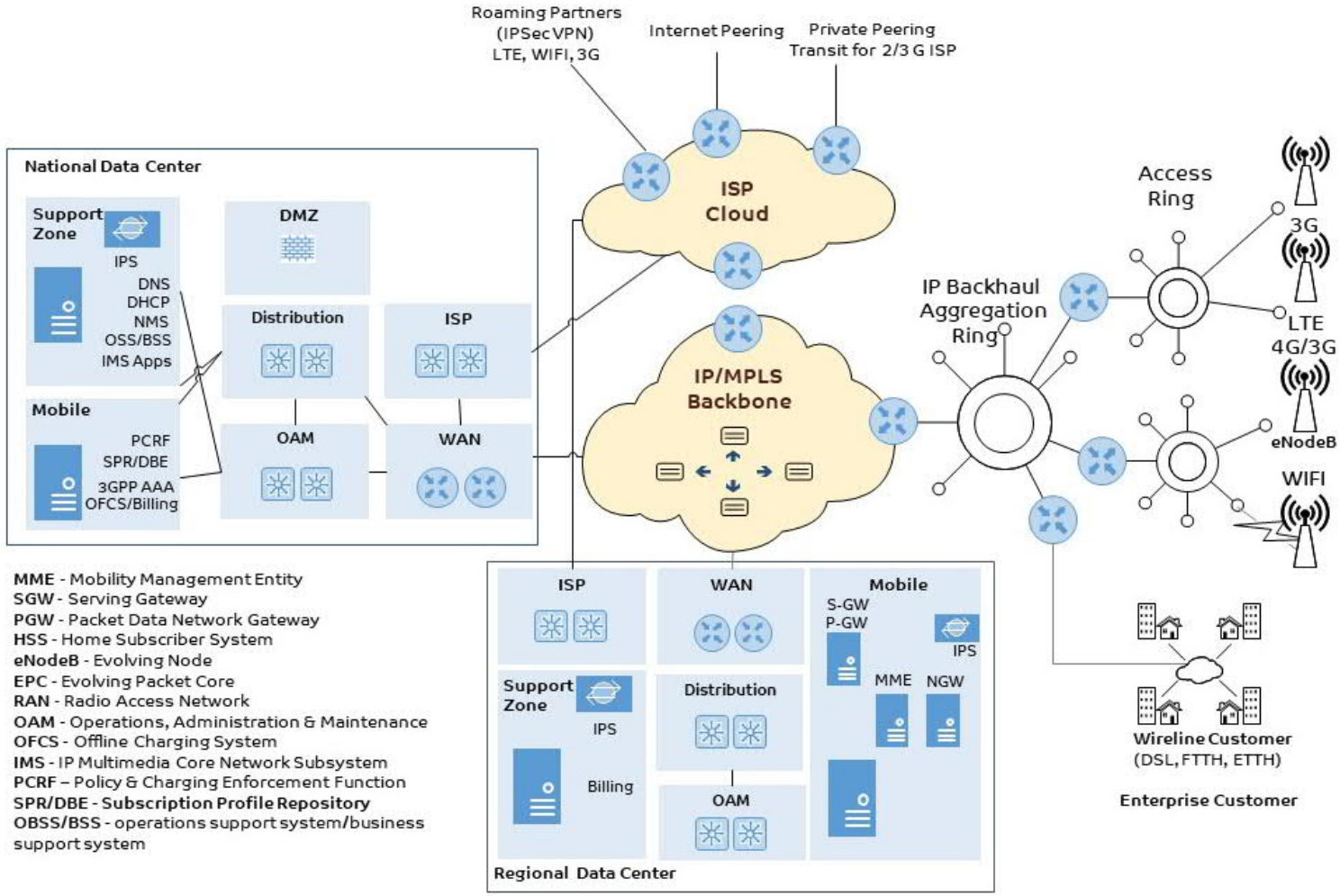
Figure 32: Common Telecommunication Network Architecture



Although not part of 4G or the Long-Term Evolution (LTE) of mobile networks, some components for the 3G mobile architecture and the 3G packet gateway, or gateway GPRS support node (GGSN), is necessary. This is because the Packet Data Network Gateway (P-GW) in the LTE architecture is still expected to internetwork and interoperate with 3G architectures and devices.

Figure 33: Telecommunication Network Security shows overall telecommunication network zones to support multiple services on the same backbone infrastructure. Trusted network elements are typically located within a cable operator's managed backbone network. Untrusted network elements, such as the Roaming Partners, Internet Peering are typically located outside the telecommunication operator's network.

Figure 33: Telecommunication Network Security



The security requirements for the secure environment are provided by 3GPP security specifications:

- TS 33.102 UMTS security specification
- TS 33.401 EPS security specification

- TS 33.210 Network Domain Security
- TS 33.203 IMS security
- TS 33.220 Generic Bootstrapping architecture

Key Tools

- LTE users (AAA and PCRF), Routing Authentication
- Monitor PCEF/PCRF, IPS, Probes, NetFlow, NBAR, Topology Map, DOS, DDOS
- Security Operations Centre (collect, correlate security incidents and alerts)
- Control Plane Policing, NTP, syslog, config mgmt.

5.8.6.1 IP Blackhaul Security

- KEv2/IPsec with integrity and confidentiality protection mandatory for all traffic (control/user/management plane)
- In case S1 and X2 user plane interfaces are trusted (e.g. physically protected), the use of IPsec/IKEv2 based protection is not needed [3GPP TS 33.401 V11.2.0 (2011-12)] and this holds also for control and management traffic
- Profiling of IKEv2/IPsec specified; IKEv2 based on certificates eNB comes equipped with id, private/public key pair, manufacturer certificate, can be integrated into the operator PKI via certificate enrolment

5.8.6.2 Network Domain Security IP Core

Threats

- Mobile to Mobile Spewing Attacks
- DOS Attacks in downlink direction from Internet
- TCP based attacks from Internet (Syn, session hijack, resource exhaustion etc.)
- UDP Based attacks like Smurf attack.
- ICMP Attacks like ping of death. Fragmentation attacks.
- Layer 4 protocol anomalies attacks
- Malware/Spyware prevention

Design Considerations

- IKE/IPsec profiles specified similar as for backhaul link (IKEv2 or v1, peer authentication based on certificates, IPsec ESP in tunnel mode)

- IPsec mandatory to use for integrity protection of control traffic between “security domains”
  - Traffic between serving network and home network when roaming in specific cases, also encryption is mandatory
- Mandatory encryption for interface between:
  - Core and 3G radio network controller, if they are in different security domains protects 3G radio interface keys sent to the controller
  - MME in serving network and HSS in home network
- Security Gateways (SEGs) to be used at security domain borders terminate IKE/IPsec
  - Rogue MME connecting to HSS or PCRF
  - HSS, PCRF protections against DOS/DDOS attacks
  - Database must be protected against protocol anomalies attacks like SQL Slammer worm or resource consumption attacks
  - CDR protection against manipulation by both internal and external attackers

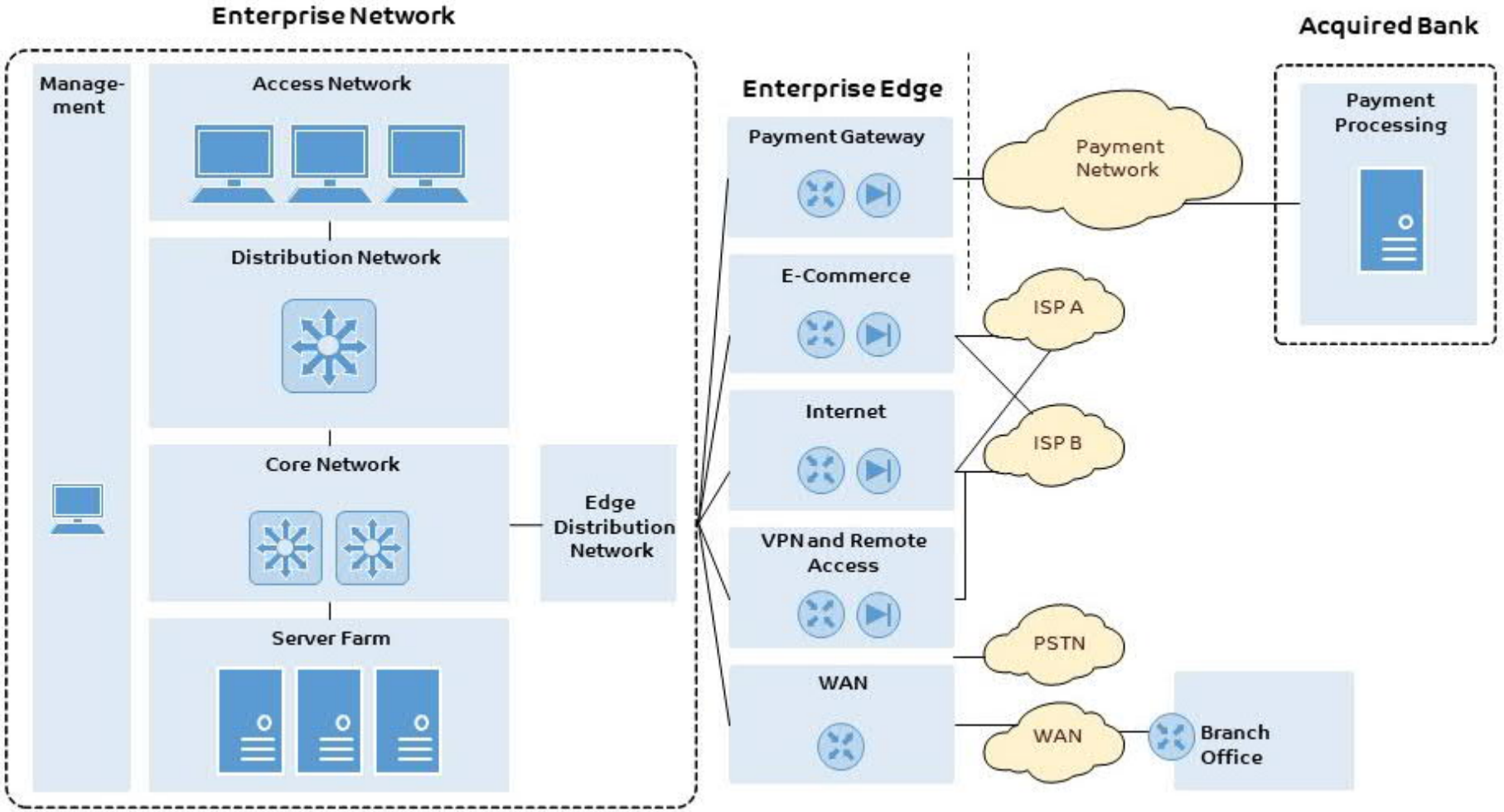
5.8.6.3 Payment Network Security

The diagram shows the configuration for enterprise network of which have three POS terminals and the other on-line payment. It also shows a centralized payment gateway and an application server to back-office systems, though these are integration add-ons and not part of the out-of-the-box solution

Some POS functions, such as payments by credit or debit card, are processed through a common Payment Gateway that can connect to a payment processor. The payment gateway converts the message from XML to ISO 8583 or a variant message format (format understood by EFT Switches) and then forwards the transaction information to the payment processor used by the merchant's acquiring bank

Thus, the payment processor forwards the transaction to the card association (I.e.: Visa/MasterCard/American Express) which routes the transaction to the issuer bank

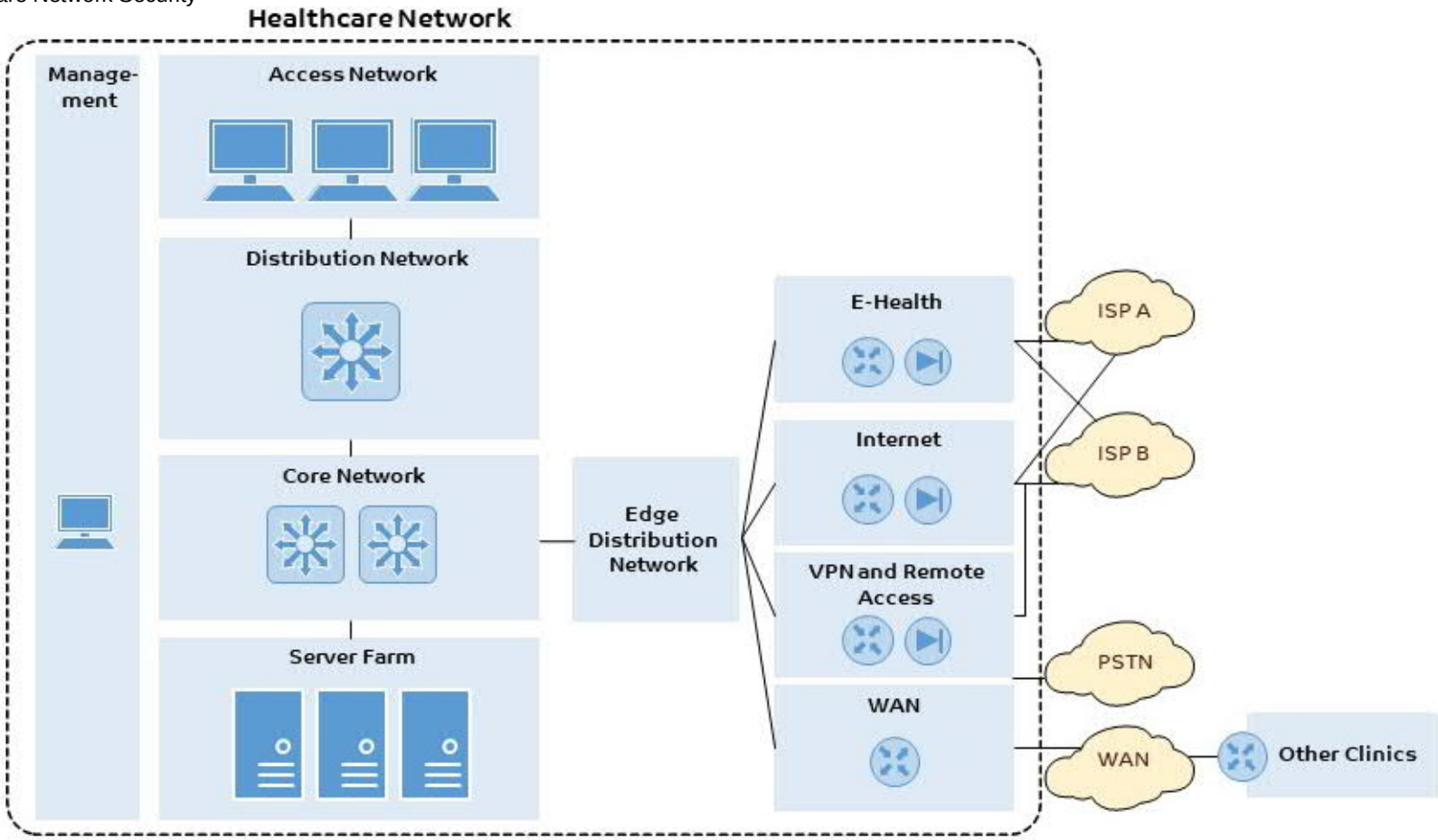
Figure 34: Payment Network Security



5.8.7 Healthcare Network Security

Entities providing healthcare services need to make sure that their enterprise network infrastructure consider the network security practices, services, and products that can mitigate the inherent risks associated with protecting healthcare data.

Figure 35: Healthcare Network Security



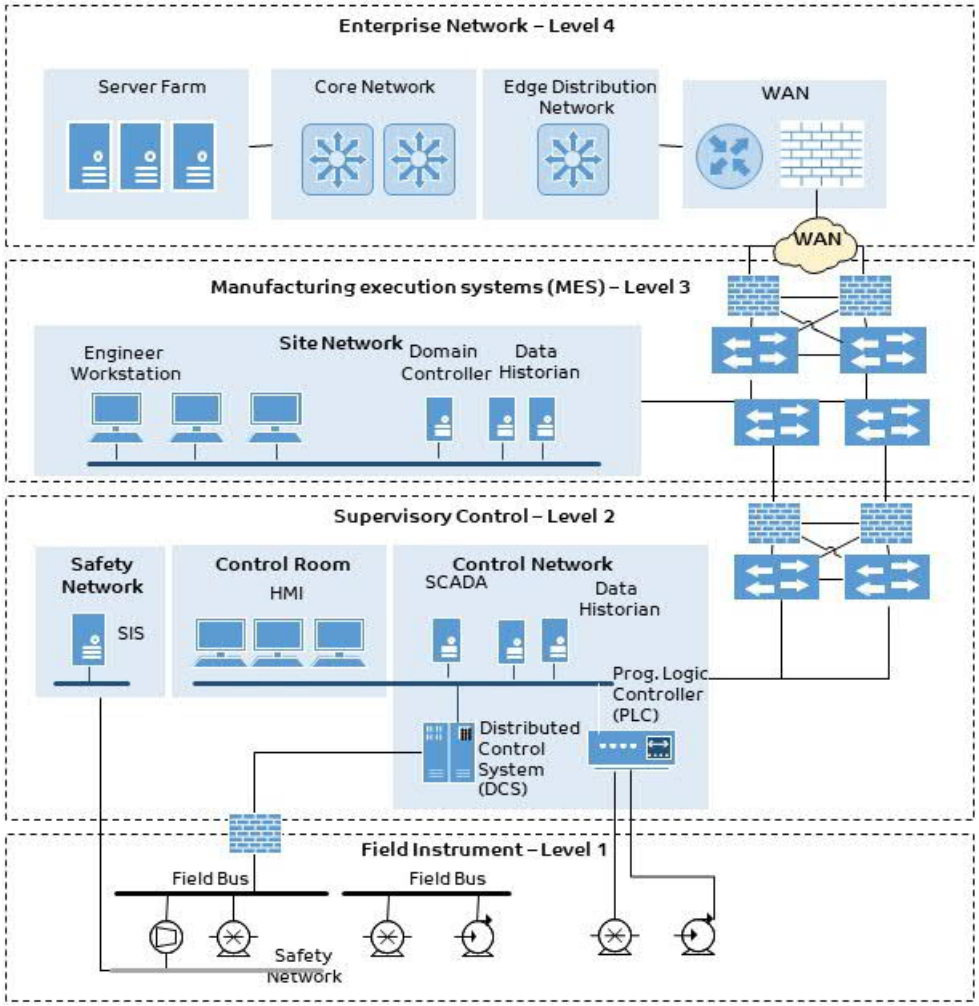
- An effective Network security must continually evolve and change to defend against new threats and to accommodate changing business requirements
- All aspects of the network, including applications, desktops, laptops, and servers, and network devices (routers, switches, wireless access points, and appliances) must play a part in protecting the organization from internal and external threats
- Security must be integrated into the operations of the network and into the devices on the network. This integrated approach is the foundation of a self-defending network

- A successful security solution requires comprehensive, integrated safeguards throughout the network infrastructure—not just a few specialized security devices
- Security solutions should be modular to keep costs down and ensure scalability and flexibility
- A layered, in-depth defence strategy provides more complete protection and minimizes areas of potential vulnerability
- Security should be integral to the overall architecture from the beginning—not considered later or as a separate component

5.8.8 Industrial Control System (ICS) Network Security

Industrial Control System (ICS) network topologies vary among implementations (i.e., Energy or Utility sectors). The various topologies used, including point-to-point, series, series-star, and multi-drop.

Figure 36: DCS Implementations



Distributed Control Systems (DCS) are used to control production systems within the same geographic location for oil refineries, water and wastewater treatment, electric power generation plants, chemical manufacturing plants, automotive production, and pharmaceutical processing facilities.

The concept of protection by zones and conduits is illustrated in*Error! Reference source not found.* for a typical plant environment. The methods are described ISA/IEC-62443, “Network and system security for industrial-process measurement and control.”

Design Considerations

From *Error! Reference source not found.*, we can see that the enterprise or enterprise system zone (Level 4) is connected to the plant computer network system (called the plant DMZ, Level 3), which is usually a general-purpose computer network, and is typically connected through a stateful-type IT firewall to the enterprise system.

The plant DMZ (Level 3) is connected to the ICS (Level 2) typically through a specialized firewall or security appliance (a term used by some manufacturers to differentiate their product), which is later connected to the Safety Instrumented Systems SIS (Level 2), again through a specialized firewall or security appliance. If the ICS is large enough or has separate functional areas (e.g. PLCs or process areas), there may be more defined zones with specialized firewall or security appliances

It's typical to have a stateful firewall at the central control centre connection to the enterprise network. A specialized firewall or security appliance should be in place between the central control centre and distributed control locations (typically RTU sites), and a specialized firewall or security appliance firewall at each control location

Firewalls are required at both ends because of the geographical distribution; a cyber-threat attack may backdoor into the control centre from one of the control locations. Depending on the design, there may or may not be separate SIS zones.

Whitelisting should be used rather than blacklisting and should follow the rule that if a system or user doesn’t need to communicate with a system, it should not be allowed. Blanket access should not be allowed

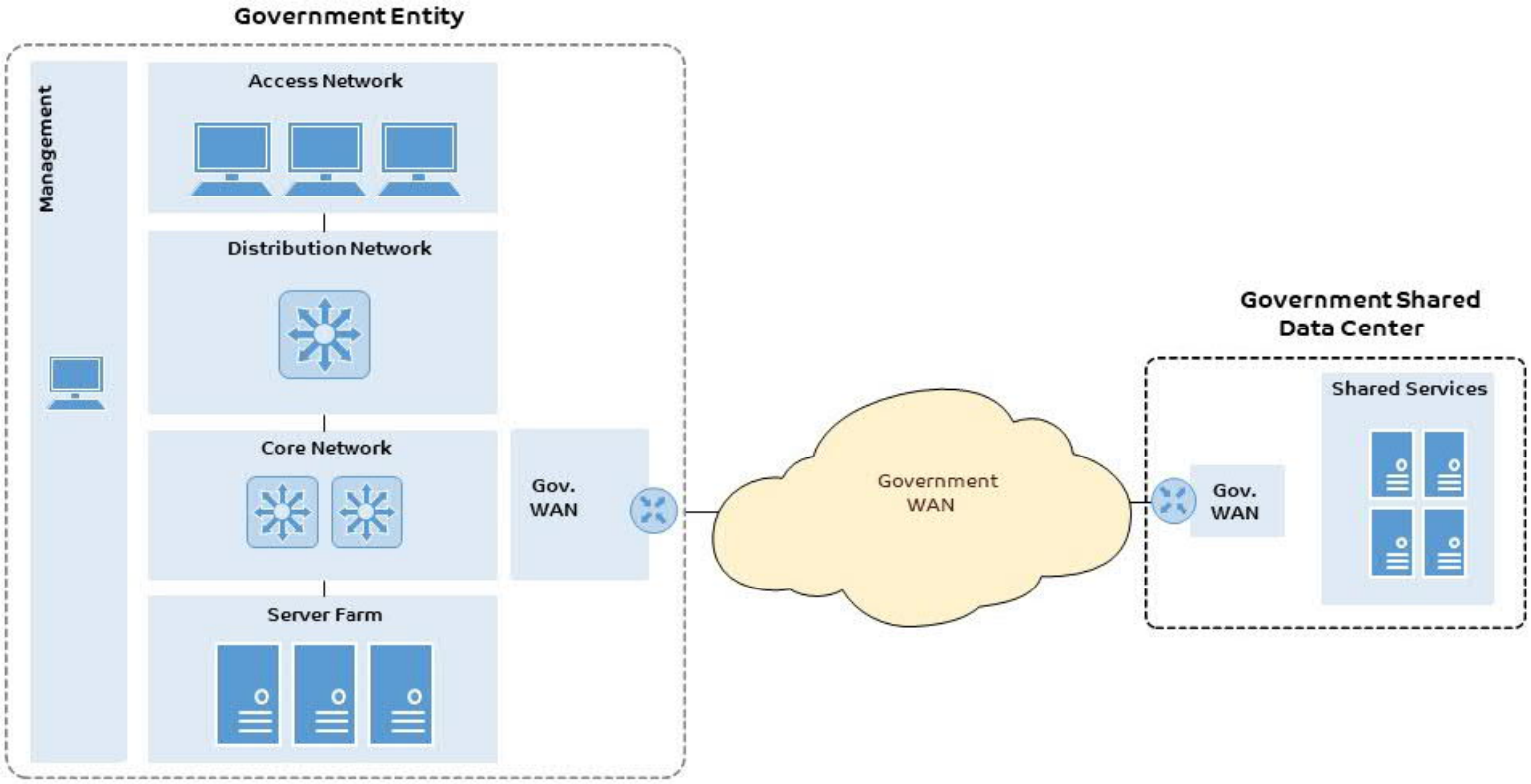
The read-only transactions should limit your risk from a cyber-threat to vulnerabilities of the firewall. This can be done with a data diode (unidirectional data flow) or a firewall with deep packet inspection (DPI) that only allows reads. Level 1 is where the field instruments interface with the process and do the actual work

Level 1 is where the field instruments interface with the actuators and sensors. These are connected to PLC in Level 2 via analog or discrete digital signals which does not require firewall. But an increasing number use fieldbus or some other field network must be protected by dedicated firewall.

5.8.9Government Network Security

Government my implement a secure wide area network (WAN) that allows officials at local public-sector organizations to interact and share data privately and securely with central government departments.

Figure 37: Government WAN and Shared Data Centre



Above figure illustrates a Government WAN providing a network which create a VPN or provision a circuit-based link through its network for a sub-entity. In doing so, it secured the sub-entity's traffic from everyone else's traffic. However, the entity can implement IPSec to further encrypt network traffic.

Routers can combine security and network functions in a single device, independently delivering VPN, stateful firewall, intrusion protection, and URL filtering in addition to full-featured IP routing.

Depending on budget constraints, traffic load, security requirements, and service load, this may or may.

5.9 Type of tools or software that should be deployed for Network Security:

Following table, define features of security devices, tools, which will help establish secure network architecture model

Table 26: Network Security Tools

Type of Tool	Features Required from security monitoring perspective
Application Proxy Firewall	• Leverage basic network stack functionality to sanitize application level traffic • Block java or active X • Filter out “bad” URLs • Ensure well-formed protocols or block suspect aspects of protocol
Packet Filter Firewall	• Operates at Layer 3 in router or HW firewall • Has access to the Layer 3 header and Layer 4 header • Can block traffic based on source and destination address, ports, and protocol
Stateful Packet Filters	• Evolved as packet filters aimed for proxy functionality • In addition to Layer 3 reassembly, it can reconstruct layer 4 traffic • Some application layer analysis exists, e.g., for HTTP, FTP, H.323 • Called context-based access control (CBAC) • Some of this analysis is necessary to enable address translation and dynamic access for negotiated data channels • Reconstruction and analysis can be expensive • Must be configured on specified traffic streams • At a minimum the user must tell the Firewall what kind of traffic to expect on a port • Degree of reconstruction varies per platform, e.g. IOS does not do IP reassembly
Identity Aware Firewall	• Use TACACS+ or Radius to authenticate, authorize, account for user with respect to FW - For administration of FW - For traffic passing through FW • Authorization for executing commands on the device • Download or enable ACL’s • Extended Authentication (XAuth) to integrate AAA with VPN authentication and other security mechanisms, thus is forcing remote users to respond with their credentials before being allowed access to the VPN
NIDS	• Detection can be viewed in two parts - Anomaly detection: Use statistical techniques to determine unusual behaviour - Misuse detection: Use signatures to determine occurrence of known attacks • Detection can be performed on host data (HIDS), network data (NIDS), or a hybrid of both
Intrusion Protection Systems (IPS)	• Inline NIDS

Type of Tool	Features Required from security monitoring perspective

	• Requires very fast signature handling
	  - Slow signature handling will not only miss attacks, but it will also cause the delay of valid traffic
	  - Specialized hardware required for high volume gateways
	• When IDS is inline, the intrusion detector can take direct steps to remediate.

Honey Pots	• Reconnaissance protection and attention diversion
	• Deploy a fake system
	  - Observe it being attacked
	• Resource management
	  - Cannot be completely passive
	  - Must provide enough information to keep attacker interested
	• Scale
	  - Host, network, dark address space

Data Sources (Traffic Monitoring)	• Direct data
	  - Network packets
	  - System calls
	• Indirect data
	  - Syslog data, Windows event logs
	  - Events from other intrusion detection systems
	  - NetFlow information generated by routers about network traffic

Next Generation Firewalls (NGFW)	• In addition to the Stateful inspection functions of a firewall, NGFW are application aware firewalls and provide better application visibility and control
Unified Threat Management	• Provision to have the functions of Network firewall and Intrusion Detection/Prevention, and some other features such as content filter, web caching as one solution
Industrial firewalls Management system (For OT Systems)	• Provision to export log data to the central logging server • Provision to export specific duration of logs
Network access control	• Provision to enforce security policy by granting access to only those resource (devices) that are approved as per the security policy • Provides authentication and authorization to allow specific data to specific users by identifying a user, the device used to access the network and the role defined on the network
SIEM	• A centralized log aggregator and correlation engine • Capable of collecting SNMP and security event logs from Network based services and appliances • Should support syslog log format • Provision to export specific duration of log data

Type of Tool	Features Required from security monitoring perspective
Access Control Lists (ACLs)	• Used to define traffic streams - Bind ACL's to interface and action • Access Control Entry (ACE) contains - Source address - Destination Address - Protocol, e.g., IP, TCP, UDP, ICMP, GRE - Source Port - Destination Port • ACL runtime lookup - Linear - N-dimensional tree lookup (PIX Turbo ACL) - Object Groups - HW classification assists
Ingress and Egress Filtering Intermediate Firewall/Router	• Ingress filtering - Filter out packets from invalid addresses before entering your network • Egress filtering - Filter out packets from invalid addresses before leaving your network • Limit number of half open connections

5.10 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards

Table 27: Network Configuration Management activities mapping industry information security standards – Part I of II

Service Name — Network Configuration Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference - CSC**	**Controls Reference - ISA 62443-2-1:2009**	**Controls Reference - ISA 62443-3-3:2013**
Prepare	Network infrastructure devices within the organization are inventoried	NS 1 NS 4		1	4.2.3.4	SR 7.8
Prepare	Organizational communication and data flows within the system and between interconnected systems are mapped	NS 4		12	4.2.3.4	
Implement	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	NS 1 NS 3 NS 5		3 9 11	4.3.4.3.2 4.3.4.3.3	SR 7.6
Implement	Network integrity is protected (e.g., network segregation, network segmentation)	NS 7 NS 8 NS 9 NS 10 GS 1 GS 2 GS 6 GS 7		9 14 15 18	4.3.3.4	SR 3.1 SR 3.8
Implement	Configuration change control processes are in place	CM 1 CM 4 CM 5 CM 6		3 11	4.3.4.3.2 4.3.4.3.3	SR 7.6
Implement	Communications and control networks are protected	NS 4 NS 5 NS 6		8 12 15		SR 3.1 SR 3.5 SR 3.8 SR 4.1 SR 4.3 SR 5.1 SR 5.2 SR 5.3

Service Name — Network Configuration Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference - CSC**	**Controls Reference - ISA 62443-2-1:2009**	**Controls Reference - ISA 62443-3-3:2013**
						SR 7.1 SR 7.6
Implement	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations				4.3.2.5.2	SR 7.1 SR 7.2
Maintain	A baseline of network operations and expected data flows for users and systems is established and managed	NS 3 NS 25 NS 27		1 4 6 12 13 15 16	4.4.3.3	
Maintain	Vulnerability scans are performed in collaboration with Security Monitoring and Operations (refer Security Monitoring and Operations capability chapter)			4, 20	4.2.3.1 4.2.3.7	
Review	Management and dashboard reporting of identified network configuration deviations.	SM 7 SM 8		19	4.3.4.5.2	
Review	Event detection information is communicated to appropriate parties * In case of Alert, Network Security Team will execute response actions * In case of Incident/Breach, Incident Response Team will execute response actions					

Table 28: Network Configuration Management activities mapping industry information security standards – Part II of II

Service Name - Network Configuration Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference - NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference -HIPAA**	**Controls Reference - Cloud Security Alliance (CCM v3.0.1)**	**Controls Reference - Controls Reference - GDPR**
Prepare	Network infrastructure devices within the organization are inventoried	A.8.1.1 A.8.1.2	CM-8 PM-5	1.1.1 1.1.4 1.1.6 1.1.7			
Prepare	Organizational communication and data flows within the system and between interconnected systems are mapped	A.13.2.1 A.13.2.2	AC-4 CA-3 CA-9 PL-8	1.1.2 1.1.3			
Implement	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4	CM-2 CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 SA-10	1.1.6 1.1.7 2.2			

Service Name - Network Configuration Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference - NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference -HIPAA**	**Controls Reference - Cloud Security Alliance (CCM v3.0.1)**	**Controls Reference - Controls Reference - GDPR**
Implement	Network integrity is protected (e.g., network segregation, network segmentation)	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3	AC-4 AC-10 SC-7	1.1.1 1.1.2 1.1.3 1.1.4 1.1.6 1.1.7 1.2.1 1.2.2 1.2.3			
Implement	Configuration change control processes are in place	A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4	CM-3 CM-4 SA-10	6.4.5 6.4.6			
Implement	Communications and control networks are protected	A.13.1.1 A.13.2.1 A.14.1.3	AC-4 AC-17 AC-18 CP-8 SC-7 SC-19 SC-20 SC-21 SC-22 SC-23 SC-24 SC-25	1.2 1.2.1 1.2.2			

Service Name - Network Configuration Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference - NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference -HIPAA**	**Controls Reference - Cloud Security Alliance (CCM v3.0.1)**	**Controls Reference - Controls Reference - GDPR**
			SC-29 SC-32 SC-36 SC-37 SC-38 SC-39 SC-40 SC-41 SC-43				
Implement	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	A.17.1.2 A.17.2.1	CP-7 CP-8 CP-11 CP-13 PL-8 SA-14 SC-6				
Maintain	A baseline of network operations and expected data flows for users and systems is established and managed	A.12.1.1 A.12.1.2 A.13.1.1 A.13.1.2	AC-4 CA-3 CM-2 SI-4	1.1.2 1.1.3			
Maintain	Vulnerability scans are performed in collaboration with Security Monitoring and Operations (refer Security Monitoring and Operations capability chapter)	A.12.6.1	RA-5				
Review	Management and dashboard reporting of identified network configuration deviations.	A.16.1.2 Clause 7.4 Clause 16.1.2	CA-2 CA-7 CP-2	10.6			

Service Name - Network Configuration Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference - NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference -HIPAA**	**Controls Reference - Cloud Security Alliance (CCM v3.0.1)**	**Controls Reference - Controls Reference - GDPR**
			IR-4 IR-8 PE-6 RA-5 SI-4				
Review	Event detection information is communicated to appropriate parties * In case of Alert, Network Security Team will execute response actions * In case of Incident/Breach, Incident Response Team will execute response actions						

Table 29: Network Access Control Management activities mapping industry information security standards – Part I of II

Service Name - Network Access Control Management						
Process Phases	**Activities/Controls**	**Controls Reference - NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
IDENTFY	Physical devices and systems within the organization are inventoried	NS 1 NS 4		1	4.2.3.4	SR 7.8
IDENTFY	Organizational communication and data flows within the system and between interconnected systems are mapped	NS 4		12	4.2.3.4	
IDENTFY	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	IG, TM		17 19	4.3.2.3.3	
PROTECT	Physical and network access to assets is managed and protected	CS 2 CS 3 CS 4 PH 1 PH 2 PH 3 PH 5 PH 7			4.3.3.3.2 4.3.3.3.8 4.3.3.3.2 4.3.3.3.8	
PROTECT	Remote access of users and devices are managed	AM 35 AM 36 AM 37 AM 38 AM 39 AM 40 AM 41		12	4.3.3.6.6	SR 1.13 SR 2.6
PROTECT	Network integrity is protected (e.g., network segregation, network segmentation)	NS 7 NS 8 NS 9 NS 10		9 14 15 18	4.3.3.4	SR 3.1 SR 3.8

Service Name - Network Access Control Management						
Process Phases	**Activities/Controls**	**Controls Reference - NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		GS 1 GS 2 GS 6 GS 7				
PROTECT	Data-at-rest is protected	CY 1 CY 2 CY 3 CY 4 CY 6 CY 7 CY 8 CY 9 CY 10 CY 11 CY 12		13, 14		SR 3.4 SR 4.1
PROTECT	Data-in-transit is protected	CY 1 CY 2 CY 3 CY 4 CY 5 CY 9 CY 10 CY 11 CY 12 NS 34 NS 38		13 14		SR 3.1 SR 3.8 SR 4.1 SR 4.2

Service Name - Network Access Control Management						
Process Phases	**Activities/Controls**	**Controls Reference - NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		NS 60 NS 61				
PROTECT	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	AM 35 AM 36 AM 37 AM 38 AM 39 AM 40 AM 41 MS 15 MS 16		3 5	4.3.3.6.5 4.3.3.6.6 4.3.3.6.7 4.3.3.6.8	
PROTECT	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)			1 12 15 16	4.3.3.6.1 4.3.3.6.2 4.3.3.6.3 4.3.3.6.4 4.3.3.6.5 4.3.3.6.6 4.3.3.6.7 4.3.3.6.8 4.3.3.6.9	SR 1.1 SR 1.2 SR 1.5 SR 1.7 SR 1.8 SR 1.9 SR 1.10
PROTECT	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties			3 5 12 14 15	4.3.3.7.3	SR 2.1

Service Name - Network Access Control Management						
Process Phases	**Activities/Controls**	**Controls Reference - NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
				16 18		
PROTECT	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations				4.3.2.5.2	SR 7.1 SR 7.2
MAINTAIN	A baseline of network operations and expected data flows for users and systems is established and managed	NS 3 NS 25 NS 27		1 4 6 12 13 15 16	4.4.3.3	
MAINTAIN	Vulnerability scans are performed in collaboration with team responsible for Security Monitoring and Operations			4 20	4.2.3.1 4.2.3.7	
REVIEW	Management and dashboard reporting of identified access control deviations.	SM 7 SM 8		19	4.3.4.5.2	
REVIEW	Event detection information is communicated to appropriate parties * In case of Alert, Network Security Team will execute response actions * In case of Incident/Breach, Incident Response Team will execute response actions					

Table 30: Network Access Control Management activities mapping industry information security standards – Part II of II

Service Name - Network Access Control Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference - PCI DSS 3.2**	**Controls Reference - HIPAA**	**Controls Reference — Cloud Security Alliance (CCM v3.0.1)**	**Controls Reference — Controls Reference - GDPR**
IDENTFY	Physical devices and systems within the organization are inventoried	A.8.1.1 A.8.1.2	CM-8 PM-5	1.1.1 1.1.4 1.1.6 1.1.7			
IDENTFY	Organizational communication and data flows within the system and between interconnected systems are mapped	A.13.2.1 A.13.2.2	AC-4 CA-3 CA-9 PL-8	1.1.2 1.1.3			
IDENTFY	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	A.6.1.1	CP-2 PS-7 PM-11	8.1 8.1.1 8.1.2 8.1.3 8.1.4 8.4 8.5 8.6 8.8			
PROTECT	Physical and network access to assets is managed and protected	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3	PE-2 PE-3 PE-4 PE-5 PE-6 PE-8	1.1.1 1.1.4 1.1.6 1.1.7			

Service Name - Network Access Control Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference - PCI DSS 3.2**	**Controls Reference - HIPAA**	**Controls Reference — Cloud Security Alliance (CCM v3.0.1)**	**Controls Reference — Controls Reference - GDPR**
		A.11.2.5 A.11.2.6 A.11.2.7 A.11.2.8					
PROTECT	Remote access of users and devices are managed	A.6.2.1 A.6.2.2 A.11.2.6 A.13.1.1 A.13.2.1	AC-1 AC-17 AC-19 AC-20 SC-15	8.3.1 8.3.2			
PROTECT	Network integrity is protected (e.g., network segregation, network segmentation)	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3	AC-4 AC-10 SC-7	1.1.1 1.1.2 1.1.3 1.1.4 1.1.6 1.1.7 1.2.1 1.2.2 1.2.3			
PROTECT	Data-at-rest is protected	A.8.2.3	MP-8 SC-12 SC-28	4.1 4.3			
PROTECT	Data-in-transit is protected	A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3	SC-8 SC-11 SC-12	4.1 4.3			

Service Name - Network Access Control Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference - PCI DSS 3.2**	**Controls Reference - HIPAA**	**Controls Reference — Cloud Security Alliance (CCM v3.0.1)**	**Controls Reference — Controls Reference - GDPR**
PROTECT	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	A.11.2.4 A.15.1.1 A.15.2.1	MA-4				
PROTECT	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	A.7.1.1, A.9.2.1	AC-1 AC-2 AC-3 AC-16 AC-19 AC-24 IA-1 IA-2 IA-4 IA-5 IA-8 PE-2 PS-3				
PROTECT	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	A.6.1.2 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5	AC-1 AC-2 AC-3 AC-5 AC-6 AC-14 AC-16 AC-24	6.4.2 7.1 7.2	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii)		
PROTECT	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	A.17.1.2 A.17.2.1	CP-7 CP-8, CP-11 CP-13				

Service Name - Network Access Control Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference - PCI DSS 3.2**	**Controls Reference - HIPAA**	**Controls Reference — Cloud Security Alliance (CCM v3.0.1)**	**Controls Reference — Controls Reference - GDPR**
			PL-8 SA-14 SC-6				
MAINTAIN	A baseline of network operations and expected data flows for users and systems is established and managed	A.12.1.1 A.12.1.2 A.13.1.1 A.13.1.2	AC-4 CA-3 CM-2 SI-4	1.1.2 1.1.3			
MAINTAIN	Vulnerability scans are performed in collaboration with team responsible for Security Monitoring and Operations	A.12.6.1	RA-5				
REVIEW	Management and dashboard reporting of identified access control deviations.	A.16.1.2, Clause 7.4 Clause 16.1.2	CA-2 CA-7 CP-2 IR-4 IR-8 PE-6 RA-5 SI-4	10.6			
REVIEW	Event detection information is communicated to appropriate parties * In case of Alert, Network Security Team will execute response actions * In case of Incident/Breach, Incident Response Team will execute response actions						

Table 31: Network Monitoring Management activities mapping industry information security standards – Part I of II

Service Name - Network Monitoring Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference - ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identify	Physical devices and systems within the organization are inventoried	NS 1 NS 4		1	4.2.3.4	SR 7.8
Identify	Organizational communication and data flows within the system and between interconnected systems are mapped	NS .4		12	4.2.3.4	
Identify	External network systems are catalogued	NS 1 NS 4		12		
Identify	Adequate capacity to ensure availability is maintained	SM 1 SM 2 SM 3 SM 4 SM 5 SM 6 SM 7 SM 8 SM 9		3 6 13 15	4.3.4.5.6 4.3.4.5.7 4.3.4.5.8	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9 SR 6.1 SR 6.2
Detect	Detected events are analysed to understand attack targets and methods	SM 1.		3 6 13 15	4.3.4.5.6 4.3.4.5.7 4.3.4.5.8	R 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9

Service Name - Network Monitoring Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference - ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
						SR 6.1 SR 6.2
Detect	Event data are collected and correlated from multiple sources and sensors	SM 1 SM 2 SM 3 SM 4 SM 5 SM 6 SM 7 SM 8 SM 9		1 3 4 5 6 7 8 11 12 13 14 15 16		SR 6.1
Detect	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	CM 1 PR 8 MS 15 MS 16			4.3.3.3.7	
Detect	Network Vulnerability scans are performed in collaboration with team responsible for Security Monitoring and Operations	IM 9		4 20	4.2.3.1 4.2.3.7	
Detect	Network Monitoring processes are tested	SM 1			4.4.3.2	SR 3.3
Detect	Network Audit/log records are determined, documented, implemented, and reviewed	AC 4 AC 5 AC 7 AC 8		19	4.3.4.5.2	

Service Name - Network Monitoring Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference - ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Respond	Notifications from detection systems are investigated	IM 4		4 6 8 19	4.3.4.5.6 4.3.4.5.7 4.3.4.5.8	SR 6.1
Respond	Coordination with internal and external stakeholders occurs consistent with response plans	IM 4 IM 7		19	4.3.4.5.5	
Respond	Event detection information is communicated to appropriate parties * In case of Alert, Network Security Team will execute response actions * In case of Incident/Breach, Incident Response Team will execute response actions					
Recover (In collaboration with Teams responsible for Security Monitoring and Operation and Incident Handling and Response)	Recovery plan is executed during or after a cybersecurity incident	IM 4		10		

Service Name - Network Monitoring Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference - ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Recover (In collaboration with Teams responsible for Security Monitoring and Operation and Incident Handling and Response)	Incidents are contained	IM 1 IM 2 IM 3 IM 4 IM 5 IM 6 IM 7 IM 8 IM 9		19	4.3.4.5.6	SR 5.1 SR 5.2 SR 5.4
Recover (In collaboration with Teams responsible for Security Monitoring and Operation and Incident Handling and Response)	Incidents are mitigated	IM 1 IM 2 IM 3 IM 4 IM 5 IM 6 IM 7 IM 8 IM 9		4 19	4.3.4.5.6 4.3.4.5.10	
Recover (In collaboration with Teams responsible for Security Monitoring and Operation and	Newly identified vulnerabilities are mitigated or documented	IM 9		4		

Service Name - Network Monitoring Management						
Process Phases	Activities/Controls	Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)	Controls Reference — NICS (National ICS Security Standard v3.0)	Controls Reference — CSC	Controls Reference - ISA 62443-2-1:2009	Controls Reference — ISA 62443-3-3:2013
Incident Handling and Response)						

Table 32: Network Monitoring Management activities mapping industry information security standards – Part II of II

Network Security - Network Monitoring Management							
Process Phases	Activities/Controls	Controls Reference — ISO/IEC 27001:2013	Controls Reference — NIST SP 800-53 Rev. 4	Controls Reference — PCI DSS 3.2	Controls Reference -HIPAA	Controls Reference — Cloud Security Alliance (CCMv3.0.1)	Controls Reference - GDPR
Identify	Physical devices and systems within the organization are inventoried	A.8.1.1 A.8.1.2	CM-8 PM-5	1.1.1 1.1.4 1.1.6 1.1.7			

Network Security - Network Monitoring Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference -HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Identify	Organizational communication and data flows within the system and between interconnected systems are mapped	A.13.2.1 A.13.2.2	AC-4 CA-3 CA-9 PL-8	1.1.2 1.1.3			
Identify	External network systems are catalogued						
Identify	Adequate capacity to ensure availability is maintained	A.12.4.1 A.16.1.1 A.16.1.4	AU-6 CA-7 IR-4 SI-4	12.10.1			
Detect	Detected events are analysed to understand attack targets and methods	A.12.4.1 A.16.1.1 A.16.1.4	AU-6 CA-7 IR-4 SI-4				
Detect	Event data are collected and correlated from multiple sources and sensors	A.12.4.1 A.16.1.7	AU-6 CA-7 IR-4 IR-5 IR-8 SI-4	10.2 10.2.2 10.2.3 10.2.4			
Detect	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	A.11.1.2 A.11.2.4 A.11.2.5 A.11.2.6	MA-2 MA-3 MA-5 MA-6				

Network Security - Network Monitoring Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference -HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Detect	Network Vulnerability scans are performed in collaboration with team responsible for Security Monitoring and Operations	A.12.6.1	RA-5				
Detect	Network Monitoring processes are tested	A.14.2.8	CA-2 CA-7 PE-3 SI-3 SI-4 PM-14	10.2			
Detect	Network Audit/log records are determined, documented, implemented, and reviewed	A.16.1.2 Clause 7.4 Clause 16.1.2	CA-2 CA-7 CP-2 IR-4 IR-8 PE-6 RA-5 SI-4	10.6.1 10.6.2 10.7			
Respond	Notifications from detection systems are investigated	A.12.4.1 A.12.4.3 A.16.1.5	AU-6 CA-7 IR-4 IR-5 PE-6 SI-4				
Respond	Coordination with internal and external stakeholders occurs consistent with response plans	Clause 7.4	CP-2 IR-4 IR-8				

Network Security - Network Monitoring Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference -HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Respond	Event detection information is communicated to appropriate parties * In case of Alert, Network Security Team will execute response actions * In case of Incident/Breach, Incident Response Team will execute response actions						
Recover (In collaboration with Teams responsible for Security Monitoring and Operation and Incident Handling and Response)	Recovery plan is executed during or after a cybersecurity incident	A.16.1.5	CP-10 IR-4 IR-8				
Recover (In collaboration with Teams responsible for Security Monitoring and Operation and Incident Handling and Response)	Incidents are contained	A.12.2.1 A.16.1.5	IR-4				
Recover (In collaboration with Teams responsible for Security Monitoring and	Incidents are mitigated	A.12.2.1, A.16.1.5	IR-4				

Network Security - Network Monitoring Management							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference -HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Operation and Incident Handling and Response)							
Recover (In collaboration with Teams responsible for Security Monitoring and Operation and Incident Handling and Response)	Newly identified vulnerabilities are mitigated or documented	A.12.6.1	CA-7 RA-3 RA-5				

6 Data Protection

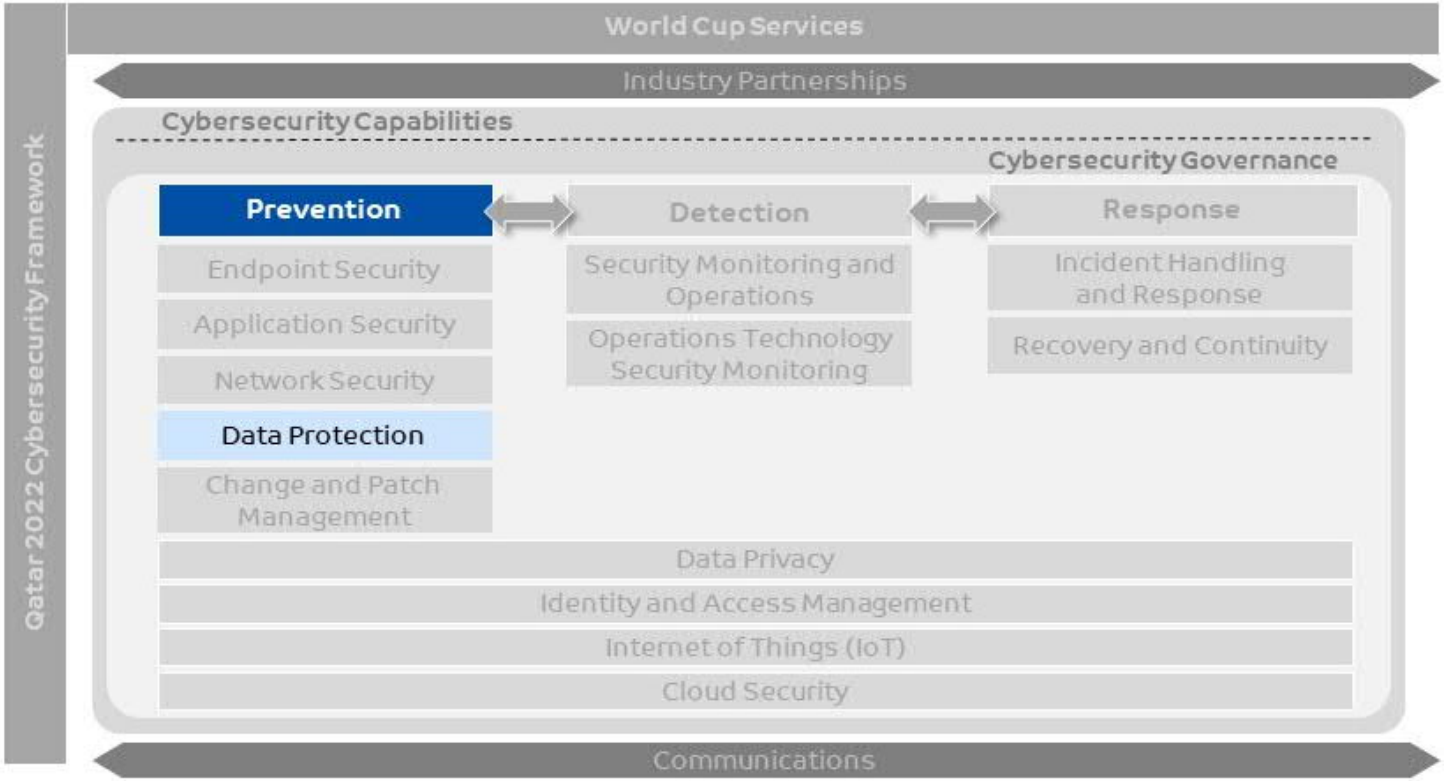
6. Capability Description – Data Protection

A capability that prevent classified information from leaving an entity's boundaries without authorization or unauthorized use of data in general.

This capability will help implementing the processes, controls and technologies required to build a sustainable data protection program aligned to the business and focused on protecting the data that matters most with respect to services provided to the world cup.

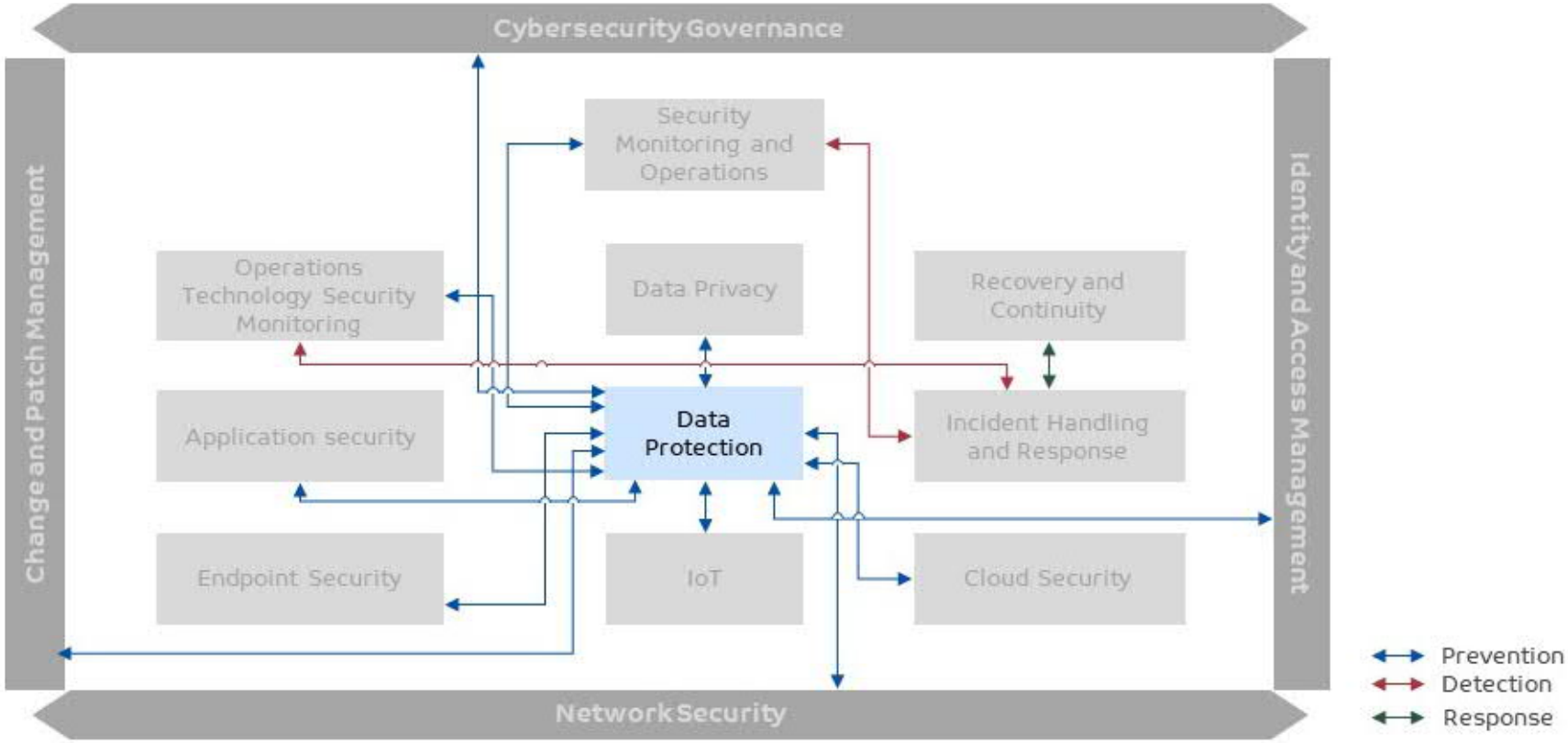
This chapter focuses on 'Data Protection" capability defined under the 'Prevention' pillar of the world cup cybersecurity capabilities

Figure 38: Cybersecurity capabilities – Data Protection



Following figure depicts linkage of Data Protection with other cybersecurity capabilities defined in the framework.

Figure 39: Data Protection linkage with other capabilities



6.1 Prerequisites

Following are the prerequisites, which are required for a successful Data Protection capability:

- Security risks identified for the information/data to be protected during the risk assessment have been communicated and considered while defining data protection requirements
- Information to be protected have been identified in all assets including data in endpoints, networks, applications, data and cloud devices or services (refer to other capability chapters such as cybersecurity governance, endpoint security, application security, network security, data privacy and cloud security for more guidance)
- Complementing Information security processes and capabilities must be applied as well to support the confidentiality, integrity and availability of data (refer to other capability chapters such as cybersecurity governance, identity and access management, endpoint security, application security, network security, data privacy and cloud security)
- Appropriate logs and events have been enabled on identified information assets for collection and analysis (refer to other capability chapters such as endpoint security, network security and application security)
- The entity's IT team should be notified of any change management activities (refer to change management capability)
- Define dependencies with other capabilities such as 'governance' to set the scene of what Information needs to be protected i.e. identify the business process-->Information related to the business process-->classify and label Information-->protect Information
- Appropriate physical security controls have been implemented to protect the data misuse

6.2 Data Protection Service

From world cup perspective, the ***Table 33: Data Protection Service*** describes respective activities that needs to be conducted for the Data Protection service. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal data protection policies, procedure and guidelines
- Define data protection program scope and identify target assets
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define acceptance standards and include national and sector data protection requirements (eLaw, NIA, PCI DSS)
- Deploy/configure appropriate solutions to align with established standards
- Deploy and train team members to support
- Identify opportunities of automation where applicable
- Define the acceptable services levels for the remediation activity
- Continually improve policy, procedure & guidelines with changing risks and lessons learned

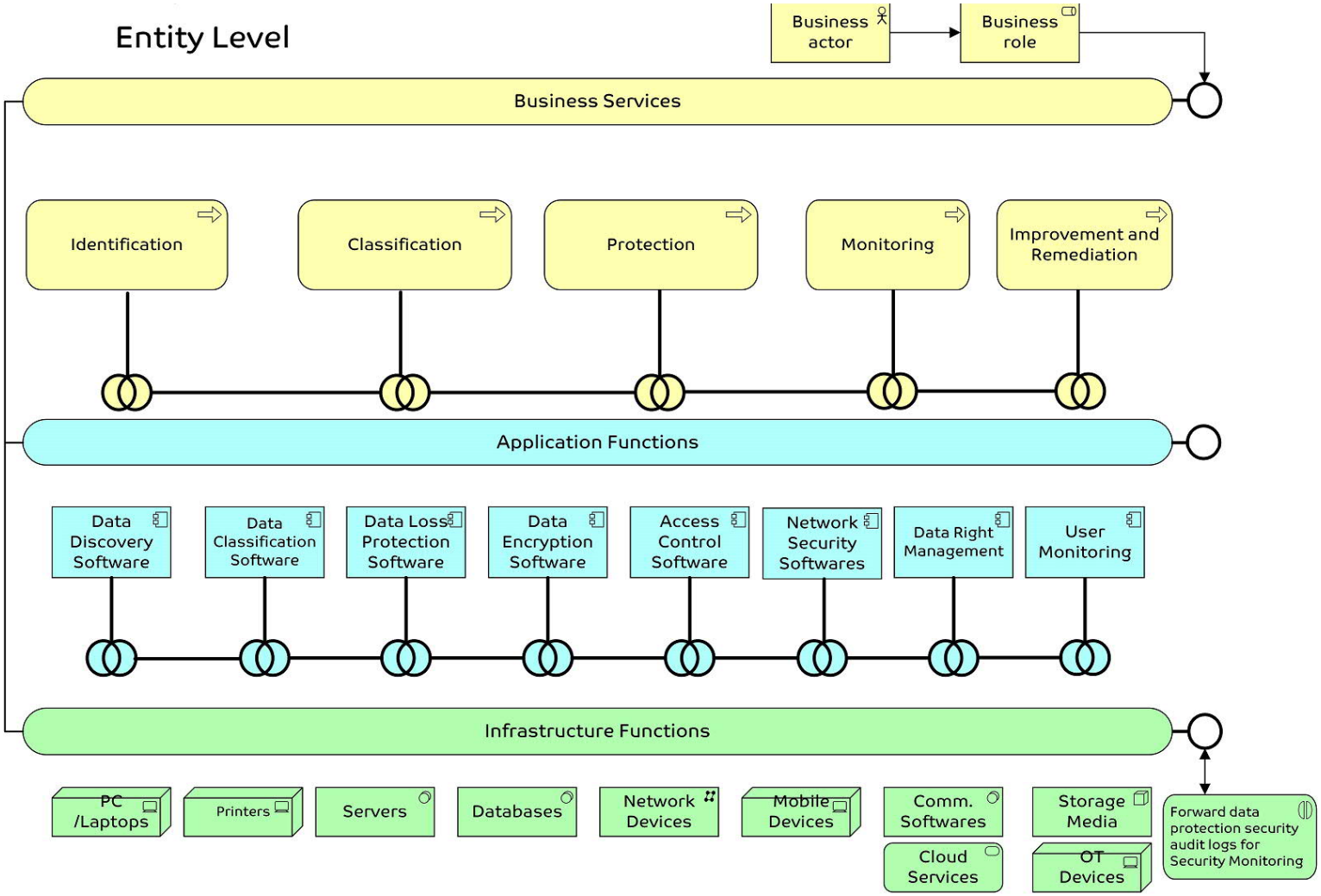
Table 33: Data Protection Service

Service Name: Data Protection	
Description	Data Protection processes identifies confidential data, tracks and monitor that data as it moves through and out of the entity and prevents unauthorized disclosure of these data.
Process Phases	**Activities/Controls**
Identify	• Understand the entity's information assets • Identify all information sources that needs to be protected based on its level of sensitivity, value, and criticality
Classify	• Data labelling as it is created, using labels that are clear and meaningful • Data classification process according to its value, sensitivity, risk of loss or compromise, legal and retention requirements of the entity • Data categorized in terms of its need for protection (i.e. Public, Internal, Sensitive, Restricted, etc.)
Protect	• Protect data based on its classification, with the highest protections applied to the most sensitive data
Monitor	• Understand how data is used and identify existing behaviour that puts data at risk • Monitor all data movement to gain visibility into sensitive data movement and determine the issues that need to be addressed
Improve and remediate	• Continuously improve and remediate identified errors and processes • Data Declassification or destruction and secure disposal

6.3 Data Protection Capability Model

Following figure illustrates an architecture model established for Data Protection capability at Entity level:

Figure 40: Data Protection Capability Model



Above figure defines the Data Protection capability model in layered approach**:**

- **The Business layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- **The Application layer** supports the business layer with application services which are realized by (software) application components.
- **The Infrastructure layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

6.4 Information Flow at various levels

There is no requirement to share data protection service information to the sector/national level.

6.4.1Services expected at each level

Data protection service will be applicable to all the applications used for world cup irrespective of the level (i.e. Entity/Sector/National) it is being used.

6.5 Milestones

Following milestones have been defined for Data Protection:

- Determine data protection objectives and identification of data assets that need to be protected
- Data Classification processes are performed
- Protection of entity's data is enabled
- Monitoring of entity's data is enabled and reported
- Improvement and remediation processes have been implemented to achieve the defined objectives

6.6 Skills required for Data Protection

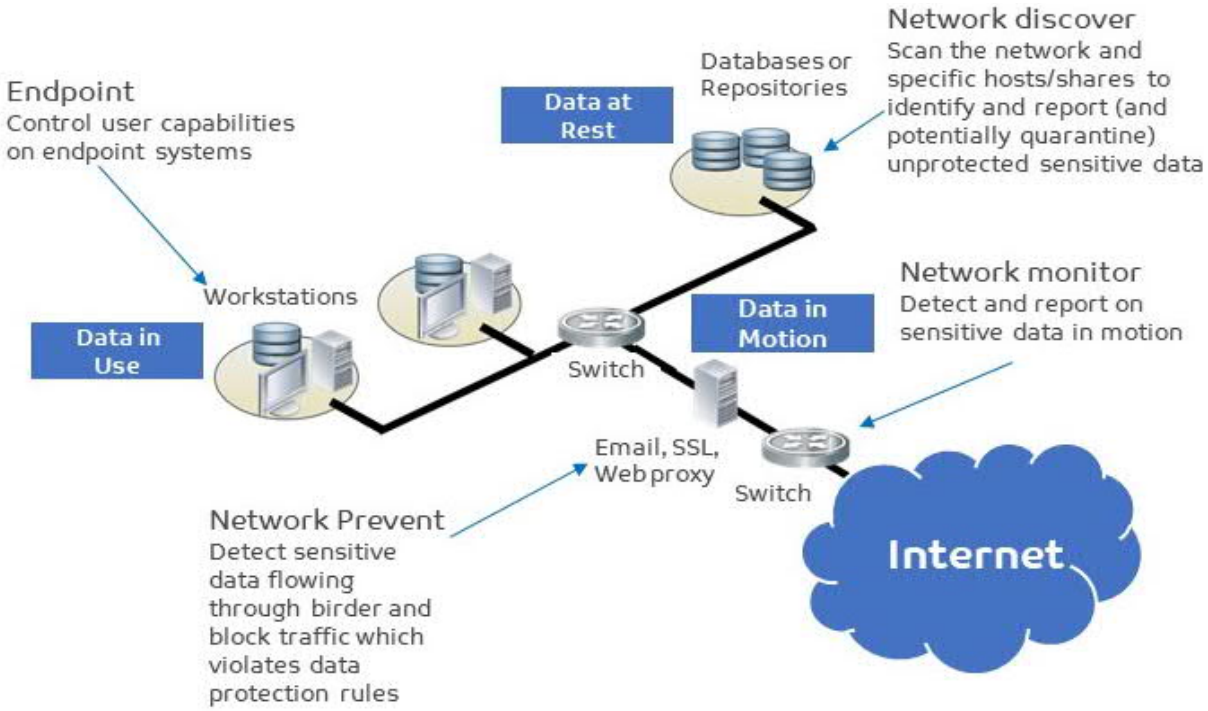
Following are the skills expected from personnel executing Data Protection activities:

- Data Protection roles and responsibilities must be clearly defined, and stakeholders from across the enterprise should be continuously engaged
- Accountability for the program should be clearly established with effective governance processes
- Data owners/creators must understand their responsibilities for classifying and protecting sensitive information
- Structure for making data-related decisions which defines roles/responsibilities, ownership/stewardship, and handles communication of data governance determinations
- Data governance must be a shared responsibility between the business and technology
- Understands how data is used within business processes and its impact on desired business process outcomes
- Experience with data analysis and data quality assessment techniques
- Capable of examining data trends to determine the root cause of variations
- Possesses knowledge of data lifecycle activities such as data definitions, data lineage (data life cycle that includes the data's origins, what happens and where it moves over time) and data quality
- Ability to interpret and define complex reporting requirements and provide appropriate information to data owners to collectively support responsibilities
- Understands how data is used within business processes and its impact on desired business process outcomes
- Experience with data analysis and data quality assessment techniques
- Capable of examining data trends to determine the root cause of variations
- Possesses knowledge of data lifecycle activities such as data definitions, data lineage and data quality

6.7 Technology

Following figure shows which technologies and their location in the entity are vital to have and should be considered for a successful Data Protection capability.

Figure 41: Data Protection Architecture



Technical controls are necessary to effectively prevent and detect data loss events. Tools supporting data protection programs should be integrated to allow for correlation and effective analysis, including technology such as data loss prevention tools, full disk encryption, removable media controls, proxy servers and content filters.

6.8 Data Protection Technologies

6.8.1Data in Motion Technologies

- Technologies for Data in Motion (Data in Transit) should be able to capture and examine all network communications, and store the resulting objects for analysis as needed
- Should be able to monitor all emails and web mails, and apply actions such as quarantine or flag or block to data that is in violation of policy

- The technology should also support encrypted traffic analysis within the limits of the applicable entity's privacy and security policies
- Scope**:**
  - E-Mails communications
  - File transfers (e.g. with third parties etc.)
  - Web traffic (e.g. Webmail, blog, social network etc.)
  - Other channels (e.g. instant messaging, P2P etc.)
  - Other outbound traffic
- Objective:
  - Better understand data loss risks across the enterprise by analysing network traffic flowing from the (internal) network to the (external) Internet.

Table 34: Data in Motion Technologies

Focus Area	Objectives	Supporting Technologies
Perimeter security	Prevent unencrypted sensitive data from leaving the perimeter. And encrypted traffic within the limits of the applicable privacy policies	DLP technology, firewalls, proxy servers
Network monitoring	Log and monitor network traffic to identify and investigate inappropriate strange, abnormal classified data transfers	DLP technology
Internet access control	Prevent users from accessing unauthorized sites or uploading data through the web through personal webmail, social media, online backup tools, etc.	Proxy servers, content filters, AD Controls, Segregation of networks
Data collection and exchange with third parties	Data exchange with third parties only occurs through secure channels	Secure E-mail, secure FTP, secure APIs, encrypted physical media
Use of instant messaging	Prevent file transfers to external parties through instant messaging and other non-web-based applications	Firewalls, proxy servers, workstation restrictions, corporate level messaging solutions
Remote access	Remote access to the company network is secure and control the data that can be saved through remote facilities such as Outlook Web Access	Encrypted remote access, restrictions on use of remote access tools to prevent data leakage to non-corporate assets
Additional authentication	Advanced authentication for added security on classified data	Two factor authentication solutions, one-time password etc.

6.8.2Data in Use Technologies

- Technologies for Data in Use (Data handling) should be able to react to user actions such as copying data and files to removable media, using Bluetooth, copy and paste certain types and classified data from a data repository and that are in violation of policy
- Removable media should be disabled by default across all infrastructure and granted on a case-by-case basis. Alternatively, read-only permissions should be the bare minimum acceptable controls
- Scope:
  - Communication peripherals (i.e. Bluetooth, infrared, Wi-Fi, etc)
  - Storage media (e.g. USB, external HD, thin clients, etc)
  - Communication software (i.e. browser web, E-mail client, etc)
  - Other actions (e.g. copy/paste)
- Objective:
  - Better understand data loss risks across the enterprise by analysing suspicious events generated by the endpoints

Table 35: Data in Use Technologies

Focus Area	Objectives	Supporting Technologies
Privileged user monitoring	Monitor the actions of privileged users with the ability to override DLP controls, perform mass data extracts, etc.	Security information and event monitoring, operating database and application log files
Access/usage monitoring	Monitor access and usage of high-risk data to identify potentially inappropriate usage.	Security information and event monitoring, operating database and application log files, endpoint DLP logs
Data sanitation	Sanitize/anonymize sensitive data when it is not required for the intended use.	Data sanitation routines and programs
Use of test data	Do not use or copy sensitive data into non-production systems. Sanitize data before moving into test systems when possible.	Data sanitation routines and programs
Data redaction	Remove sensitive data elements from reports, interfaces and extracts when they are not necessary for the intended use.	Data redaction tools
Export/save control	Restrict user abilities to copy sensitive data into unapproved containers, such as e-mail, web browsers, etc., including controlling the ability to copy, paste and print sections of documents.	Endpoint DLP technology, application controls

6.8.3Data at Rest Technologies

- Technologies for Data at Rest should be able to detect potential violations of data security and compliance, identifying confidential and sensitive data stored in your repositories. Solutions scan, detect and flag data from all relevant repositories
- Solutions scan, detect and flag data from all relevant repositories
- Technologies should ensure declassification and disposal of data on a periodic basis to re-evaluate the classification of data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value
- Scope**:**
  - Desktop/Laptop hard drives
  - File server/NAS/SAN
  - Cloud based storage and containers
  - Collaboration software (i.e. SharePoint, Documentum etc.)
  - DBMS (i.e. Oracle, Microsoft, DB2, Sybase etc.)
- Objective:
  - Better understand data loss risks across the enterprise by analysing data repositories utilized by your organization

Table 36: Data at Rest Technologies

Focus Area	Objective	Supporting Technologies
Endpoint security	Restrict access to local admin functions such as the ability to install software and modify security settings. Prevent malware, viruses, spyware, etc.	Operating system workstation restrictions, security software (Anti-Virus, personal firewall, etc.), and endpoint DLP technology.
Host encryption	Ensure hard disks are encrypted on all servers, workstations, laptops and mobile devices.	Full disk encryption tools.
Mobile device protection	Harden mobile device configurations and enable features such as password protection, remote wipe facilities, etc.	Built in security features, third-party mobile device control products.
Network/intranet storage	Govern access to network-based repositories containing sensitive data on a least privilege basis.	Access control software and permission control in operating systems, databases and file storage systems.
Physical media control	Prevent the copying of sensitive data to unapproved media. Ensure authorized data extraction only takes place on encrypted media.	Endpoint DLP technology, endpoint media encryption tools, operating system workstation restrictions.
Disposal and destruction	Ensure all equipment with data storage capabilities are clean or destroyed as part of the equipment disposal process. (Including devices such as digital copiers, fax machines, etc.)	Data erasure/data wiping software.

6.8.4Data in the Cloud Technologies

- Technologies for data in the Cloud can identify whether confidential or sensitive information have been stored in Cloud-bases storage services
- Scope:
  - Cloud storage services (e.g. Dropbox, OneDrive, Box, Google Drive etc.)
  - Cloud-based services (e.g. Office365, Salesforce, Service Now etc.)
  - Cloud service providers (e.g. Azure, AWS etc.)
- Objective:
  - Detect prohibited cloud services
  - Detect anomalous behaviours that might be indicative of data leakage
  - Compare usage and access of cloud services to determine if in line with company security policies

6.9 Data Classification Categories

Data can be classified into below four categories as part of data classification following the level of confidentiality of the information to provide access only for authorized persons.

Table 37: Data classification categories (reference NIA 2.0)

Level	Description of classification level	Target Audience
Public	Information which is intended or approved for public release. Classification label: “Public”	All internal employees/approved third parties/public
C1 Restricted	For internal use and the information which is considered sensitive but is not likely to have a significant impact to the organization if compromised and the disclosure would cause light to moderate damage to the affected party. Classification label: “Internal”	Only approved internal groups/departments with a documented business need to know
C2 Restricted	Sensitive information that in conjunction with other data could have a negative impact to the organization's competitive advantage in the market, if compromised. Sensitive information protected by regulatory statutes (e.g. HR data, sensitive constituent data, etc.) Classification label: “Limited Access”	The access is for defined users, roles or user groups, according to specific rules
C3 Restricted	Confidential information whose disclosure would cause severe damage to the affected party (Board/executive/minister level management changes, decisions etc.). Extremely sensitive information, that if compromised, is likely to have a direct negative impact to	Limited to a very small set of personnel. Only approved individuals with a documented business-need to know. For

Level	Description of classification level	Target Audience
	the organization's competitive advantage in the market, reputation or compliance with applicable regulations Material. Classification label: "Restricted"	example, approved individuals on Research and Development teams
C4 National Security	It is the highest level of classified information Material would cause "exceptionally grave damage" to national security if made publicly available. Markings (Confidential, Secret, Top Secret)	Limited to a very small set of personnel (Military, Intelligence, etc)

6.10 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards.

Table 38: Data Protection activities mapping industry cyber security standards – Part I of II

Service Name Data Protection						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identify	Understand what company's information assets are	CS8 CS9 CS12 IE1 IE2 GS5 GS13 SU10	6.2.1 6.8.1	12	4.2.3.4	
Identify	Identify the data; its value and information that need to be protected			13, 14	4.2.3.6	

Service Name Data Protection						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Classify	Classify data as it is created, using labels that are clear and meaningful			13, 14	4.2.3.6	
Classify	Data classification process according to its value, sensitivity, risk of loss or compromise, legal and retention requirements of the entity			13, 14	4.2.3.6	
Classify	Data categorized in terms of its need for protection (i.e. Public, Internal, Sensitive, Restricted etc.)		6.6.14 6.6.21	13, 14		SR 3.4, SR 4.1
Protect	Protect data based on its classification, with the highest protections afforded to the most sensitive data		5.2.2 6.6.1 6.8.2 6.8.3	13, 14		SR 3.1, SR 3.8, SR 4.1, SR 4.2
Monitor	Understand how data is used and identify existing behaviour that puts data at risk			13	SR 5.2	
Monitor	Monitor all data movement to gain visibility into sensitive data movement and determine the issues that need to be addressed			1, 2, 3, 5, 9, 12, 13, 15, 16		

Service Name Data Protection						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Improve and remediate	Continuously improve and remediate identified errors and processes			4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8		
Improve and remediate	Data Declassification and disposal		6.7.1 6.7.2 6.8.3	1	4.3.3.3.9, 4.3.4.4.1	SR 4.2

Table 39: Data Protection activities mapping industry cyber security standards – Part II of II

Data Protection							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Identify	Understand what company's information assets are	A.13.2.1, A.13.2.2	AC-4, CA-3, CA-9, PL-8	1.1.2, 1.1.3	164.308(a)(1)(ii)(A) 164.308(a)(3)(ii)(A) 164.308(a)(8) 164.310(d)	DSI-01, DSI-02	
Identify	Identify the data; its value and information that need to be protected	A.8.2.1	CP-2, RA-2, SA-14, SC-6	9.6.1, 12.2	164.308(a)(7)(ii)(E)	DSI-01, DSI-02	
Classify	Classify data as it is created, using labels that are clear and meaningful	A.8.2 Information Classification A.8.2.2 Labelling of Information	MP-3, CP-2, RA-2, SA-14, SC-6	9.6.1, 12.2	164.308(a)(7)(ii)(E)	DSI-04	
Classify	Data classification process according to its value, sensitivity, risk of loss or compromise, legal and retention requirements of the entity	A.8.2 Information Classification A.8.2.1 Classification of information	RA-2, CP-2, RA-2, SA-14, SC-6	9.6.1, 12.2	164.308(a)(7)(ii)(E)	DSI-01, DSI-03	
Classify	Data categorized in terms of its need for protection (i.e. Public, Internal, Sensitive, Restricted etc.)	A.8.2.3	MP-8, SC-12, SC-28	3.1, 3.3, 3.4, 3.5, 3.6, 3.7	164.308(a)(1)(ii)(D) 164.308(b)(1) 164.310(d) 164.312(a)(1) 164.312(a)(2)(iii) 164.312(a)(2)(iv) 164.312(b)	DSI-01. DSI-02, DSI-03	

Data Protection							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
					164.312(c) 164.312(d) 164.314(b)(2)(i)		
Protect	Protect data based on its classification, with the highest protections afforded to the most sensitive data	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	SC-8, SC-11, SC-12	4.1, 4.2, 4.3	164.308(b)(1) 164.308(b)(2) 164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii) 164.314(b)(2)(i)	DSI-07, DSI-05	
Monitor	Understand how data is used and identify existing behaviour that puts data at risk	A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3	AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4		164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.310(b) 164.310(c) 164.312(a) 164.312(e)	DSI-02, DSI-03,	

Data Protection							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Monitor	Monitor all data movement to gain visibility into sensitive data movement and determine the issues that need to be addressed	A.12.4.1, A.14.2.7, A.15.2.1	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	10.1, 10.6.1, 11.1, 11.4, 11.5, 12.10.5	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.310(d)(1) 164.310(d)(2)(iii) 164.312(b) 164.314(b)(2)(i)	CCC-04, IAM-03, IAM-13	
Improve and remediate	Continuously improve and remediate identified errors and processes	A.16.1.6, Clause 9, Clause 10	CA-2, CA-7, CP-2, IR-8, PL-2, PM-6				
Improve and remediate	Data Declassification and disposal	A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7	CM-8, MP-6, PE-16	2.4, 9.5, 9.6, 9.7, 9.8, 9.9, 11.1.1	164.308(a)(1)(ii)(A) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv) 164.310(d)(1) 164.310(d)(2)		

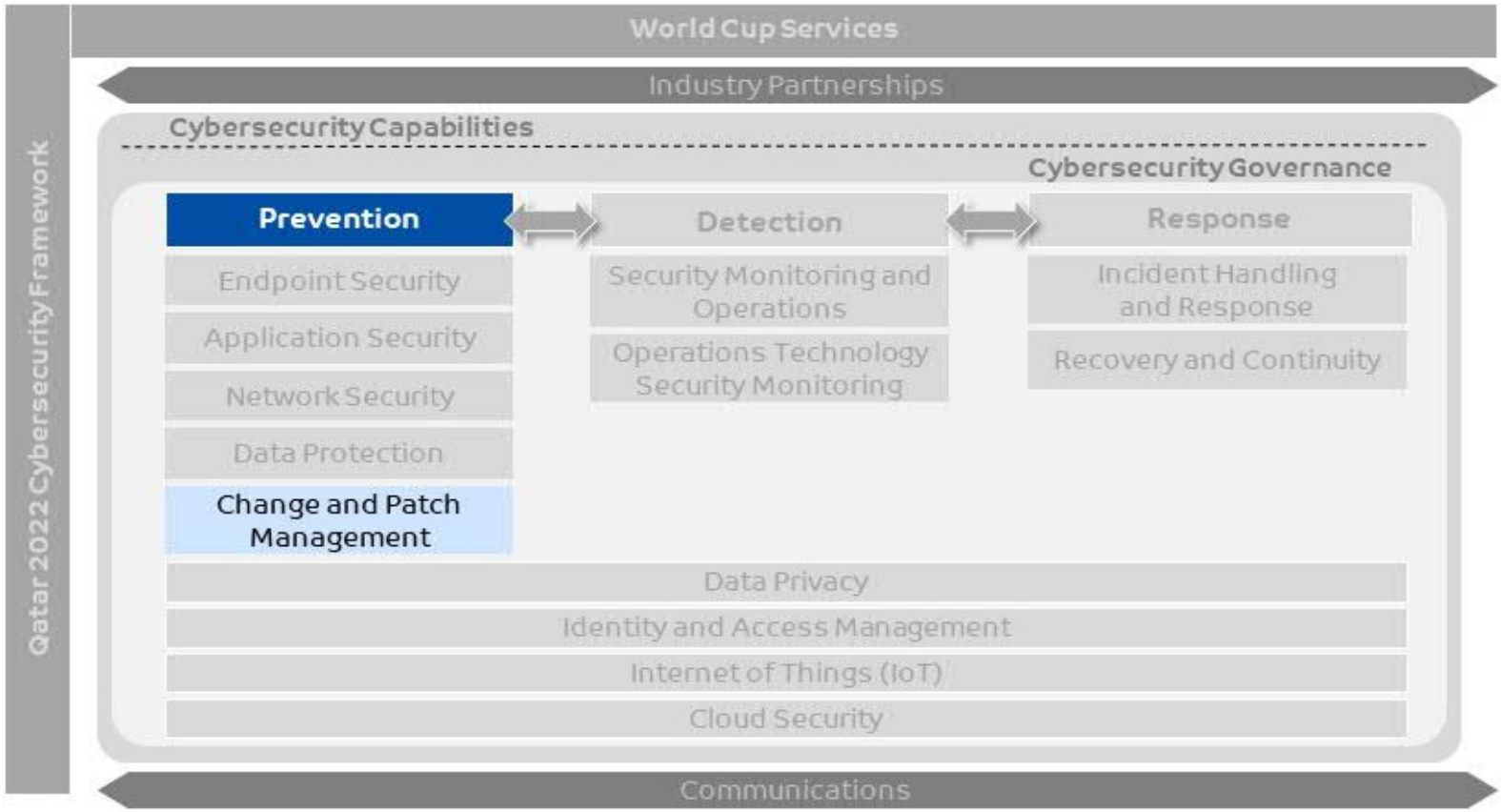
7 Change and Patch Management

7. Capability Description – Change and Patch Management

A preventive cybersecurity capability that ensures required changes affecting assets are deployed in controlled manner.

This chapter focuses on ‘Change and Patch Management’ capability defined under the ‘Prevention’ pillar of world cup cybersecurity capabilities.

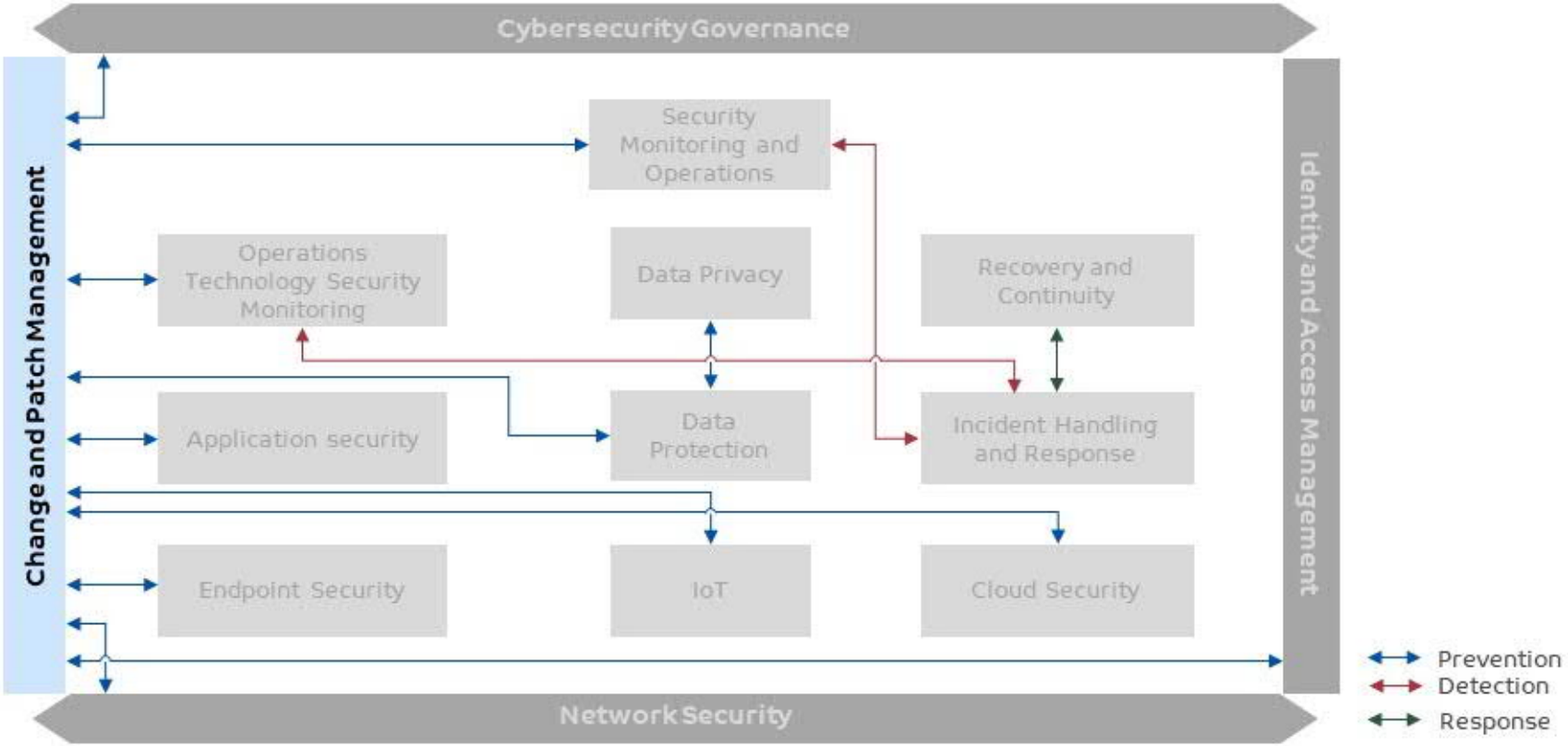
Figure 42: Cybersecurity capabilities – Change and Patch Management



The Change and Patch Management capability is a centre for all technological changes occurring in a technology environment. In other words, all information assets changes on endpoints, IoT, and OT devices configurations, patch deployment, and recovery activities undergo through a controlled environment and will be managed with this capability.

Following figure depicts linkage of Change and patch management with other cybersecurity capabilities defined in the framework

Figure 43: Change and Patch Management linkage with other capabilities



7.1 Prerequisites

Following are the prerequisites, which are required to be accomplished for Change and Patch Management capability:

- Change control committee is established, roles and responsibilities are defined and communicated
- Change impact criteria are defined and implemented for all changes, configurations, and patches on all information assets
- An information asset repository has been established and is maintained to track all changes, configurations, and patches on infrastructure components such as endpoints, network components, applications, cloud applications, other operation technologies
- Access to the change management application and information assets is compliant with Identity and Access Management capability
- Security Operation teams are notified in a timely manner for scheduled / unscheduled changes, configurations and patch deployment activities
- Unauthorized changes are detected, treated, and notified by respective stakeholders
- SLAs are defined and maintained to ensure changes, configurations, and patches go through a secured controlled environment
- Change impact criteria is defined and implemented for all information assets affecting network, applications, cloud hosted infrastructure / applications, endpoints devices, and infrastructure security
- All cybersecurity capabilities follow a controlled process for change and patch management activities
- Security risks identified for the changes during the risk assessment have been communicated and considered while defining change and patch management processes

7.2 Change and Patch Management Service

From world cup perspective, the ***Table 40: Change and Patch Management*** describes cybersecurity security service that has been defined under this capability and respective activities that needs to be conducted for each process. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal policies, procedures and guidelines
- Establish governance and assign roles and responsibilities for authorization, approvals, deployment, and recovery teams (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define the impact and risk criteria for change, configuration, and patch deployment activities
- Deploy and train team members to support
- Define services levels for change deployment, remediation and planned activities
- Define rules of engagement which will be followed
- Continually improve policy, procedure & guidelines with changing risks and lessons learned

Following table describes activities established for Change and Patch Management:

Table 40: Change and Patch Management Service

Service Name: Change and Patch Management	
Description	A Change and Patch Management process is essential for changes, configurations, patching and information asset disposal activities on information assets are securely configured, verified, deployed, and implemented.
Process Phases	**Activities/Controls**
Requirement Gathering	• Activities and processes are defined to ensure that business and security requirements are met • Secure communication channels are established and maintained for communicating change, configuration, and patch requirements
Identification	• Define a process to allocate/identify required changes, patches, configuration and disposal of information assets requirements • Establish a process to alert/notify relevant stakeholders on the required procedures for secure change, patch and configuration deployment • Define a process to assess the change and security impact associated with all changes, patches, and configuration of assets • Define rollback/recovery procedures to help restore undesired outcomes resulting impact on business/security operations • Define a process to continuously log and document change, configuration, and patch deployments plan • Establish a process to notify stakeholders in the event of breach and downtime resulting from changes, configuration, and patch deployment • Define a process to detect, alert, investigate, and notify relevant stakeholders for unauthorized changes • Establish a process to receive timely notification/alerts of required patches on information assets from third-party vendors
Authorization	• Define authorization mechanisms to ensure change, patch, and required configurations activities are consistent and inline security/business requirements
Approvals	• Define and maintain a process to oversee all activities relating to changes, patches, configurations and disposal of information assets to communicate clear decisions to stakeholders • Define a process to ensure that deployed proposed changes, patches, and required configurations meet business and security requirements • Establish and maintain secure communication channels to communicate, agree, and approve service outage and business outage resulting from change, configuration, and patch deployment activities within the change control committee
Implementation	• Establish a process to define and document change, configuration, and patch deployment plans • Define mechanisms to address security requirements on production systems • Define a process to ensure that changes, configuration, and patch deployment are tested in testing environment and meet security requirements • Define mechanisms to alert/notify respective teams for change, configuration, and patch deployment and monitoring activities • Maintain segregation of duties in deployment activities and environments in terms of approvals, testing/verification, development, and deployment • Establish a process for notifying internal and external stakeholders for planned and unplanned outages

Service Name: Change and Patch Management	
	• Define and document, and communicate required rollback /recovery procedures to ensure that unsuccessful changes, configurations, and patch deployment activities are remediated
Logging	• Define and maintain an asset repository to log all changes, configurations, and patches in terms of requirement descriptions, impact ratings, category, authorizations, and approvals • Establish a process to log and track issues and risks associated with the changes, configurations, and patches are communicated and audited/reviewed by respective stakeholders • Establish a process to capture, log, and report change, configuration, and patch deployment outcomes are correctly distributed among respective stakeholders • Define escalation mechanisms and actions plans with internal and external stakeholders in the event the security breach/unauthorized changes have occurred

7.2.1Change Categories (Reference Q-CERT)

During the requirement Gathering, stage of the Change and Patch Management process, changes, patches, and configuration requirements are captured and categorized. Change categorization is important from a tracking, and priority perspective.

The following table describes the categorization of change in the form changes (e.g. based on the nature of the change) that should be categorized in following/similar categories affecting cybersecurity of information assets.

Following table describes the categorization of change in the form changes (e.g. based on the nature of the change) it will be categorized in following categories (Reference Q-CERT):

Table 41: Change Categorization (Reference Q-CERT)

Change Categories	Change Examples
Major Change	• Change that results in business interruption during regular business hours • Change that results in business or operational practice change • Changes in any system that affects disaster recovery or business continuity • Introduction or discontinuance of an information technology service
Maintenance and Minor Change	• Application level security changes/patches • Operating system patches (critical, hotfixes, and service packs) • Regularly scheduled maintenance • Changes that are not likely to cause a service outage

Emergency and Unplanned Outage Changes	• A severe degradation of service needing immediate action • A system/application/component failure causing a negative impact on business operations • A response to a natural disaster • A response to an emergency business need • A change requested by emergency responder personnel

7.2.2Change Logging Considerations

Following table shows which information from change, configuration, and patch repository logging information that are essential and considered while performing change and patch management activities:

Table 42: Change request form containing information used to log a Change and Patch Management Activities

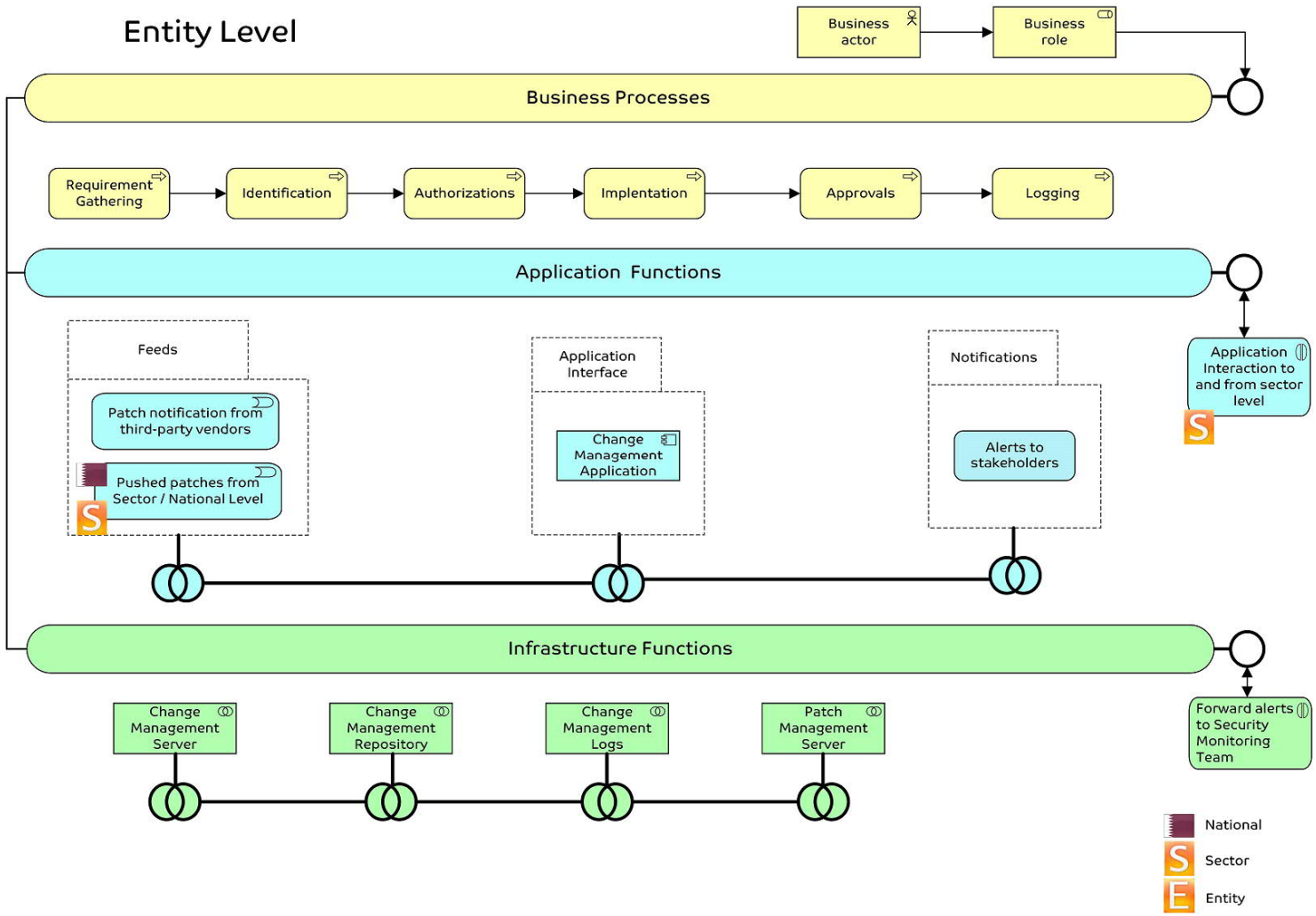
Change Request Form	
Change Request Number [CR]	
Change Category	
Requested by	
Date	
Department, location telephone	
Description of change	
Applicable asset(s) hostname/IP address	
Change needed by [date]	
Reason for change	

Change Request Form	
Change requestor signature	
Approval signature	
Change Implementation Plan	
Change Implementers	
Security Manager Sign-Off	
Testing Results	
Implementation Results	
Implementation sign off	
Change Impacts	
Change Priority	
Environment Impacted	
Estimated Resources	
Testing Plan	
Rollback Plan	
Description of Change Components	
Change Status (Accepted/Rejected/In Process)	
Change Rejection Reason (If applicable)	
Date Scheduled	
Comments	

7.3 Change and Patch Management Capability Model

Following figure illustrates an architecture model of various functions established for Change and Patch Management capability at entity level:

Figure 44: Change and Patch Management Capability Model



Above figure defines the Change and Patch Management capability model in layered approach:

- **The Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles
- **The Application Functions layer** supports the business layer with application services which are realized by (software) application components

- **The Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- The infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

7.4 Information Flow at various levels

There is no requirement to share change and patch management information to the sector/national level.

7.4.1 Services expected at each level

Change and patch management service will be applicable to all the applications used for world cup irrespective of the level (i.e. Entity/Sector/National) it is being used.

7.5 Milestones

Following milestones have been defined for Change and Patch Management:

- Change and Patch Management policies, processes, procedures, service level agreements (SLAs), are executed, maintained, and communicated with stakeholders to ensure that changes, patches, and configurations are timely and securely deployed/configured in a controlled change management environment
- Analysis are conducted to ensure changes, patches, and configuration changes are properly categorized and prioritized based on business/security requirement (e.g. vulnerability management, required security patch, etc.) and detection of unusual events (e.g. Security Monitoring and Operations cybersecurity services) to help support a secure change-controlled environment
- Change and Patch Management activities are properly logged, communicated, and assigned to internal and external stakeholders via secured channels
- Secure change and patch management activities are controlled to prevent unauthorized changes, minimize impact, rollback/ recover timely by addressing security requirements and responding to vulnerabilities on production environment
- Monitoring of change, configuration, and patch activities are in place to ensure that changes have been deployed successfully as per requirement and can detect unauthorized changes (e.g. Security Monitoring and Operations cybersecurity services)

7.6 Skills required for Change and Patch Management

Following are the skills expected from personnel executing Change and Patch Management activities:

- Perform event coordination of change, patch and configurations activities from various sources
- Knowledge of systems and network administration
- Operational knowledge of network and security appliances

7.7 Technology

Following table defines features of change and asset repositories which will help during change, patches and configuration management

Table 43: Tools and its features required for Change and Patch Management activities

Type of Tool	Features Required from Change and Patch Management perspective
Change Repository	• log and track all change requests • log and track change approvers/change control committee • e-mail integration
Asset Management Repository	• Tracking of assets and its configurations in terms of patches, updates • Integration with e-mail servers for alerts

7.8 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards

Table 44: Change and Patch Management activities mapping industry cyber security standards – Part I of II

Service Name - Change and Patch Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Requirement Gathering	Activities and processes are defined to ensure that business and security requirements are met					
Requirement Gathering	Secure communication channels are established and maintained for communicating change, configuration, and patch requirements					

Service Name - Change and Patch Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identification	Define a process to allocate/identify required changes, patches, configuration and disposal of information assets requirements	CM 1				
Identification	Establish a process to alert/notify relevant stakeholders on the required procedures for secure change, patch and configuration deployment	CM 3				
Identification	Define a process to assess the change and security impact associated with all changes, patches, and configuration of assets	CM 4				
Identification	Define rollback/recovery procedures to help restore undesired outcomes resulting impact on business/security operations					
Identification	Define a process to continuously log and document change, configuration, and patch deployments plan	CM 5				
Identification	Establish a process to notify stakeholders in the event of breach and downtime resulting from changes, configuration, and patch deployment					
Identification	Define a process to detect, alert, investigate, and notify relevant stakeholders for unauthorized changes					
Identification	Establish a process to receive timely notification/alerts of required patches on information assets from third-party vendors					

Service Name - Change and Patch Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Authorization	Define authorization mechanisms to ensure change, patch, and required configurations activities are consistent and inline security/business requirements					
Approvals	Define and maintain a process to oversee all activities relating to changes, patches, and configurations communicate clear decisions to stakeholders				4.2.2.2	
Approvals	Define a process to ensure that deployed proposed changes, patches, and required configurations meet business and security requirements					
Approvals	Establish and maintain secure communication channels to communicate, agree, and approve service outage and business outage resulting from change, configuration, and patch deployment activities within the change control committee					
Implementation	Establish a process to define and document change, configuration, and patch deployment plans					
Implementation	Define mechanisms to address security requirements on production systems					
Implementation	Define a process to ensure that changes, configuration, and patch deployment are tested and meet security requirements					

Service Name - Change and Patch Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Implementation	Define mechanisms to alert/notify respective teams for change, configuration, and patch deployment and monitoring activities					
Implementation	Maintain segregation of duties in deployment activities and environments in terms of approvals, testing/verification, development, and deployment					
Implementation	Establish a process for notifying internal and external stakeholders for planned and unplanned outages					
Implementation	Define and document, and communicate required rollback /recovery procedures to ensure that unsuccessful changes, configurations, and patch deployment activities are remediated					
Logging	Define and maintain an asset repository to log all changes, configurations, and patches in terms of requirement descriptions, impact ratings, category, authorizations, and approvals					
Logging	Establish a process to log and track issues and risks associated with the changes, configurations, and patches are communicated and audited/reviewed by respective stakeholders					
Logging	Establish a process to capture, log, and report change, configuration, and patch deployment outcomes are correctly distributed among respective stakeholders					

Service Name - Change and Patch Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Logging	Define escalation mechanisms and actions plans with internal and external stakeholders in the event the security breach/unauthorized changes have occurred. SLAs with vendors/service providers include security requires and compensation of breach/business disruptions.					

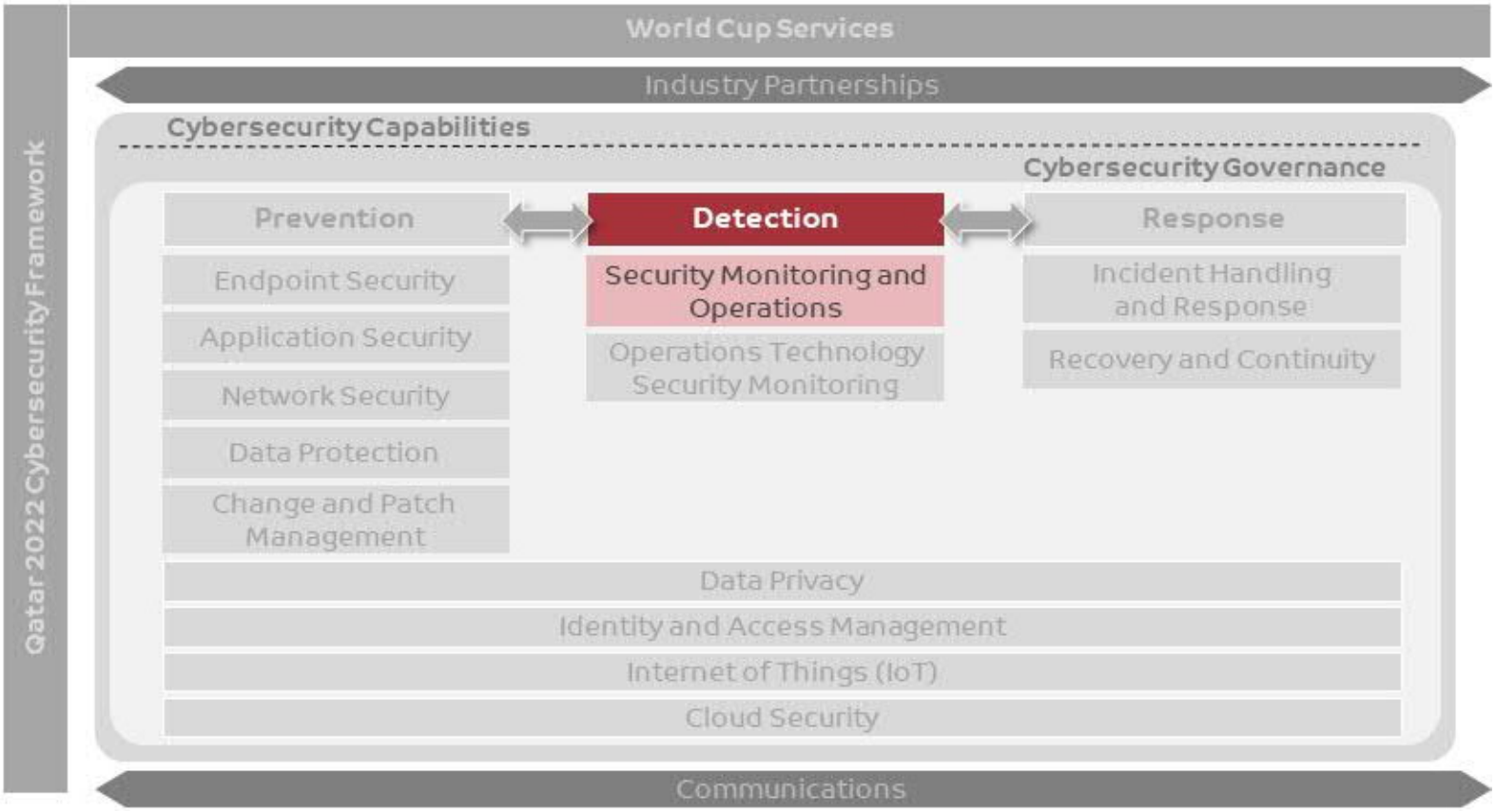
8 Security Monitoring and Operations

8. Capability Description – Security Monitoring and Operations

A capability that assesses deficits in the current state of security architecture and influence meaningful changes that are continuously monitored for deviations from their expected security posture.

This chapter focuses on ‘Security Monitoring and Operations’ capability defined under the ‘Detection’ pillar of world cup cybersecurity capabilities.

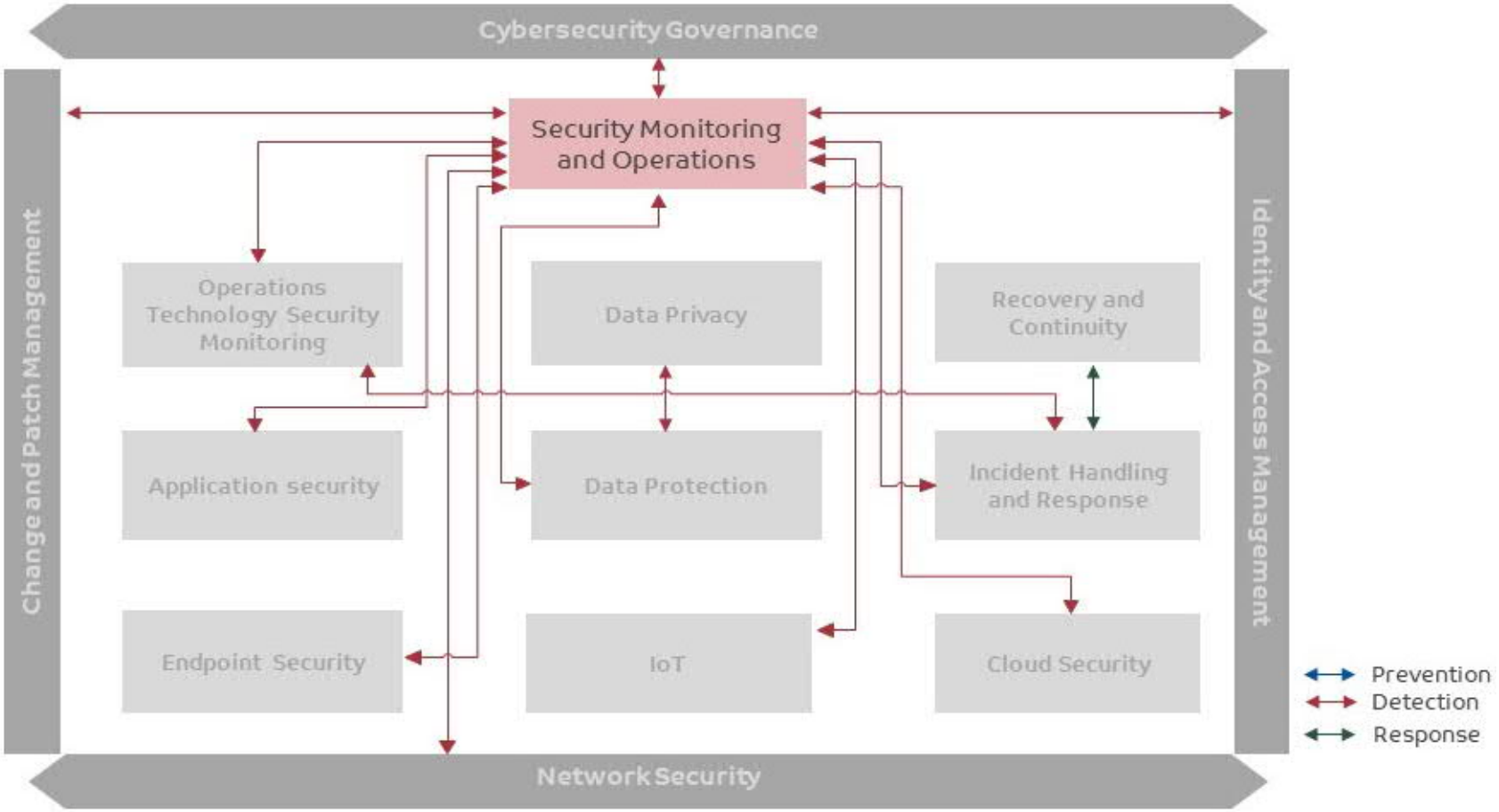
Figure 45: Cybersecurity capabilities – Security Monitoring and Operations



Security Monitoring and Operations is one of the most important capabilities within the information security portfolio to deliver cybersecurity services.

Following figure depicts linkage of Security Monitoring and Operations with other cybersecurity capabilities defined in the framework

Figure 46: Security Monitoring and Operations linkage with other capabilities



8.1 Prerequisites

Following are the prerequisites which are required to be accomplished for security monitoring and operations:

- Information assets have been identified from where the security logs will be collected
- Appropriate security logs have been enabled on identified information assets for collection and analysis (refer to endpoint security, network security and application security capability chapters)
- Network vantage points have been identified from where flow-based traffic and/or packet-based traffic (optional) will be collected. Specifically, on switches and/or VLANs configured which can help enormously for lateral movement detection.
- All collected security logs have been classified with the confidentiality rating as defined by applicable law or regulation followed (refer data protection capability chapter)
- Appropriate data-in-motion controls have been implemented as per applicable confidentiality rating while transmission
- Logs containing personal information have appropriate privacy protection measures in place as per applicable law or regulation (refer data privacy capability chapter)
- Collected security logs have been maintained for minimum period as specified by applicable law and regulation
- All system's clock has been synchronized with authoritative time source to generate accurate time stamps for security logs
- Change management database should be accessible to security monitoring team for correlation of alerts with approved changes. The security monitoring team should be notified for scheduled changes and maintenance activities
- SLAs have been defined with third-party vendors from service availability and support management perspective
- Security monitoring requires inputs from risk assessment to monitor security risks on information assets

8.2 Various services under Security Monitoring and Operations capability

From world cup perspective, table 45 to 48 describes cybersecurity services that have been defined under this capability and respective activities that needs to be conducted for each service. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal policies, procedures, and guidelines
- Define program scope and identify target assets
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define severity classification and acceptance standards
- Deploy/configure appropriate solutions to align with establish standards
- Deploy and train team members to support
- Identify opportunities of automation where applicable
- Define services levels for remediation activity
- Define rules of engagement which will be followed
- Continually improve policy, procedure & guidelines with changing risks and lessons learned

8.2.1Security Monitoring

Following table describes activities established for Security Monitoring services:

Table 45: Security Monitoring

Service Name: Security Monitoring	
Description	Security monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. As a pre-requisite of security monitoring a baseline of network operations and expected data flows for users and systems is established and managed (refer to Network Security capability chapter)
Process Phases	**Activities/Controls**
Collection	• Security audit/log records are determined, documented, implemented, and reviewed in accordance with policy • Roles and responsibilities for order of operation are well defined to ensure accountability • Detection activities comply with all applicable requirements • Cyber threat intelligence is received from information sharing forums and sources
Fusion	• Event data are aggregated and correlated from multiple sources and sensors • Malicious code is detected • Unauthorized mobile code is detected
Analysis	• Detected events are analysed to understand attack targets and methods; accordingly, triage is conducted • Impact of events is determined • Incident alert thresholds are established • Monitoring for unauthorized personnel, connections, devices, and software is performed • The network is monitored to detect potential cybersecurity events • The physical environment is monitored to detect potential cybersecurity events • Personnel activity is monitored to detect potential cybersecurity events • Vulnerability scans are performed • External service provider activity is monitored to detect potential cybersecurity events
Action	• Event detection information is communicated to appropriate parties - In case of Alert, Security Monitoring Team will execute response actions - In case of Incident/Breach, Incident Response Team will execute response actions • Detection processes are tested • Detection processes are continuously improved

8.2.2Vulnerability Management and Penetration Testing

Following table describes activities established for Vulnerability Management and Penetration Testing services:

Table 46: Vulnerability Management and Penetration Testing

Service Name: Vulnerability Management and Penetration Testing	
Description	Vulnerability Management is a cyclic process that identify, classify, remediate and mitigate vulnerabilities. [refer Cybersecurity governance chapter for security awareness and trainings to address weakness of personnel from various attacks such as social engineering]. Penetration Testing is a methodology where an attempt is being made to exploit identified vulnerability in a controlled and constrained environment.
Process Phases	**Activities/Controls**
Discover	• Conduct vulnerability scans and review system configurations • Subscribe to public and vendor security advisories • Use threat intelligence to discover/detect vulnerabilities that are exploited in the wild • Log and track vulnerabilities • Execute proof of concepts or exploits in controlled way to verify and validate the findings • Establish the level of exploitation to be conducted, in all cases avoid service level disruption with exploitation
Qualify	• Analyse vulnerabilities to determine applicability and evaluate severity • Designate risk ownership • Assign remediation tasks • Schedule remediation based on defined service levels
Treat	• Determine and document remediation of vulnerability • Schedule treatment activity based defined on service levels • Apply remediation steps to affected systems, adhering to established procedures • All changes on the affected systems must go through change management process
Monitor and Report	• Monitor process activity and report on compliance against established policies and service levels • Identify process deviations and policy exceptions and recommend corrective actions to enable continuous improvement • Collect data indicators and compare against established metrics for management reporting • Assess the effectiveness of the program on a regular basis through review of capabilities, skill sets and technical solutions • Facilitate third-party attack and penetration testing to independently assess the effectiveness of the program

8.2.3Threat Intelligence

Following table describes activities established for Threat Intelligence service:

Table 47: Threat Intelligence

Service Name: Threat Intelligence	
Description	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace Or hazard
Process Phases	**Activities/Controls**
Collect	• Cyber threat intelligence is received from information sharing forums and sources • Save applicable threat intelligence feeds before it is being analysed or consumed
Analyse	• Verify threat intelligence received from sector and or national level • Optional, in case entity by themselves has subscribed external threat intelligence - Analyse the collected threat intelligence for relevance and applicability - Discard feeds or threat intelligence that are not relevant or applicable
Integrate	• Integrate analysed threat intelligence where it will be consumed (e.g.- Firewall, IPS/IDS etc.) or correlated (e.g. – SIEM) • Define roles and responsibilities of the personnel for integration/implementation of analysed threat intelligence • Verify the implementation where applicable • Verify the efficacy of threat intelligence feeds
Produce (Disseminate)	• Define a format (for example: STIX, TAXII, CyboX) to share analysed threat intelligence to various stakeholders • Define a process to produce internal cyber threat intelligence observed in organization environment and use it in the most appropriate technology used within the organization • Define a process to export internal threat intelligence created to be integrated/consumed by other stakeholders with whom the threat intelligence has been shared

8.2.4Threat Hunting

Following table describes activities established for Threat hunting service:

Table 48: Threat Hunting

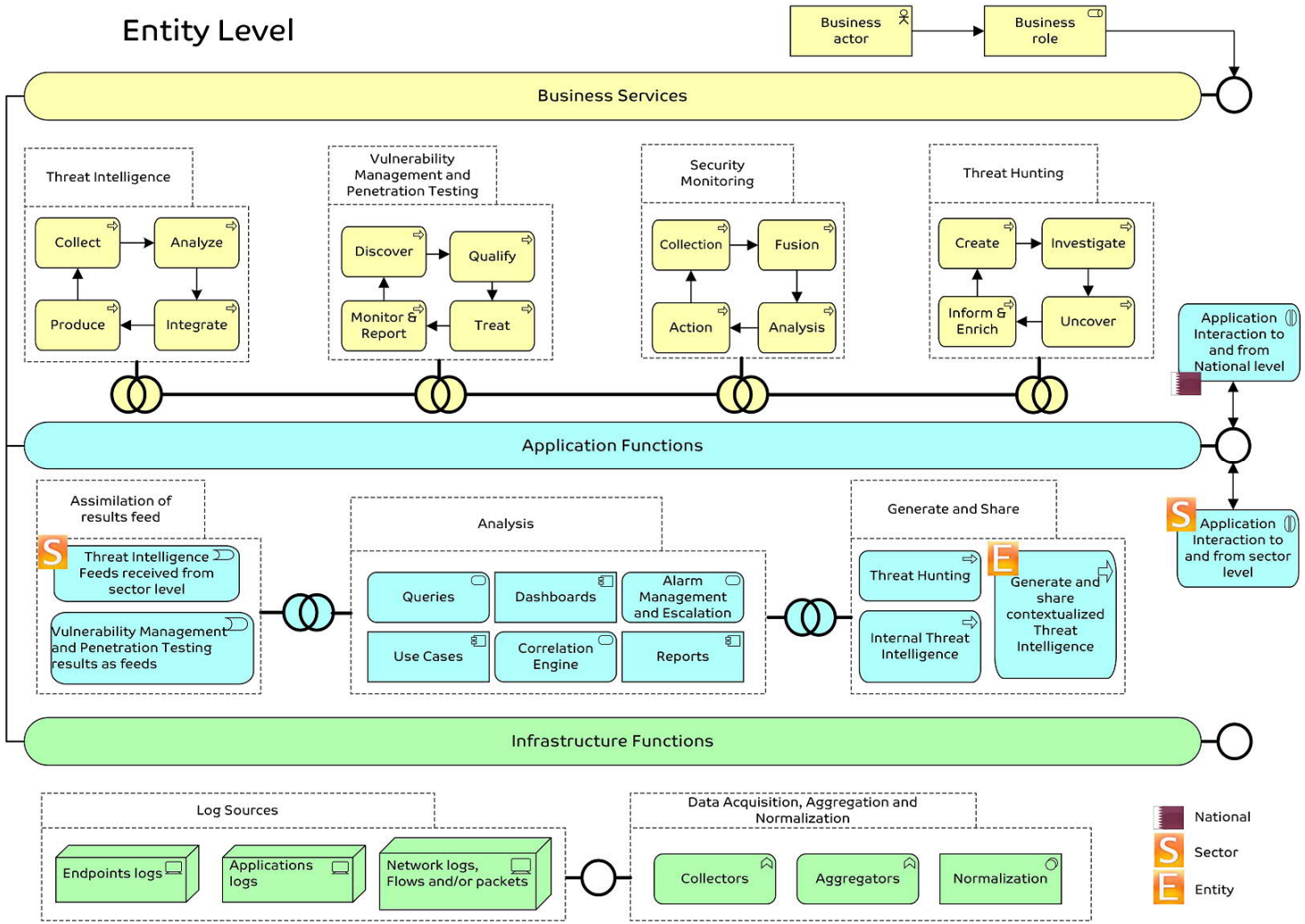
Service Name: Threat Hunting	
Description	Process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.

Service Name: Threat Hunting	
Process Phases	**Activities/Controls**
Create	• Create a hypothesis, by - Evaluating the information collected by security monitoring tools for anomalous activities - Processing data from multiple tools and sources to identify indicators of compromise that have been overlooked or assigned low-priority ratings by automated systems - Developing and exploring possible attack scenarios
Investigate	• Investigate using various tools and techniques such as linked data analysis • Leverage on all kind of collected data for investigation such as raw data, linked data and machine learning to fuse disparate datasets • Leverage Tactics, Techniques and Patterns (TTPs) information received from threat intelligence for investigations
Uncover	• Discover Tactics, Techniques and Patterns (TTPs) as disclosed in malicious patterns from the collected data
Inform & Enrich	• Use discovered TTPs - For automating the hunts such as defining a use case in SIEM - As the indicators in prevention and detection tools and appliances for rapid defined actions

8.3 Security Monitoring and Operations Capability Model

Following figure illustrates an architecture model of various functions established for Security Monitoring and Operations capability at entity level:

Figure 47: Security Monitoring and Operations Capability Model



Above figure defines the Security Monitoring and Operations capability model in layered approach:

The **Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.

- The **Application Functions layer** supports the business layer with application services which are realized by (software) application components.

- The **Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform.

8.4 Information Flow in various levels

Cybersecurity services defined under this capability are tightly coupled with the similar services running at sector and national level. All the identified threats and risks targeting at the world cup services and associated information assets, must be shared with sector and national level.

8.4.1Services expected at each level

Following table describes services expected at each level of world cup ecosystem:

Table 49: Services expected at each level – Security Monitoring and Operations

Entity	Sector	National
• Security Monitoring and Operations • Threat Intelligence (Implementation)	• Security Monitoring and Operations • Threat Intelligence - Implementation - Sharing with Entities in their sector	• Security Monitoring and Operations • Threat Intelligence - Collation - Contextualization for country and sector level - Sharing with sector level

* Entities which do not fall under any sector should forward their information to national level security monitoring team

Compendium – Security Monitoring and Operations

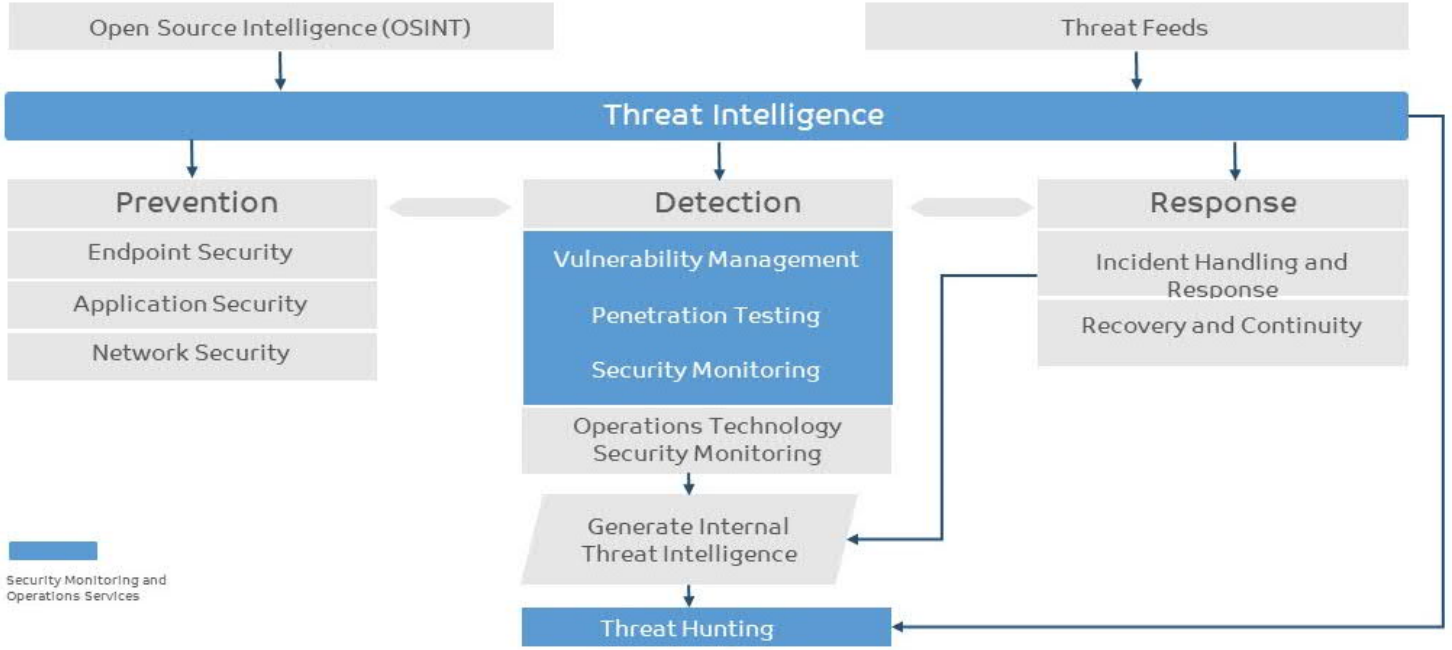
8.5 Milestones

Following milestones have been defined for security monitoring and operations:

- Anomalous activity is detected in a timely manner and the potential impact of events are understood
- The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures
- Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events

8.6 Information Flow among various activities under Security Monitoring and Operations

Figure 48: Information Flow in Security Monitoring and Operation activities



Above figure shows graphical representation of the information flow among various activities of security monitoring and operations services:

- Threat intelligence is collected from open source intelligence (OSINT) sources and Threat feeds subscribed
- Threat intelligence is contextualized as applicable
- Contextualized threat intelligence is implemented on prevention, detection and response functions of cybersecurity
- Internal threat intelligence is derived from security monitoring and operations technology security monitoring activities
- This derived information is used in conducting threat hunting activities to identify new attack patterns and again induced in threat intelligence process for all cybersecurity functions

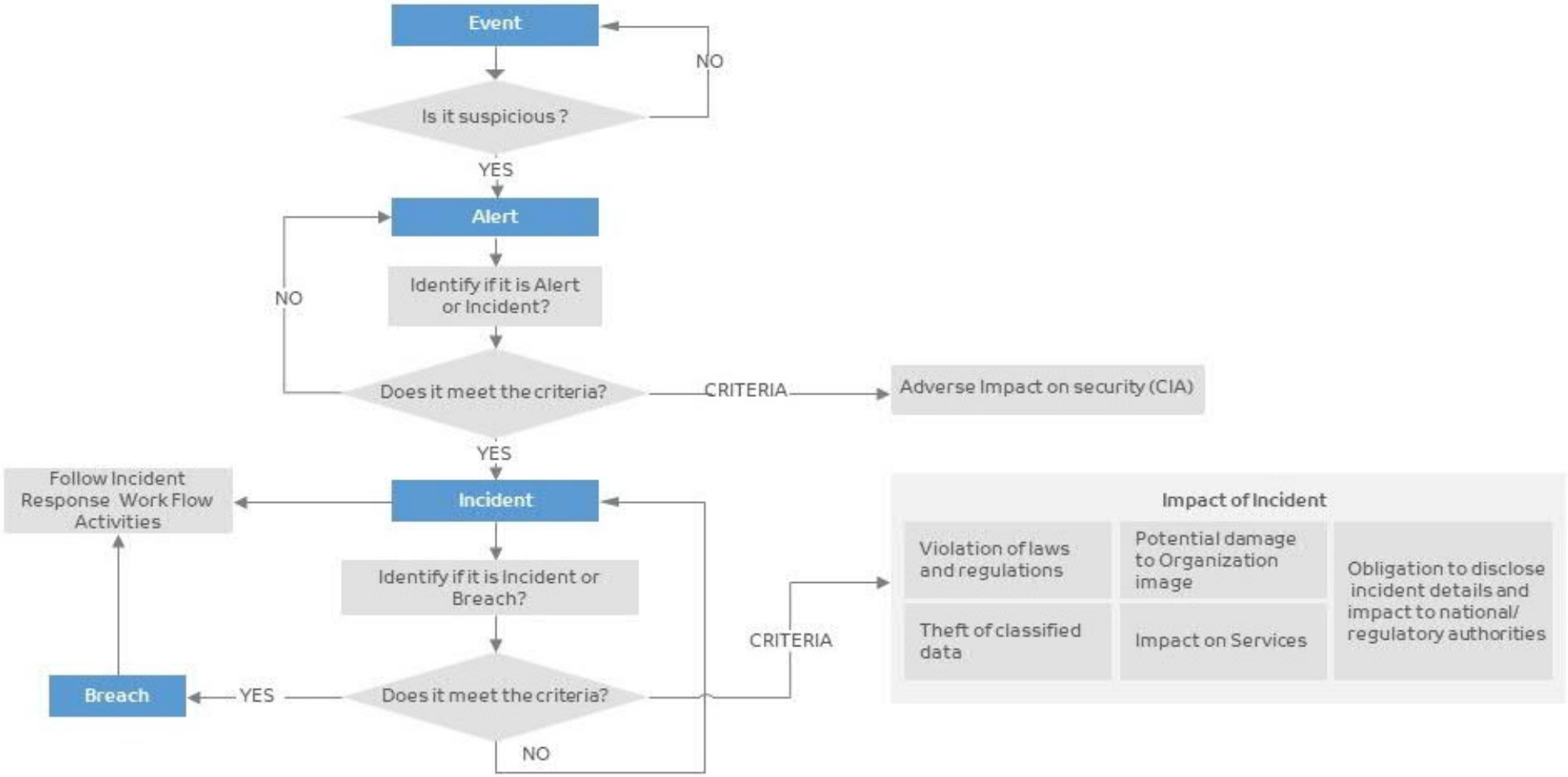
8.7 Criteria to categorize Event in Alert/ Incident/ Breach

Following are some the important definitions that needs to be considered while defining the categorization criteria:

- **Event:** An action marked, logged to a point in time that may require additional assessment
- **Alert:** a notification that change is observed to the normal behaviour of a system/environment/process/ workflow
- **Incident:** an adverse event that compromises Confidentiality, Integrity or Availability of an information asset, and has been verified as a potential threat.
- **Breach:** an incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party.

Following figure defines the criteria that needs to be followed for categorization among alert/event/incident/breach.

Figure 49: Criteria to categorize Event and Incident



8.8 Log sources

Following figures shows which logs from Network (data in motion) and from Endpoint system (data at rest) are important and should be considered and collected for security monitoring.

Figure 50: Network log sources

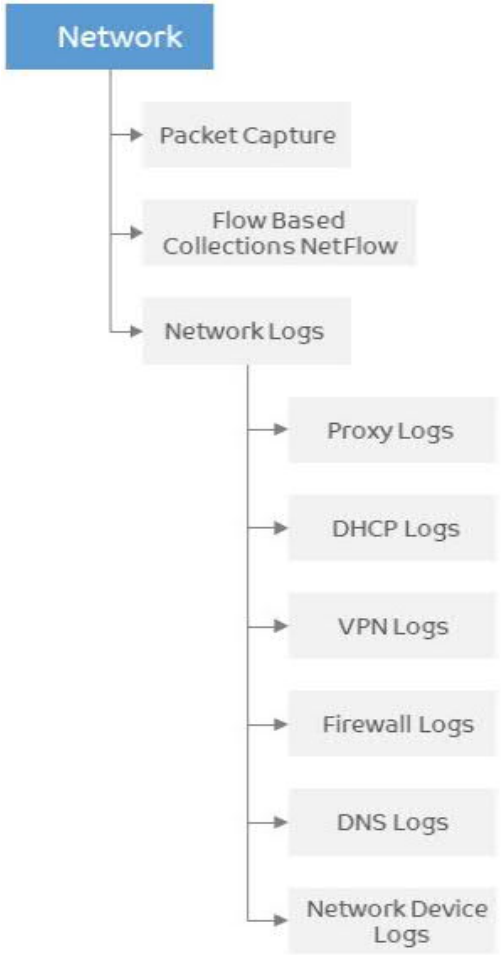
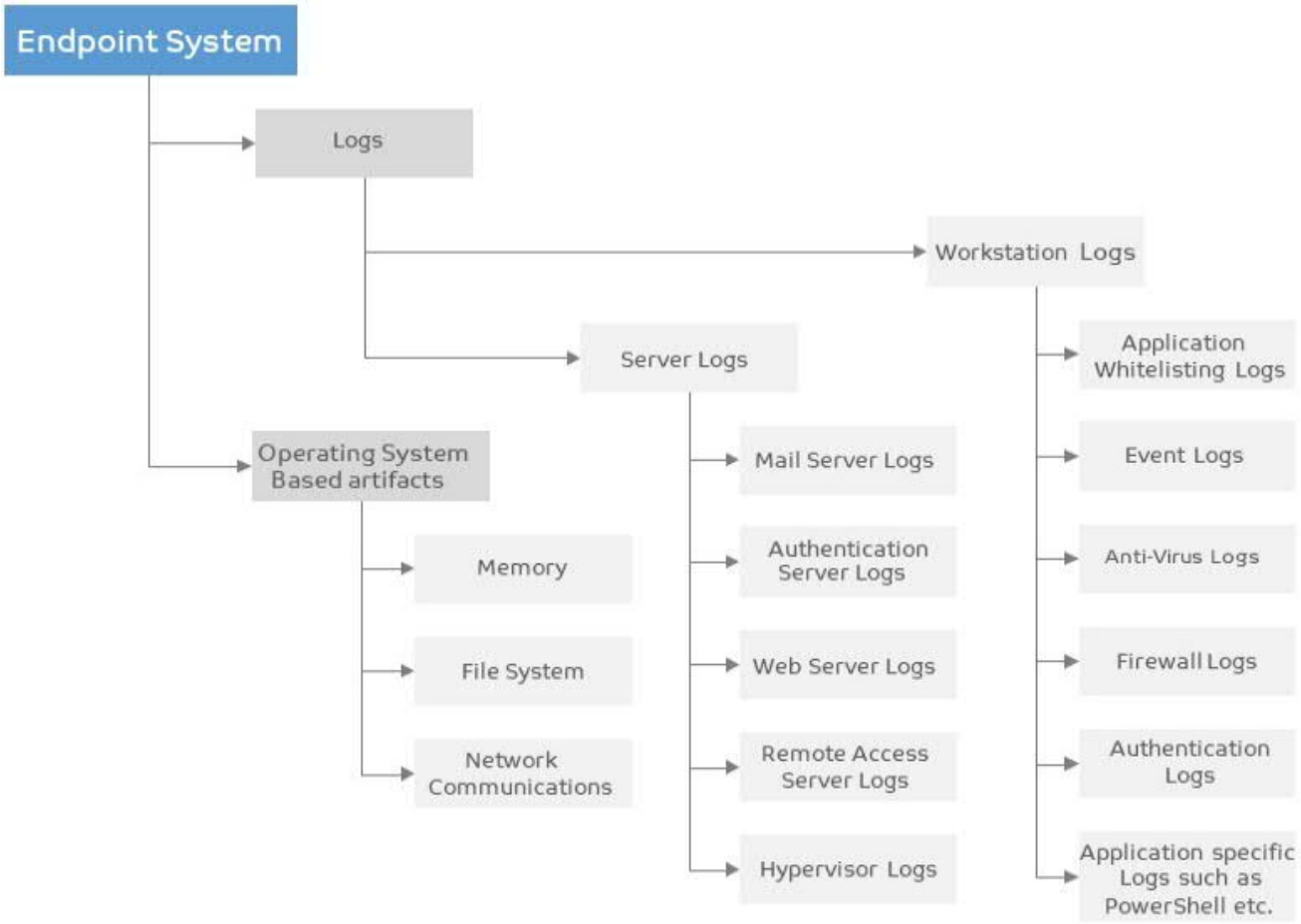


Figure 51: Endpoint system log sources



8.9 Skills required for Security Monitoring and Operations

Following are the skills expected from personnel executing Security Monitoring and Operations activities:

- Perform event analysis by correlating data from various sources
- Possess knowledge on log management & correlation, logs generated by various applications or appliances of IT infrastructure
- Competent to create custom signature/rules for detection and prevention technologies being used in organization
- Ability to create customized scripts for automation as well as for analysis
- Ability to create various use cases based on environment for better detection of anomalies
- Facilitate in developing, tuning and implementing threat detection analytics, security sensors and SOC Infrastructure
- Should be able to conduct vulnerability assessments and penetration activities
- Provide support for new analytic methods for detecting threats
- Provide support to Incident Response team for collecting evidences and in motoring of mitigation steps
- Should be able to identify gaps in detection processes
- Suggested professional certifications which can help personnel to attain skills for the services defined under security monitoring and operations:

Table 50: Security Monitoring and Operations suggested certifications

Category	Suggested Certifications
Security Monitoring (Blue Team)	• SANS GIAC Continuous Monitoring Certification (GMON) • SANS GIAC Certified Detection Analyst (GCDA)
Threat Intelligence	• SANS GIAC Cyber Threat Intelligence (GCTI)
Threat Hunting	• SANS GIAC Certified Intrusion Analyst (GCIA) • SANS GIAC Certified Incident Handler (GCIH)
Vulnerability Assessment and Penetration Testing	• Offensive Security Certified Professional (OSCP) • SANS GIAC Penetration Tester (GPEN) • SANS GIAC Web Application Penetration Tester (GWAPT) • SANS GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) • EC-Council Licensed Penetration Tester (LPT) • SANS GIAC Assessing and Auditing Wireless Networks (GAWN) • SANS GIAC Mobile Device Security Analyst (GMOB)
Security Analysis (General)	• EC-Council Certified Ethical Hacker (CEH), • SANS GIAC Certified Enterprise Defender (GCED) • SANS GIAC Security Essentials (GSEC)

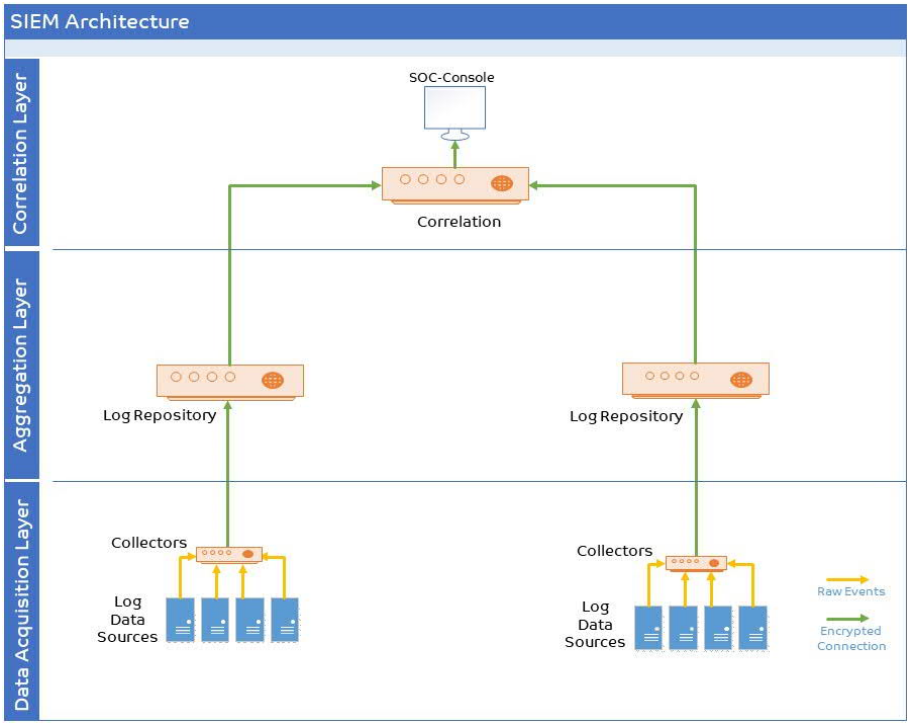
8.10 Technology – Security Monitoring and Operations

Since logs are collected and retained for business operations purposes, logs are widely available and raw log data can be aggregated for centralized analysis. SIEM or related platform can be significantly useful to conduct such analysis. Following sections briefly discuss about SIEM.

8.10.1 SIEM Architecture

SIEM will be the most important component of SOC. Following figures shows high level SIEM Architecture that can be followed for implementation:

Figure 52: High Level SIEM Architecture

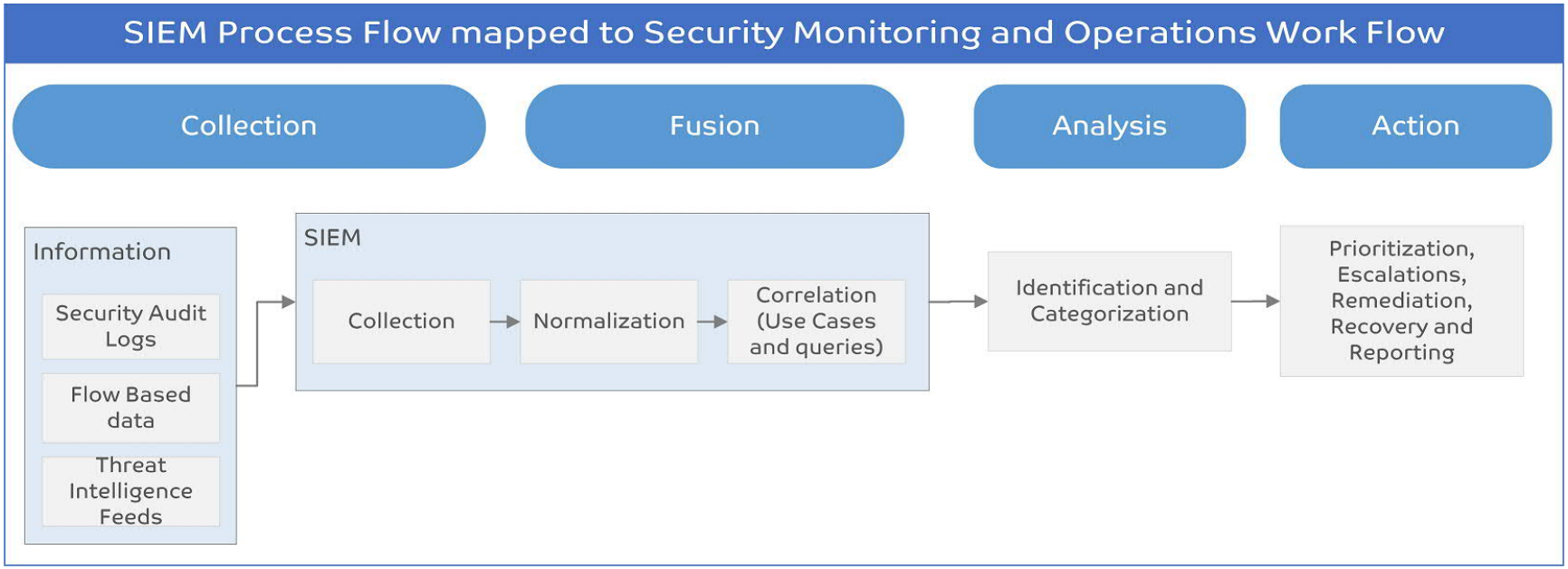


As shown in figure above:

- At data acquisition layer Collectors will collect the logs from all identified log sources, normalize and categorize in common format
- At aggregation layer Log repository will collect the data and store with capabilities of searching & reporting
- At correlation layer data collected in all log repositories will be correlated with meaningful use cases

Following figure shows the mapping between SIEM work flow and Security Monitoring activities:

Figure 53: SIEM workflow mapping with Security Monitoring activities



Above figure depicts:

- **Collection**: it defines the systematic approach to gather timely and relevant information viz. security audit logs, flow-based data, Packet Capture data (optionally) and Threat Intelligence feeds, that will be collected in SIEM solution.
- **Fusion**: the information will be normalized and correlated.
  - Normalization uses standardized queries to evaluate data from multiple resources and isolate signs of anomalous or malicious activity. It transforms data from disparate sources and reorganizes it such that data is consistent and the dependencies & relationships within the data are logical.
  - Event correlation defines the process of identifying the relationships between data. It can identify relationships between events on different devices throughout the network. This provides visibility and allows the security operations team to identify and respond to events that indicate security threats.
- **Analysis**: at this stage identification and categorization is being done.
  - Identification depends on the learning the nature and relevance of an event and discerning its criticality.
  - Categorization often applies based on the type and impact of the threat.
- **Action**: this is the stage where actual response actions will be initiated.
  - Prioritize the response actions based on the urgency to the identified event
  - All relevant stakeholders will be notified

- In case of Alert, Security Monitoring Team will execute response actions
- In case of Incident/Breach, Incident Response Team will execute response actions
- Remediation actions will be implemented with various teams' support including Incident Response and Operations teams

8.10.2 Use Cases

A Use Case is a Logical, Actionable and Reportable component of SIEM. It can be either a Rule, Report, Alert or Dashboard which solves a set of requirements.

Use cases are different for each environment and requires logs/artefacts to be collected from various sources. It is important to understand the methodology for building a use case according to the environment and available data sources. Following section defines the use case methodology that can be followed.

8.10.2.1 Use Case Methodology

Use cases must be developed based on requirements. A fixed methodology must be used while working on a use case. High level steps would include:

Step 1: Information Gathering

- Understanding the flow of data and work-flow activities pertinent to the function being monitored by the given use case
- Identifying all the touchpoints involved, i.e. firewalls, network elements, and, asset servers and databases, etc.
- Aligning the criticality of aforesaid assets with the overall criticality of the business function being served by the use case at hand
- Identifying mandates and/or regulatory requirements whose purview the use case may fall under
- Identify report template
- Identify external entity linkages
- Identify behavioural and historical inputs

Step 2: Defining Functional Content Design Points

- Define severity of alert to be raised at the SOC in case the use case is triggered
- Define method of first alert to be raised at the SOC in case the use case is triggered, i.e. dashboard alert, e-mail, etc.
- Define the reporting buckets in which this event would qualify to be compiled, i.e. daily, weekly, for a specific regulatory requirement, etc.
- Define filters to trap all constituent relevant (sub)events
- Define time and frequency factors for events to be considered a genuine advent of anticipated use case issue
- Define parameters based upon which sub-events would qualify to be a part of one set or another
- Define correlation and overlap points in order to merge multiple streams of sub-events
- Define master level meta-tags to facilitate correct category-based roll-up of use cases into larger groups for consolidated dashboards
- Define layout of dashboards and rendition of their constituent data monitors
- Define behavioural and historical holding structures

Step 3: Implementation of Functional Content in SIEM and Related SOC Sub-systems

- Create building block level filters and objects
- Create correlation rule(s)
- Implement alarm mechanisms
- Tie in with reporting templates
- Tie in with dashboards
- Tie in with external support sub-systems, e.g. trouble-ticketing system
- Implement resource allocation and management to ensure integrity of functional content

8.10.2.2 Required Use Cases

Number of use cases differs as per requirements and available data sources. Following activities should be considered while maintaining the use cases:

- Define use cases to detect current attacks
- Test the use case before applying it on production
- Use case list to be reviewed periodically
  - Additional data sources may be added to make correlation more meaningful
  - Use cases for specific attacks may not be required, thus can be deleted to reduce administrative overheads

Following are the use cases which entities should implement in their SOC:

1. Creation or deletion of accounts in short amount of time
2. Disabling of accounts
3. Adding of accounts to privileged groups and tracking of privileged account usage
4. Unauthorized use of VPN account and remote access to sensitive data
5. Login of the same account from 2 different locations in a short space of time
6. Multiple system brute force for a single user
7. Infected machine generating outbound traffic
8. Detection of data leakage or data exfiltration
9. Detection of Malware outbreaks on single machine or multiple machines
10. Track removing of evidence such as deleting the audit logs
11. Suspicious admin activity such as logging onto many different devices in a short amount of time compared to usual
12. Incoming or outgoing communication with TOR hosts
13. Monitoring of large or sensitive data copied to removable media and the use of removable media
14. Monitoring of access to sensitive data and sensitive databases

15. Application monitoring of applications such as web sites, mobile applications, web interfaces, web application firewalls, SQL injection, API monitoring and application logs
16. Identify unauthorized access to sensitive data
17. Identify failed access attempts to sensitive data
18. Identify successful access after failed access attempts to sensitive data
19. Monitoring of user account privilege escalation
20. Monitoring of shared account utilization
21. Detection of DOS against infrastructure
22. Mailboxes being accessed by unauthorized users or admin
23. Monitor access attempts by Ex-employees, Disabled accounts or service accounts
24. A sequence of a port scan then followed by exploitation such as SQL injection
25. Exploitation of specific servers or services specially web servers and database servers
26. Detection of phishing attacks
27. Determine activities such as after-hours activities or user logged in locally but with no physical access
28. User Behaviour monitoring, such as a normal user trying to login to a network device and make changes or perform admin duties.
29. Users trying to access Databases or database tables they don't have access too
30. Insider threat detection such as unusual or high-volume actions after hours or emailing large files to personal or competitor addresses/foreign countries
31. FTP, IM, IRC or other abnormal communication from high value host
32. Monitoring of data leak sites such as Dropbox, yousendit and pastebin
33. Monitoring of extraction of large or sensitive data through various mediums
34. Monitoring of payment services and payment service applications
35. Monitoring of security infrastructure, network infrastructure, server and hypervisor infrastructure
36. NAT cross-correlation -When a user enters the network and goes through a Network Address Translation mechanism it is important that the solution can tie together the original (external) address and the translated (internal) address.
37. Detection of statistical outliers on file access (read and modification) for a specific file, in order to detect potential file access policy violations.
38. Identify when the same entity is frequently sending data out of the internal network according to a proper user profiling and location of data
39. Identify failed access attempts to sensitive data
40. Identify critical actions to sensitive data such as deletion and creation
41. Complete user activity tracking reporting for selected users
42. Detection of reoccurring Virus Infections
43. Detection of different variants of reconnaissance activities
44. Identify multiple successful transactions with the same amounts and credentials
45. Identify when the same IP is frequently initiating unsuccessful transaction requests
46. Detection of ransomware
47. Detection of PowerShell-based attacks

8.11 Security Monitoring and Operations Strategy

Following table describes strategy bifurcated for all the cybersecurity activities defined under the purview of security monitoring and operations:

Table 51: Security Monitoring and Operations Strategy

Security Monitoring and Operations Strategy	
Host and Service Discovery	Objectives: • Identify Hosts and services that needs to be secured • Identify high value systems which stores classified information • Monitor violations of application whitelisting To Do List: • Leverage on existing asset inventory database, if available • Conduct Active Scanning to create most current database. This will also be helpful to identify the systems which are running and active on the network but missed to be included in asset inventory - Start with critical server networks - Focus on mitigating insecure and/or outdated systems - Re-scan the network at discrete intervals and report new hosts and/or services discovered • Conduct Passive scanning - It can also be used as an alternative to active scanning - It will include lockdown hosts which only respond to necessary systems and to ensure such systems' existence. Tools that can be used: • Vulnerability scanners • Host discovery tools such as Nmap • SNMP based system monitoring tools

Security Monitoring and Operations Strategy	
	• Network Management Software • Passive scanning tools like p0f
Vulnerability Scanning	Objectives: • Identify vulnerabilities in operating system and application services which can be exploited To Do List: • Conduct vulnerability scanning at discrete interval • Critical and High findings must be mitigated - Consider vulnerability scanner severity as opinion, however, the severity should be considered as per organization's environment and specifically asset value Tools that can be used: • Vulnerability scanners
Monitoring Patching	Objectives: • Mitigate risk To Do List: • Patch identified vulnerabilities including operating system and applications • Audit patch compliance at discrete intervals Tools that can be used: • Patch management tools
Monitor DNS Service Logs	Objectives: • Detect hostname lookup for known C2 domains To Do List: • Monitor

Security Monitoring and Operations Strategy	
	- Large DNS queries with high entropy1 - Large TXT record responses - High volumes of DNS resolution failures Tools that can be used: • Enable DNS Query logging
Monitor Change to Devices	Objectives: • Detect configuration change on devices To Do List: • Use operating system commands to check differences in configuration file - Automate the process with scripting and without leaking credentials • Where feasible, configure device to report all changes Tools that can be used: • Operating systems command such as diff or fc (file compare) • Built-in change detection feature of the appliances
Leveraging Firewall/Next Generation Firewall/Proxy data	Objectives: • Detect outbound anomalous traffic To Do List: • Proxy all outbound connections unless whitelisted • Use firewall and proxy to log outbound denied traffic. Use such logs for threat hunting and various use cases • Save and scan all executable files that passes via proxy • Monitor executable which downloads directly from IP address • Monitor high entropy in file and directory names • Monitor persistent outbound connections • Apply default deny policy on for outbound traffic on firewall unless whitelisted • Monitor traffic to following outbound ports

[1] Entropy defines randomly generated characters or strings used to give filenames and strings' name etc.

	- 25/TCP - 135/TCP - 137/UDP - 139/TCP - 445/TCP - 1900/UDP - 3389/TCP Tools that can be used: • Features available in current proxy and firewall • Define SIEM Use cases to analyse and alert. (It is expected that mentioned devices logs are being forwarded to SIEM)
Critical Windows Events	Objectives: • Detect anomalous activities on endpoints To Do List: • Monitor following critical windows events - Service creation - User creation - Adding users to privilege groups - Clearing the event log - RDP/Terminal Services certificate creation - Disabling host-based firewall - Adding specific firewall rules - External media detection - Lateral Movement - Monitor Event ID 4624 (An account was successfully logged on) that authenticates via local credentials. - Report any other except the actual domain, NT AUTHORITY and Window Manager - AppLocker events - Following events should be monitored ▪ Audit Mode: 8003 and 8006 ▪ Block/enforce mode: 8004 and 8007

Security Monitoring and Operations Strategy	
	Tools that can be used: • Operating system features
Situational Awareness	All security analysts associated with Security Monitoring Team should be aware of current emerging exposures. They can use variety of website which provides insights and awareness on events/incidents/breaches globally. The most important aspect of having situational awareness to include lessons learned from such cybersecurity events/incidents/breaches and turning into actions across prevention, detection and response pillars.

8.12 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards

Table 52: Security Monitoring and Operations activities mapping industry cyber security standards – Part I of II

Service Name: Security Monitoring						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Collection	Security audit/log records are determined, documented, implemented, and reviewed in accordance with policy	SM-1 SM-2 SM-4 SM-5 SM-6 SM-7 SM-8 SM-9	6.6.10 6.9.1 6.9.2 6.9.3 6.9.4 6.9.5 6.9.6 6.9.7	1 3 5 6 14 15 16	4.3.3.3.9 4.3.3.5.8 4.3.4.4.7 4.4.2.1 4.4.2.2 4.4.2.4	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12
Collection	Roles and responsibilities for order of operation are well defined to ensure accountability	SM-2	4.2.4 6.6.19	6		

Service Name: Security Monitoring						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Collection	Detection activities comply with all applicable requirements	SM2 SM3	6.6.10	6	4.4.3.2	
Collection	Cyber threat intelligence is received from information sharing forums and sources	IM7	4.2.7 4.2.8	4	4.2.3 4.2.3.9 4.2.3.12	
Fusion	Event data are aggregated and correlated from multiple sources and sensors	SM4		1 3 4 5 6 7 8 11 12 13 14 15 16		SR 6.1
Fusion	Malicious code is detected		6.4.1 6.4.2	4 7 8 12	4.3.4.3.8	SR 3.2
Fusion	Unauthorized mobile code is detected		6.4.3	7 8		SR 2.4
Analysis	Detected events are analysed to understand attack targets and	SM-8		3 6	4.3.4.5.6 4.3.4.5.7 4.3.4.5.8	SR 2.8 SR 2.9 SR 2.10

Service Name: Security Monitoring						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
	methods; accordingly, triage is conducted			13 15		SR 2.11 SR 2.12 SR 3.9 SR 6.1 SR 6.2
Analysis	Impact of events is determined			4 6		
Analysis	Incident alert thresholds are established			6 19	4.2.3.10	
Analysis	Monitoring for unauthorized personnel, connections, devices, and software is performed	SM-1		1 2 3 5 9 12 13 15 16		
Analysis	The network is monitored to detect potential cybersecurity events	SM2	6.6.10	1 7 8 12 13 15 16		SR 6.2

Service Name: Security Monitoring						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Analysis	The physical environment is monitored to detect potential cybersecurity events	SM2	5.2.1		4.3.3.3.8	
Analysis	Personnel activity is monitored to detect potential cybersecurity events		5.2.1	5 7 14 16		SR 6.2
Analysis	Vulnerability scans are performed		6.4.5	4 20	4.2.3.1 4.2.3.7	
Analysis	External service provider activity is monitored to detect potential cybersecurity events		6.3.2 6.3.3			
Action	Event detection information is communicated to appropriate parties			19	4.3.4.5.9	SR 6.1
Action	Detection processes are tested				4.4.3.2	SR 3.3
Action	Detection processes are continuously improved				4.4.3.4	

Table 53: Security Monitoring and Operations activities mapping industry cyber security standards – Part II of II

Service Name: Security Monitoring							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Collection	Security audit/log records are determined, documented, implemented, and reviewed in accordance with policy	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1	AU-1 AU-2 AU-3 AU-4 AU-5 AU-6 AU-7 AU-8 AU-9 AU-10 AU-11 AU-12 AU-13 AU-14 AU-15 AU-16	10.1 10.2 10.3 10.6.1 10.6.2	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C) 164.310(a)(2)(iv) 164.310(d)(2)(iii) 164.312(b)	IVS-01 IVS-02	
Collection	Roles and responsibilities for order of operation are well defined to ensure accountability		AU-1			SEF-03	
Collection	Detection activities comply with all applicable requirements	A.18.1.4 A.18.2.2 A.18.2.3	AC-25 CA-2 CA-7 SA-18 SI-4 PM-14		164.308(a)(1)(i) 164.308(a)(8)	IVS-01	Article 32

Service Name: Security Monitoring							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Collection	Cyber threat intelligence is received from information sharing forums and sources	A.6.1.4	SI-5 PM-15 PM-16	6.1			
Fusion	Event data are aggregated and correlated from multiple sources and sensors	A.12.4.1 A.16.1.7	AU-6 CA-7 IR-4 IR-5 IR-8 SI-4	10.1 12.10.5	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.308(a)(8) 164.310(d)(2)(iii) 164.312(b) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii)		
Fusion	Malicious code is detected	A.12.2.1	SI-3 SI-8	v3.2 5 (all)	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)		
Fusion	Unauthorized mobile code is detected	A.12.5.1 A.12.6.2	SC-18 SI-4 SC-44	v3.2 5 (all)	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)		
Analysis	Detected events are analysed to understand attack targets and methods; accordingly, triage is conducted	A.12.4.1 A.16.1.1 A.16.1.4	AU-6 CA-7 IR-4 SI-4	10.6.1 11.4 12.5.2	164.308(6)(i)	IVS-13	
Analysis	Impact of events is determined	A.16.1.4	CP-2 IR-4 RA-3 SI-4	12.5.2	164.308(a)(6)(ii)		

Service Name: Security Monitoring							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Analysis	Incident alert thresholds are established	A.16.1.4	IR-4 IR-5 IR-8	12.5.2	164.308(a)(6)(i)		
Analysis	Monitoring for unauthorized personnel, connections, devices, and software is performed	A.12.4.1 A.14.2.7 A.15.2.1	AU-12 CA-7 CM-3 CM-8 PE-3 PE-6 PE-20 SI-4	10.1 10.6.1 11.1 11.4 11.5 12.10.5	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.310(d)(1) 164.310(d)(2)(iii) 164.312(b) 164.314(b)(2)(i)	IVS-06	
Analysis	The network is monitored to detect potential cybersecurity events		AC-2 AU-12 CA-7 CM-3 SC-5 SC-7 SI-4	10.6.1 11.4	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(8) 164.312(b) 164.312(e)(2)(i)		
Analysis	The physical environment is monitored to detect potential cybersecurity events	A.11.1.1 A.11.1.2	CA-7 PE-3 PE-6 PE-20	9.1.1	164.310(a)(2)(ii) 164.310(a)(2)(iii)		

Service Name: Security Monitoring							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Analysis	Personnel activity is monitored to detect potential cybersecurity events	A.12.4.1 A.12.4.3	AC-2 AU-12 AU-13 CA-7 CM-10 CM-11	9.1.1	164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A) 164.308(a)(5)(ii)(C) 164.312(a)(2)(i) 164.312(b) 164.312(d) 164.312€		
Analysis	Vulnerability scans are performed	A.12.6.1	RA-5	11.2	164.308(a)(1)(i) 164.308(a)(8)	IVS-05	
Analysis	External service provider activity is monitored to detect potential cybersecurity events	A.14.2.7 A.15.2.1	CA-7 PS-7 SA-4 SA-9 SI-4	8.1.5	164.308(a)(1)(ii)(D)		
Action	Event detection information is communicated to appropriate parties	A.16.1.2 A.16.1.3	AU-6 CA-2 CA-7 RA-5 SI-4	12.1	164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii)	SEF-03	
Action	Detection processes are tested	A.14.2.8	CA-2 CA-7 PE-3 SI-3 SI-4 PM-14	10.6.1 10.9 11.4 11.5 12.10	164.306(e)		
Action	Detection processes are continuously improved	A.16.1.6	CA-2 CA-7	12.1	164.306(e) 164.308(a)(8)		

Service Name: Security Monitoring							
Process Phases	Activities/Controls	Controls Reference — ISO/IEC 27001:2013	Controls Reference — NIST SP 800-53 Rev. 4	Controls Reference — PCI DSS 3.2	Controls Reference — HIPAA	Controls Reference — Cloud Security Alliance (CCMv3.0.1)	Controls Reference — GDPR
			PL-2 RA-5 SI-4 PM-14				

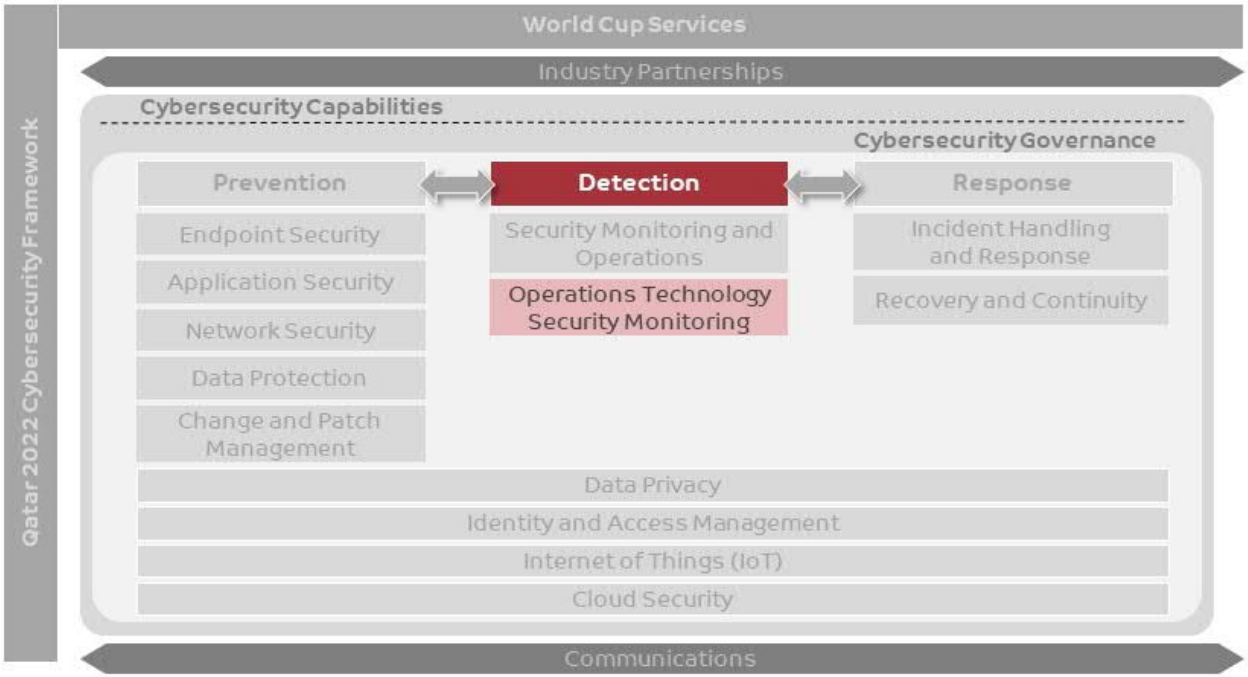
9 Operations Technology Security Monitoring

9. Capability Description – Operations Technology Security Monitoring

A capability that assesses deficits in the current state of security architecture and influence meaningful changes that are continuously monitored for deviations from their expected security posture.

This chapter focuses on ‘Operational Technology (OT) Security monitoring’ capability is defined under the ‘Detection’ pillar of world cup cybersecurity capabilities. The systems in scope under OT are mission critical systems that underpins the national critical infrastructure operations such as water, oil and gas and electricity, this capability does not cover IOT eco-systems and modern IOT networks which are more focused on consumer and customer experience. It’s highly recommended to use this capability with the adoption of the Qatari national ICS security standard version 3.0 and above.

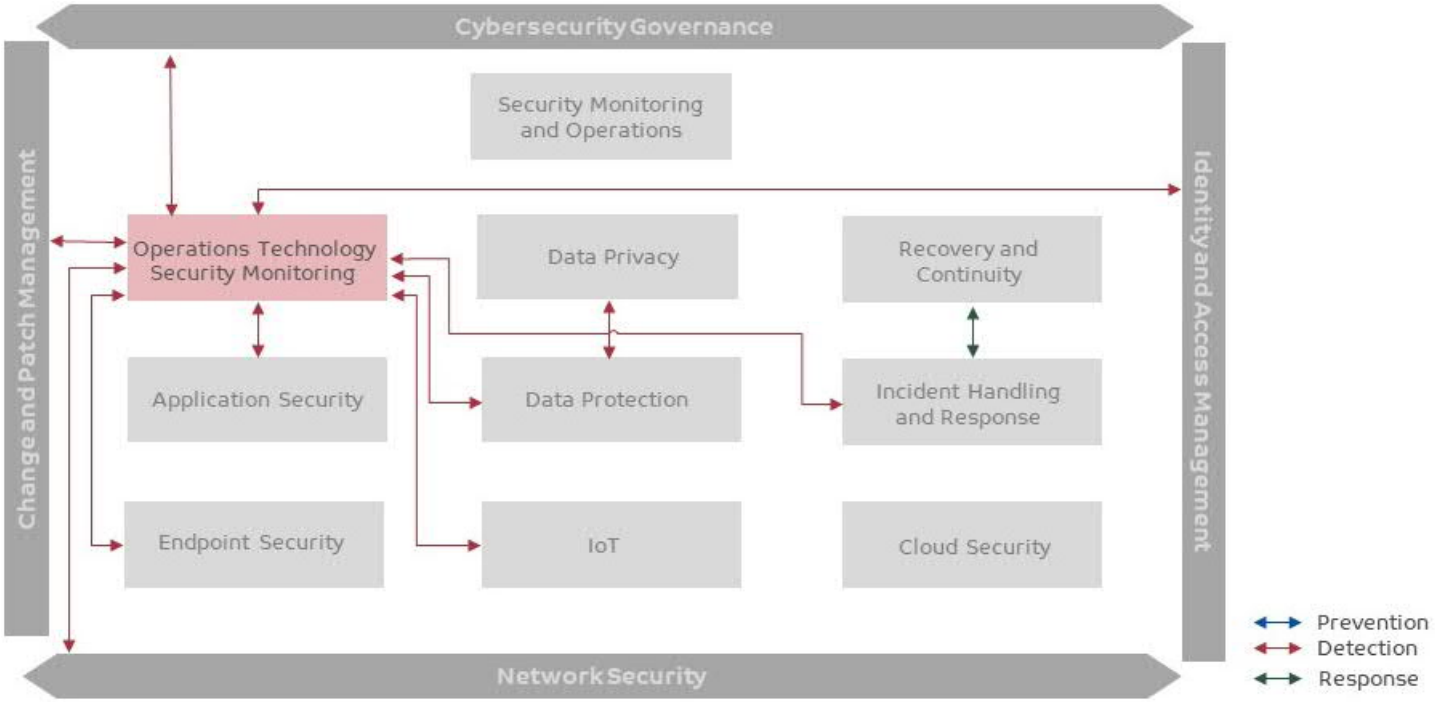
Figure 54: Cybersecurity capabilities – Operations Technology Security Monitoring



OT Security Monitoring is one of the most important capabilities within the information security portfolio to deliver cybersecurity services, especially due to its importance for ensuring the security posture of the mission critical systems that help us operate our critical infrastructure.

Following figure depicts linkage of OT security monitoring with other cybersecurity capabilities defined in the framework

Figure 55: Operations Technology Security Monitoring linkage with other capabilities



9.1 Prerequisites

Following are the prerequisites which are required to be accomplished prior to OT security monitoring:

- OT critical assets have been identified
- OT critical logs and security audit logs are identified for collection and analysis
- The appropriate logs have been enabled on the identified OT assets for collection and analysis (refer to other capability chapters such as network security and the Cybersecurity Governance chapter to help with risk assessment and asset identification)
- 3-tier OT layered architecture has been implemented, or at least the boundaries between the existing layers have been identified

- Plant network vantage points have been identified from where flow-based traffic and/or packet-based traffic will be collected (If supported by current network appliances). Specifically, on switches and/or VLANs configured which can help enormously for lateral movement detection
- Change management process in place to help in correlation of alerts with approved changes. The OT security monitoring team should be notified for scheduled changes and maintenance activities
- Confirm If any of the monitored assets have a mandatory safety requirement (SIL level) that should be maintained always
- OT Security Monitoring requires inputs from other capabilities such as SOC, Risk management for inputs that can improve monitoring such as IOCs, Threat intelligence etc.

9.2 Operations Technology Security monitoring service

From world cup perspective, the ***Table 54: OT Security Monitoring*** describes cybersecurity service that has been defined under this capability. However, from preparation/planning viewpoint, following steps must be completed:

- Establish the needed formal policies, procedures and guidelines
- Define OT monitoring program scope and identify target assets
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define severity classification and acceptance standards
- Set the OT log retention strategy (accommodating Shareholders requirements, Qatari Laws and NICS standard)
- Set a baseline of the OT environment network and systems behaviour “normalization process”
- Understanding of the safety implications of cyber security, this can be achieved by using industrial risk-based methodologies such as HAZOP to capture the implication of security on safety and production
- Deploy/configure appropriate solutions to align with establish standards
- Deploy and train team members to support
- Identify opportunities of automation where applicable
- Define services levels for remediation activity
- Define a format (for example: STIX, TAXII) to share analysed OT threat intelligence to various stakeholders
- Continually improve policy, procedure & guidelines with changing risks and lessons learned

Table 54: OT Security Monitoring

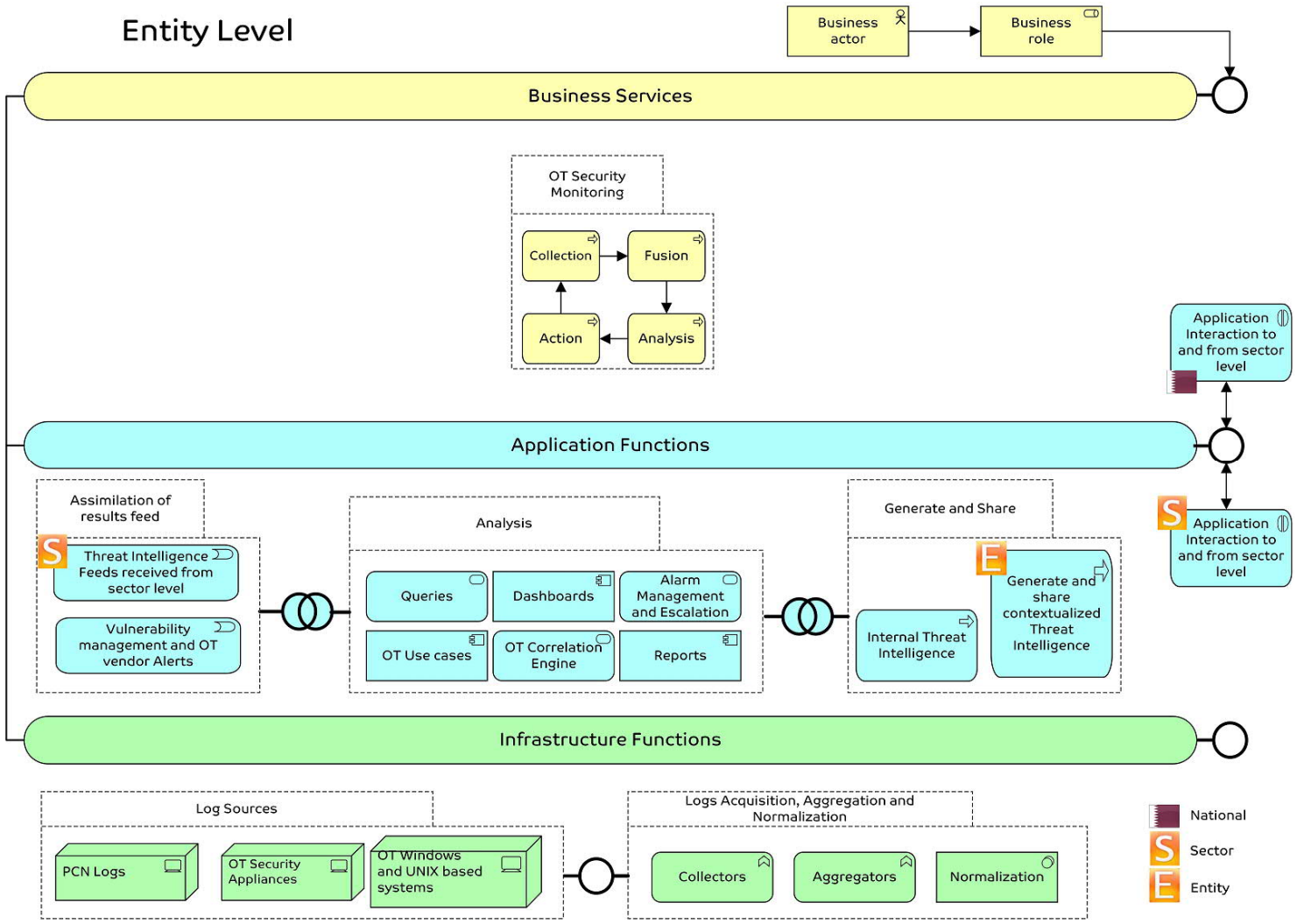
Service Name: OT Security Monitoring	
Description	OT cyber security monitoring is a proactive capability that ensures the reliable, safe and secure operations of the Operational Technologies (OT) utilized in the national critical infrastructures with respect to services provided to the world cup.
Process Phases	**Activities/Controls**

Service Name: OT Security Monitoring	
Collection *(Automatic)*	• OT environment logs identification (Sample list of OT logs included in the Compendium section) • Validate any reliability issues with OT vendors that may arise due to enabling logging (specially on legacy OT assets, network appliances) • Automate the collection to a central logging system (ideally within layer 3 as per the ISA99/IEC62443 model) • Fine tune the collected logs and apply enriching techniques such as linking the OT asset management system • Automate a process of collecting IOCs and threat intelligence • Subscribe to and collect threat feeds from public and community resources (free as well as commercial) • Collect any planned changes to the Industrial Process logic with help of team responsible for 'Change and Patch Management' activities (refer Change and Patch Management capability chapter)
Fusion *(Automatic)*	• Integrate and correlate (usually in OT industrial protocols capable SIEMs) • Set up use cases and rules as per planned policies • Ingest OT IOCs and Attack signatures
Analysis *(Semi-Automatic)*	• Test the Pre-set rules to ensure quality and effectiveness • Investigate alerts and conduct triage • Analyse deviations from the agreed network baseline (Cyber analytics) • Analyse new OT threat feeds and verify applicability to your systems and environment
Action *(Mostly Manual)*	• Escalation of alerts • OT Incident containment and management in alignment with operational and plant safety requirements • Reporting channels horizontally and vertically • Vendor secure communication • Initiate change management (Post remediation)

9.3 OT Security Monitoring Capability Model

Following figure illustrates an architecture model of various functions established for OT Security Monitoring at entity level:

Figure 56: OT Security Monitoring Capability Model



Above figure defines the OT Security Monitoring capability model in layered approach:

- **The Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- **The Application Functions layer** supports the business layer with application services which are realized by (software) application components.

- **The Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

9.4 Information Flow in various levels

Cybersecurity services defined under this capability are tightly coupled with the similar services running at sector and national level. All the identified threats and risks targeting at the world cup services and associated with OT systems, must be shared (bi-directionally) with sector and national level.

9.4.1 Services expected at each level

Following table describes services expected at each level of world cup ecosystem:

Table 55: Services expected at each level – OT Security Monitoring

Entity	Sector	National
• OT log collection and monitoring • OT Incident containment • Threat Intelligence (Implementation) • Integration of the OT threat event feeds and dashboard with the entity existing IT security monitoring function.	• Threat Intelligence - OT vendor communication - Disseminating vulnerability assessment results - Sharing feeds and intel with Entities in their sector	• OT Incident Handling and Response • OT Forensics • National level Threat Intelligence - Collation - Contextualization for country and sector level - Sharing with sector level

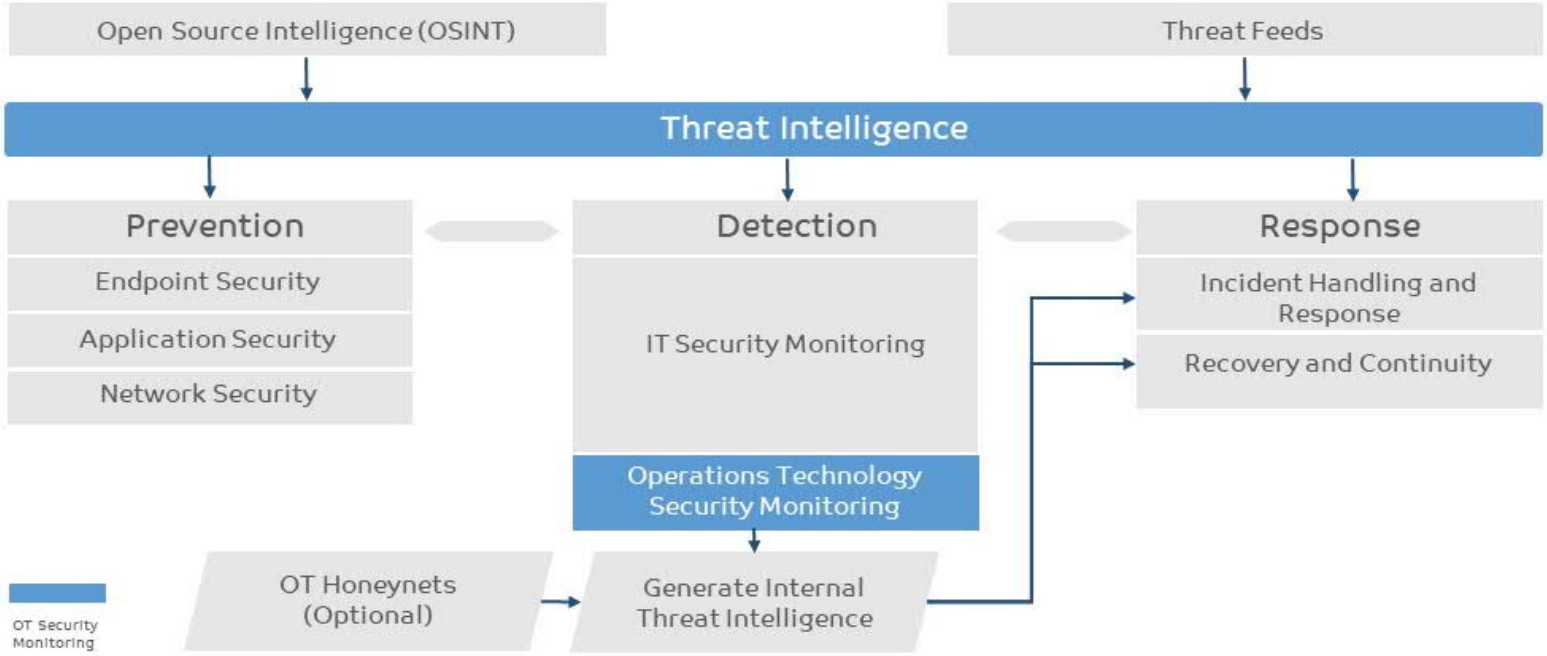
9.5 Milestones

Following milestones have been defined for OT security monitoring:

- Confirmation of critical OT systems to be monitored
- The OT systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures (at least every 60 minutes)
- Anomalous activity is detected in a timely manner (Ideally in near real time) and the potential impact of cyber event on (Operations and Safety) is understood

9.6 Information Flow among various activities under OT Security Monitoring

Figure 57: Information Flow in OT Security Monitoring



Above figure shows graphical representation of the information flow among various activities of OT security monitoring:

- OT threat intelligence is contextualized as applicable
- Contextualized OT threat intelligence is implemented on prevention, detection functions of cybersecurity
- Internal threat intelligence is derived from security monitoring and operations technology security monitoring activities
- OT vendor alerts are system and vendor specific security alerts issued by major OT vendors, applicable alerts need to be ingested into the monitoring process
- OT honey nets is an *optional method* to generate internal, entity relevant threat intelligence, this can be placed internally (within the DMZ) or internally at layer 2 in the OT network to general potentially capture malicious traffic crossing from the IT side or already traversing within the PCN (Process Control Network)

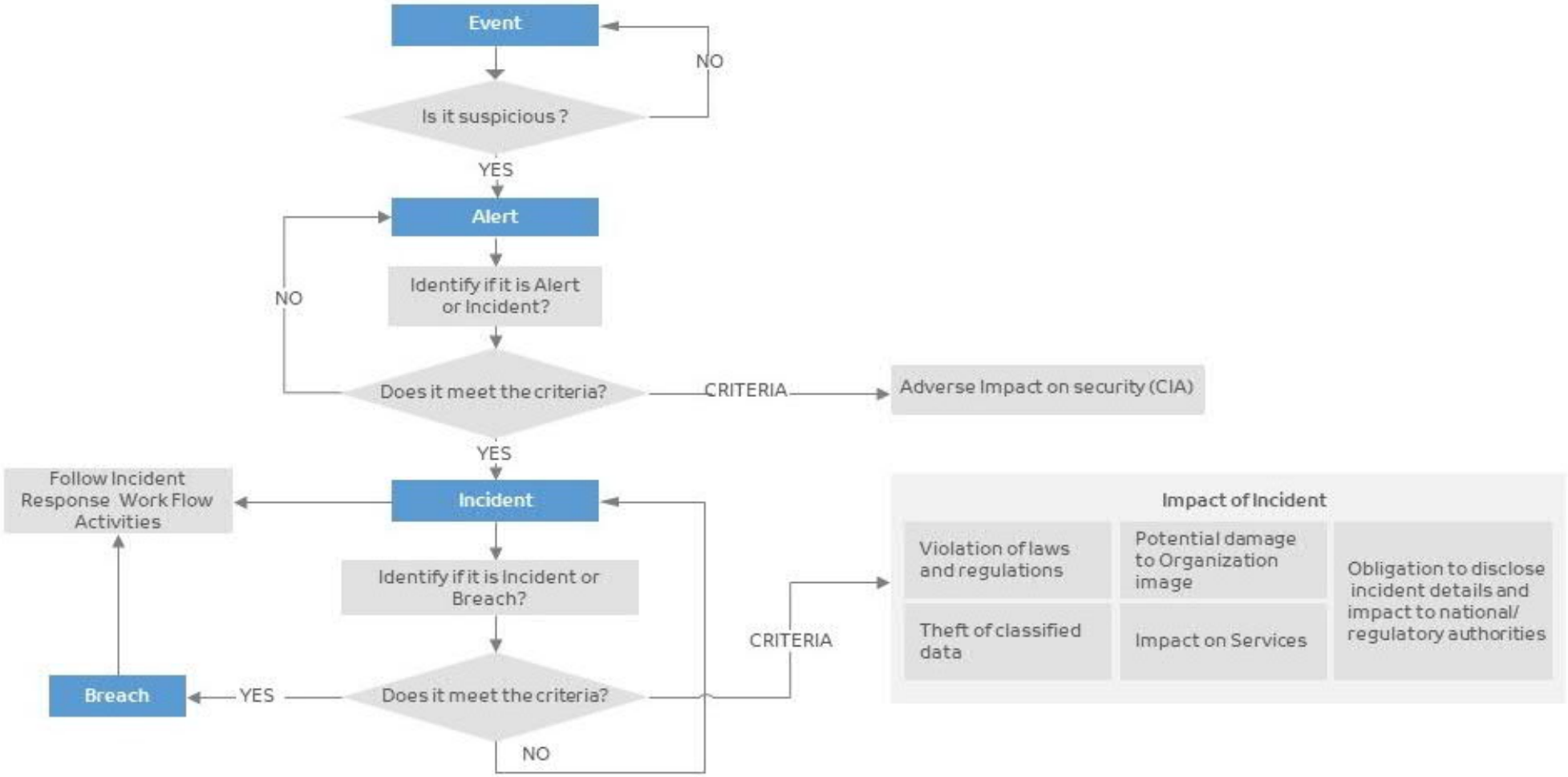
9.7 Criteria to categorize Event/Alert/Incident/Breach

Following are some the important definitions that needs to be considered while defining the categorization criteria:

- **Event:** An action marked, logged to a point in time that may require additional assessment
- **Alert:** a notification that a change is observed to the normal behaviour of a system/environment/process/workflow
- **Incident:** an adverse event that compromises Confidentiality, Integrity or Availability of an information asset, and has been verified as a potential threat. In the context of OT this means:
  - **Production incident:** Refers to any event that may indicate partial or severe impact on the plant uptime or production capacity
  - **Safety incident:** Refers to any event that may indicate a potential threat to personnel health and safety or the environment (HSE), or an incident that targets the plant safety systems
- **Breach:** an incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party.

Following figure defines the criteria that needs to be followed for categorization among alert/event/incident/breach

Figure 58: Criteria to categorize Event and Incident



9.8 Skills required for OT Security Monitoring

Following are the skills expected from personnel executing OT Security Monitoring activities:

- Solid Knowledge of the OT and ICS security domains
- Capable of Evaluating the cyber risks to SCADA, DCS, Smart Grids, DMS, and ECS systems architectures for instance
- Solid knowledge of Industrial networking protocols security such as DNP3, Modbus, Profinet, ZigBee, IEC 104 etc.
- Knowledge of OT Capable SIEM, security events logging and monitoring technologies
- Awareness of Network monitoring technology platforms
- Solid understanding of applicable best practices and security standards such as NERC-CIP, ISA99 (IEC 62443), NIST 800-82, Qatar's National ICS security standard etc.
- Good understanding of plant Process systems, plant safety and plant integrity systems and solutions
- Performing event analysis by correlating data from various sources
- Possess knowledge on log management & correlation, logs generated by various applications or appliances of OT infrastructures
- Competent to create custom signature/rules for detection and prevention technologies being used in the plant environment
- Ability to create various use cases based on environment for better detection of anomalies
- Should be able to conduct vulnerability assessments
- Provide support to Incident Response team for collecting evidences and in motoring of mitigation steps
- Should be able to identify gaps in detection processes

Suggested professional certifications which can help personnel to attain skills for the services defined under security monitoring and operations:

Table 56: OT Security Monitoring suggested certifications

Category	Suggested Certifications
Security Monitoring	• SANS GIAC Continuous Monitoring Certification (GMON)
Threat Intelligence	• SANS GIAC Cyber Threat Intelligence (GCTI)
OT Fundamentals	• SANS GIAC Global Industrial Control Systems Professional (GICSP) • ISA99/IEC62443 certified implementer
Security Analysis (General)	• EC-Council Certified Ethical Hacker (CEH), • SANS GIAC Certified Enterprise Defender (GCED) • SANS GIAC Security Essentials (GSEC) • SANS GIAC ICS Active Defence (515)

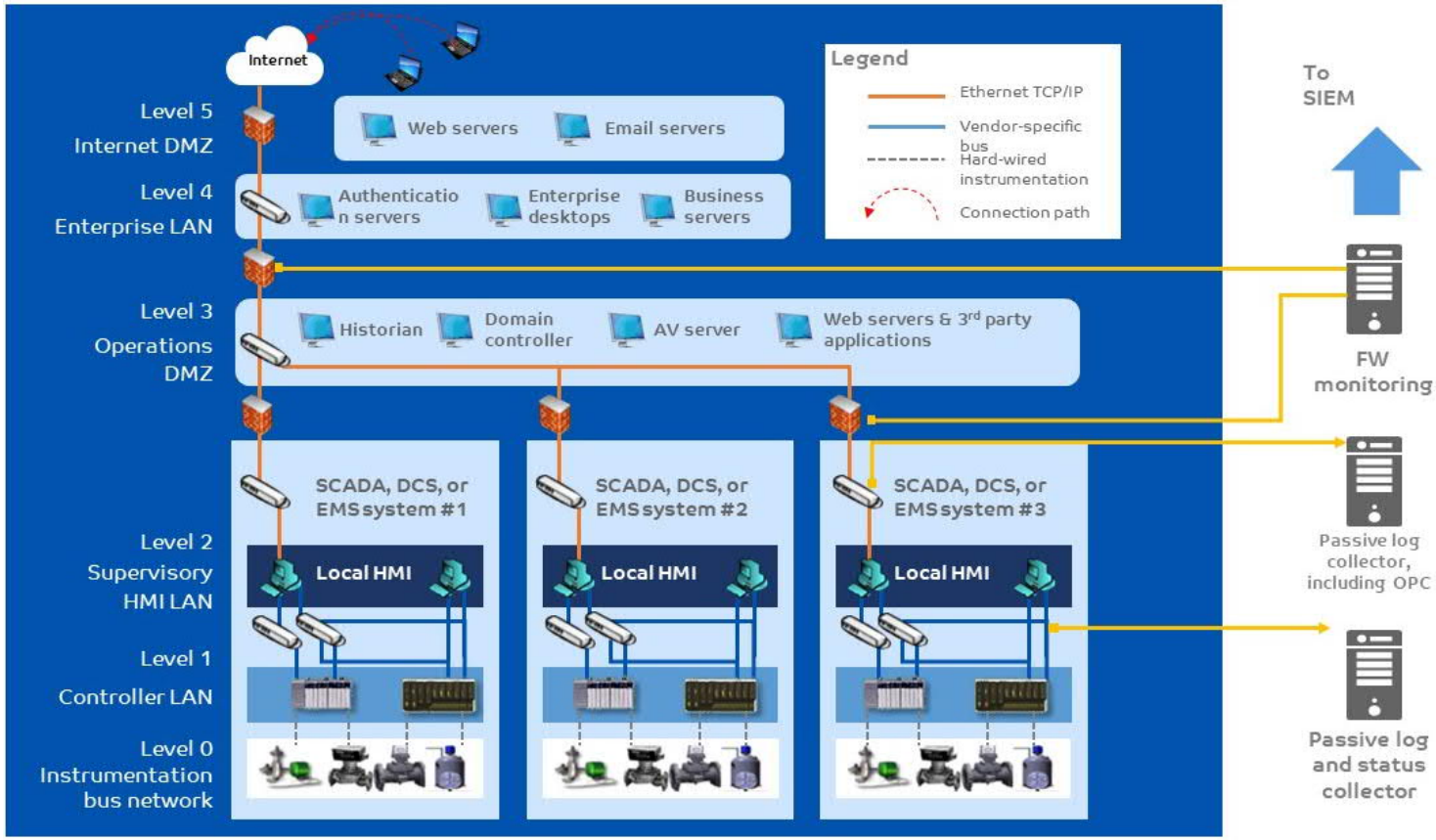
9.9 Architecture and Technology

Since OT logs are collected and retained for monitoring purposes, the below diagram highlights the proposed log sources that should be aggregated for centralized analysis. An OT SIEM platform can be significantly useful to conduct such analysis. Following sections briefly discuss about OT SIEM.

Also, the below OT model architecture (Based on ISA99/IEC 62443 standard) is the recommended layered approach across the various levels of a typical OT environment, for proper monitoring capability the entities should have the visibility and access to logs as per the graph below.

Note: The logs and status collection should be done passively. This should not affect production or conflict with any safety requirements.

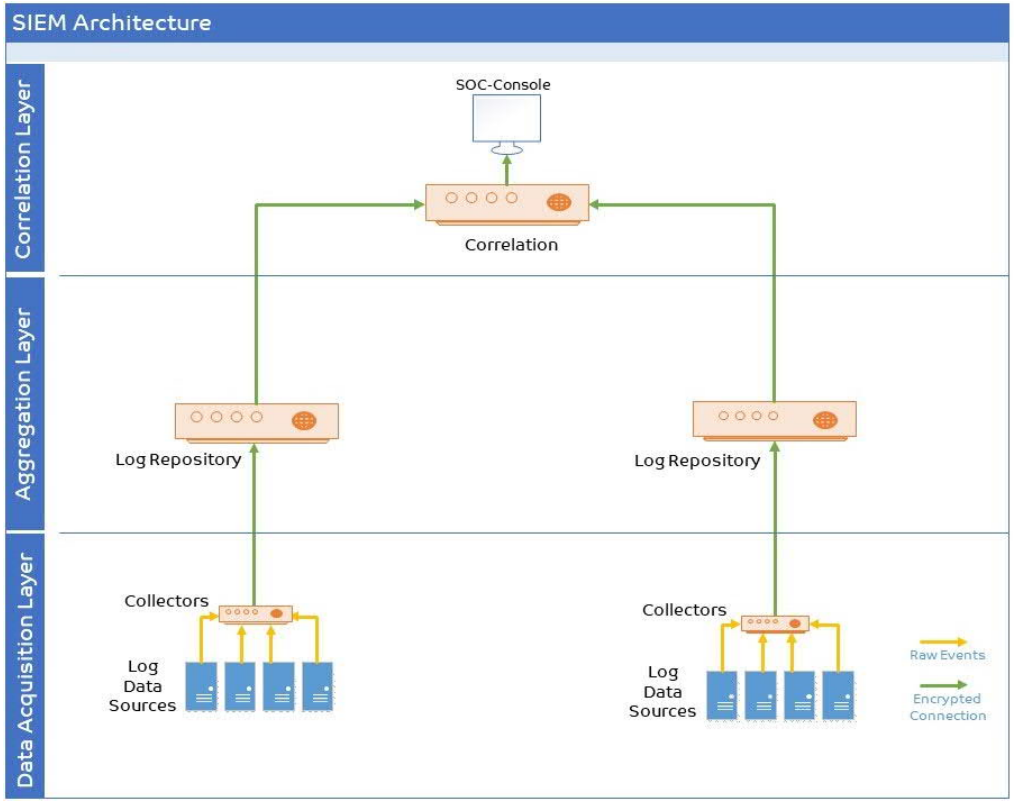
Figure 59: Vantage points for OT log collection



9.10 OT SIEM Architecture

The following figures shows high level OT SIEM Architecture that can be followed for implementation:

Figure 60: High Level OT SIEM Architecture

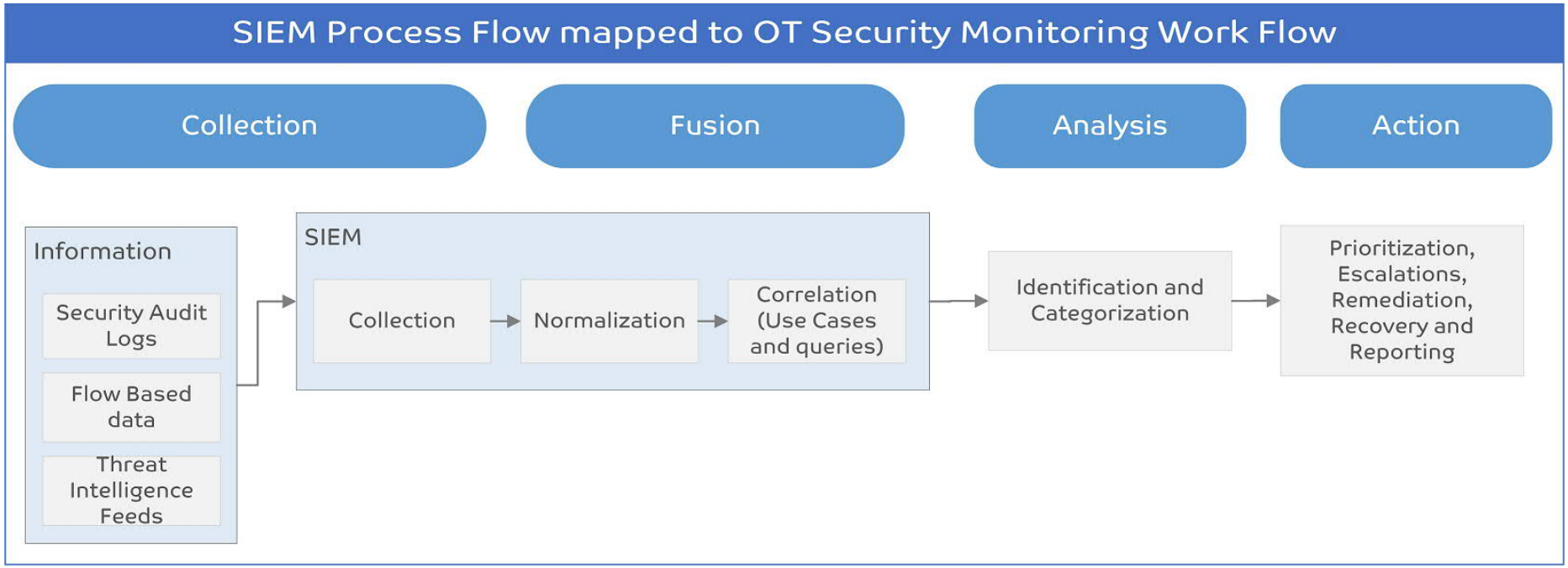


As shown in figure above:

- At data acquisition layer Collectors will collect the logs from all identified OT log sources, normalize and categorize in common format (*collection from layer 1 and above*)
- At aggregation layer Log repository will collect the data and store with capabilities of searching & reporting at an asset level (ideally *at layer 2*)
- At correlation layer data collected in all log repositories will be correlated with meaningful use cases across the OT environment (*Ideally at layer 3*)

Following figure shows the mapping between OT SIEM work flow and OT Security Monitoring activities:

Figure 61: SIEM workflow mapping with OT Security Monitoring activities



Above figure depicts:

- **Collection**: it defines the systematic approach to gather timely and relevant information from logs, flow-based data, and Threat Intelligence feeds
- **Fusion**: the information will be normalized and correlated
  - Normalization uses standardized queries to evaluate data from multiple resources and isolate signs of anomalous or malicious activity. It transforms data from disparate sources and reorganizes it such that data is consistent and the dependencies & relationships within the data are logical
  - Event correlation defines the process of identifying the relationships between data. It can identify relationships between events on different devices throughout the network. This provides visibility and allows the security operations team to identify and respond to events that indicate security threats
- **Analysis**: at this stage analysis is being done
  - Analysis will determine the relevance of an event and confirming its criticality
- **Action**: this is the stage where actual response actions will be initiated
  - Prioritize the response actions based on the urgency to the identified event
  - All relevant stakeholders will be notified
  - In case of alert, Security Monitoring Team will execute response actions
  - Containment and remediation actions will be implemented with various teams' support including Incident Response Team and Operations Team

9.11 Sample of OT security tools and appliances

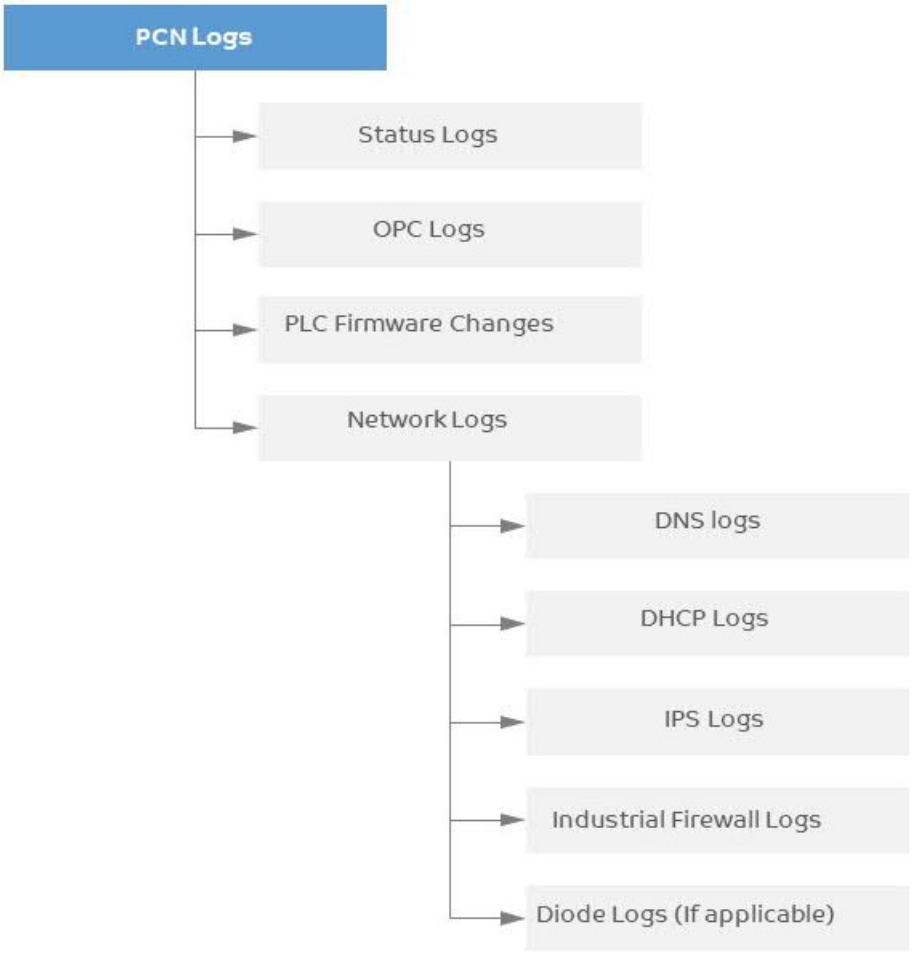
Table 57: OT Security Monitoring tools and appliances

Type of Tool	Features Required from OT security monitoring perspective
Passive Packet Capture	• Read and write to packet capture files • Distil packet capture files to other formats for more practical analysis. This offers, fast analysis against the distilled source data, while retaining the original packet capture file for in-depth analysis and extraction
Active scanning	• If technically permissible and after approval from the OT OEM vendors, specially, on the windows-based OT assets and for improved end-point security • Active scanning for missing operating system patches • Active scanning for Operating system configuration and registry changes
Historian Logs analysis tool	• Collect, parse and represent the collected data with a focus on “Status data” • Provide query-based search for specific investigations • Provision to save specific duration of data either local or on network location. • Provision to export such data
OT SIEM	• A centralized log aggregator and correlation engine • Capable of understanding and inspection of Industrial network protocols such as IE104, DNP3, Modbus, Profaned, Zigbee, and ISA100…etc. • Capable of collecting SNMP and security event logs from Network based services and appliances • Should support syslog log format • Provision to export specific duration of log data
Operating System Based logs	• Collect and parse memory dump, file system and current network communications logs • Sort logs with time of event for timeline analysis • Provision to export to other formats for more practical analysis
OT Server Logs	• Provision to export log data to the central logging server • Provision to export specific duration of logs
OT Engineering Workstation Logs	• Provision to export log data to the central logging server • Provision to export specific duration of logs
OPC Logs	• Support OPC logs collection • Supports multiple profiles of OPC connected devices • Provision to export OPC log data to the central logging server

Type of Tool	Features Required from OT security monitoring perspective
Industrial firewalls Management system	• Provision to export log data to the central logging server • Provision to export specific duration of logs
Remote access logs	• Provision to export log data to the central logging server • Provision to export specific duration of logs
Plant Assets registers	• A solution capable of indexing and registering all the plant assets automatically • Should be technology and OT vendor agnostic • Should support Automated asset discovery
AV/IPS	• Security software and network detection tools that can support in identifying malware and malicious traffic based on known signatures • Provision to export log data to the central logging server • Provision to export specific duration of logs
OT Cyber Analytics	• Solutions capable of identifying OT network anomalies based on machine learning and network and behaviour baselining • Provision to export log data to the central logging server • Provision to export specific duration of logs

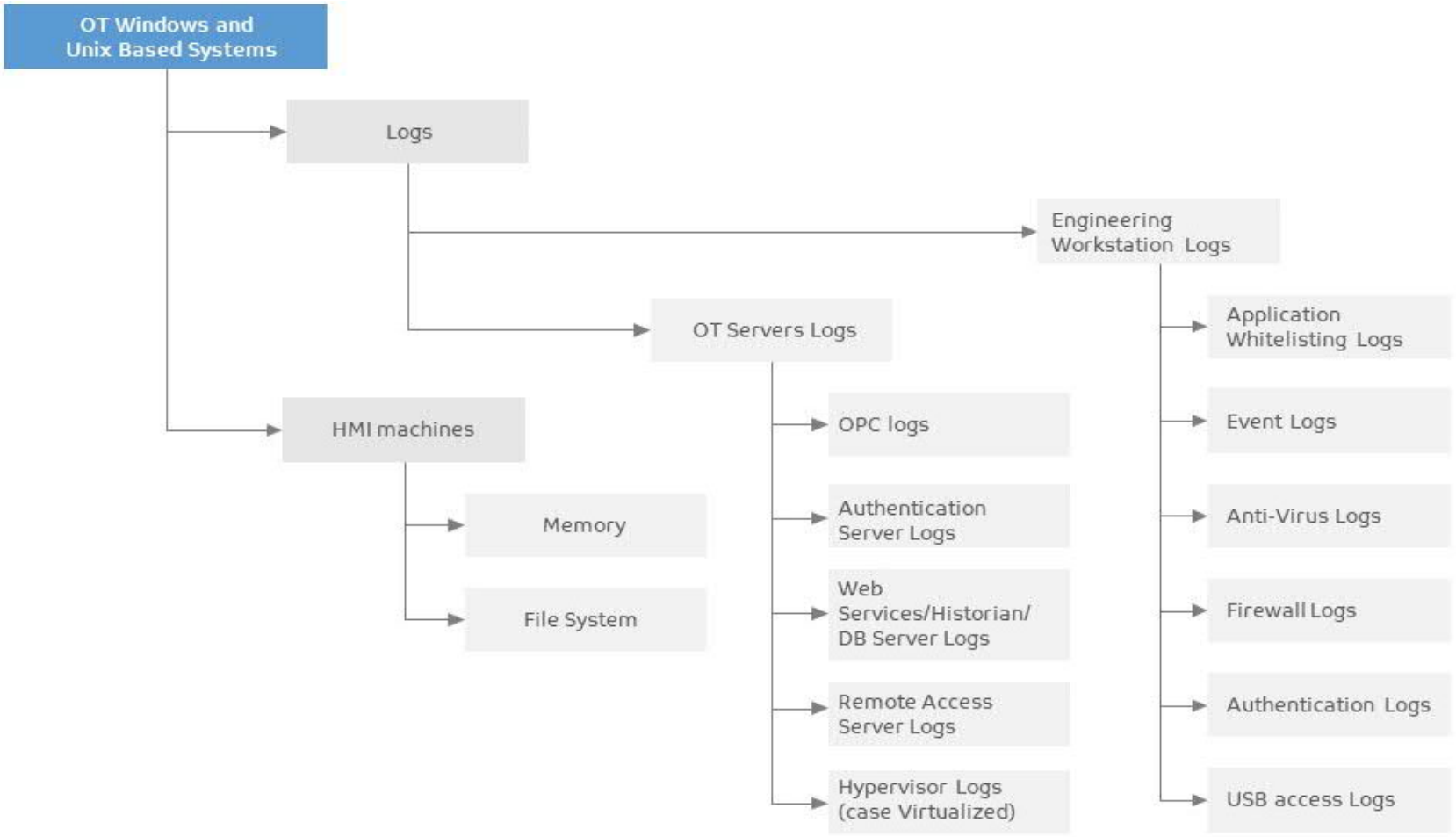
9.12 Sample OT Network Log sources

Figure 62: OT Network Log Sources



9.13 Sample OT Workstations and servers Log sources

Figure 63: OT workstation and server log sources



9.14 Use Cases

A Use Case is a Logical, Actionable and Reportable component for SIEM to monitor. It can be either a Rule, Report, Alert or Dashboard which solves a set of requirements.

9.14.1 Use Case Methodology

Use cases must be developed based on requirements. A fixed methodology must be used while working on a use case. High level steps would include:

Step 1: Information Gathering

- Understanding the flow of data and work-flow activities pertinent to the function being monitored by the given use case
- Identifying all the touchpoints involved, i.e. OT firewalls, IPS/IDS, network elements, PLCs and, asset servers and databases, etc.
- Aligning the criticality of aforesaid assets with the overall criticality of the business function being served by the use case at hand
- Identifying mandates and/or regulatory requirements whose purview the use case may fall under
- Identify report template
- Identify behavioural and historical inputs

Step 2: Defining Functional Content Design Points

- Define severity of alert to be raised in case the use case is triggered
- Define method of first alert to be raised in case the use case is triggered, i.e. dashboard alert, e-mail, etc.
- Define the reporting buckets in which this event would qualify to be compiled, i.e. daily, weekly, for a specific regulatory requirement, etc.
- Define filters to trap all constituent relevant (sub)events
- Define time and frequency factors for events to be considered a genuine advent of anticipated use case issue
- Define parameters based upon which sub-events would qualify to be a part of one set or another
- Define correlation and overlap points in order to merge multiple streams of sub-events
- Define master level meta-tags to facilitate correct category-based roll-up of use cases into larger groups for consolidated dashboards
- Define layout of dashboards and rendition of their constituent data monitors
- Define behavioural and historical holding structures

Step 3: Implementation of Functional Content in SIEM and Related SOC Sub-systems

- Create building block level filters and objects

- Create correlation rule(s)
- Implement alarm mechanisms
- Tie in with reporting templates
- Tie in with dashboards
- Tie in with external support sub-systems, e.g. trouble-ticketing system
- Implement resource allocation and management to ensure integrity of functional content

9.14.2 Sample OT Use Cases

Following are the use cases which entities may implement, and test results should be reviewed and can be validated by internal or outsourced professional services such as OT vulnerability assessment:

1. Creation, changing or deletion of multiple accounts in short amount of time
2. Disabling of engineering accounts
3. Adding of accounts to privileged groups and tracking of privileged account usage
4. Login of the same account from 2 different locations in a short space of time
5. Multiple system brute force for a single user
6. machine generating large volume of outbound traffic
7. Track removing of evidence such as deleting the audit logs
8. Unauthorized access to an engineering workstation
9. Monitoring of large or sensitive data copied to removable media and the use of removable media
10. Identify failed access attempts to sensitive data
11. Identify successful access after failed access attempts to sensitive data
12. Monitoring of plant user account privilege escalation
13. Monitoring of shared account utilization outside the normal time window
14. A sequence of a port scans within the PCN
15. Alerts raised by the OT IDS and IPS if technically supported.
16. Detection of traversing industrial protocols outside the plant network
17. Detection of industrial protocol-based connections initiated from outside the plant network
18. Detection of unplanned, unscheduled adding/removing of an asset into the environment
19. Detection of unauthorized changes into the approved, whitelisted applications inside the plant
20. Detection of unauthorized changes to any firmware inside the plant (will require asset management solutions)
21. Detection of OT protocols malformed packets and anomalous traffic flow

9.15 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards.

Table 58: Operations Technology Security Monitoring activities mapping industry cyber security standards

Service Name: OT Security Monitoring				
Process Phases	**Activities/Controls**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Collection	OT environment logs identification	6.6.10 6.9.1 6.9.2 6.9.3 6.9.4 6.9.5 6.9.6 6.9.7	4.3.3.3.9 4.3.3.5.8 4.3.4.4.7 4.4.2.1 4.4.2.2 4.4.2.4	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12
Collection	Validate any reliability issues with OT vendors that may arise due to enabling logging (specially on legacy OT assets, network appliances)			
Collection	Automate the collection to a central logging system (ideally within layer 3 as per the ISA99/IEC62443 model)	6.9.2		SR 6.1
Collection	Fine tune the collected logs and apply enriching techniques such as linking the OT asset management system			
Collection	Automate a process of collecting IOCs and threat intelligence	4.2.7 4.2.8	4.2.3 4.2.3.9 4.2.3.12	
Collection	Subscribe to and collect threat feeds from public and community sources (free as well as commercial)	4.2.7 4.2.8	4.2.3 4.2.3.9 4.2.3.12	
Collection	Collect any planned changes to the Industrial Process logic with help of team responsible for ‘Change and Patch Management’ activities			

Service Name: OT Security Monitoring				
Process Phases	**Activities/Controls**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Fusion	Integrate and correlate (usually in OT industrial protocols capable SIEMs)			
Fusion	Set up use cases and rules as per planned policies			
Fusion	Ingest OT IOCs and Attack signatures			
Analysis	Test the Pre-set rules to ensure quality and effectiveness			
Analysis	Investigate alerts and conduct triage		4.3.4.5.6 4.3.4.5.7 4.3.4.5.8	SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9 SR 6.1 SR 6.2
Analysis	Analyse deviations from the agreed network baseline (Cyber analytics)		4.3.4.3.2 4.3.4.3.3	SR 7.6
Analysis	Analyse new OT threat feeds and verify applicability to your systems and environment			
Action	Escalation of alerts		4.2.3.10	
Action	OT Incident containment and management in alignment with operational and plant safety requirements		4.3.4.5.6 4.3.4.5.10	SR 5.1 SR 5.2 SR 5.4
Action	Reporting channels horizontally and vertically		4.3.4.5.9	SR 6.1
Action	Vendor secure communication			
Action	Initiate change management (Post remediation)		4.4.3.4	

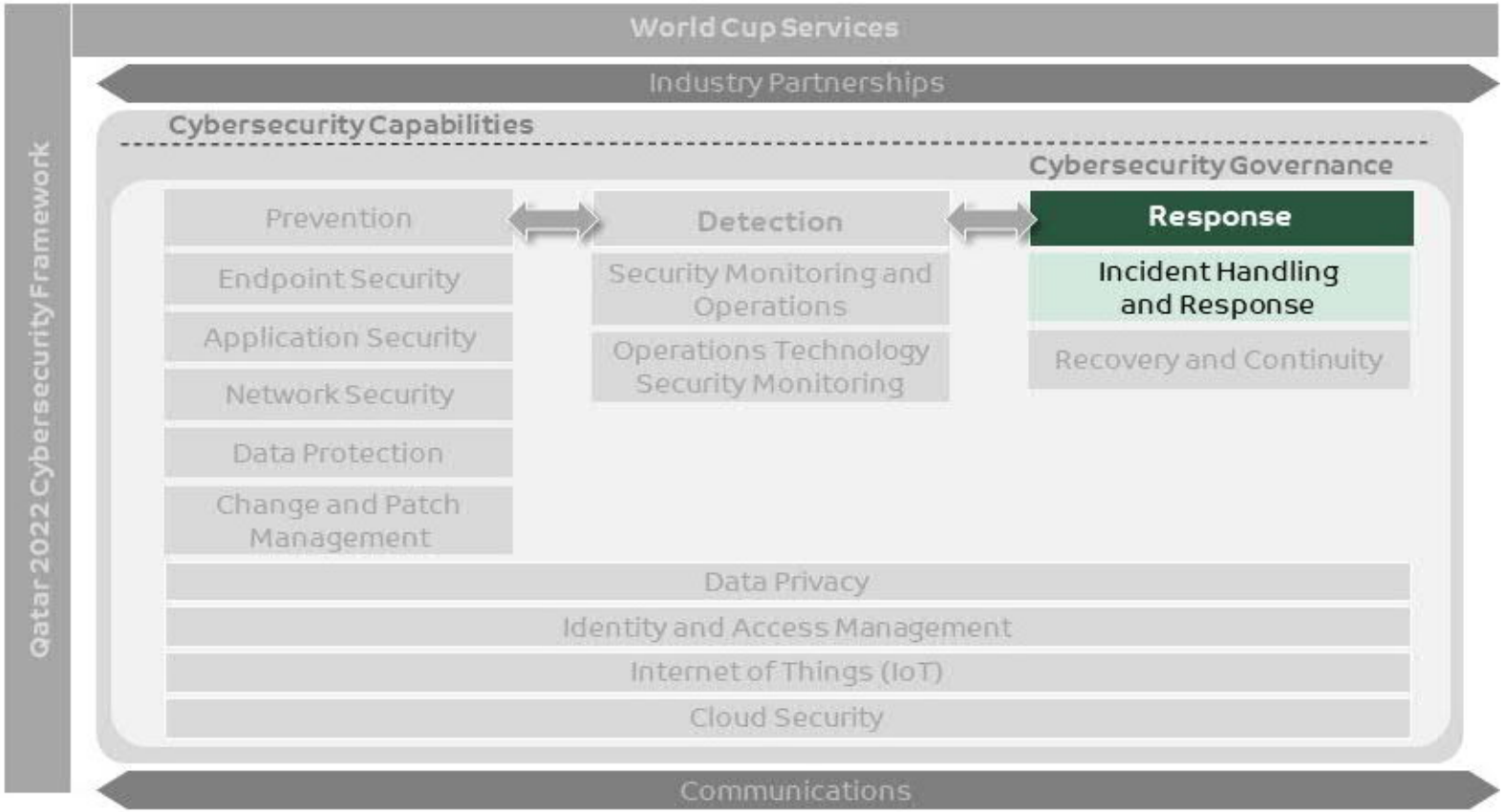
10 Incident Handling and Response

10. Capability Description- Incident Handling and Response

A reactive capability that addresses and manages effects of an attack or anomalous activity. It is an essential capability required to respond all incidents occur with respect to world cup services.

This chapter focuses on ‘Incident Handling and Response’ capability defined under the ‘Response’ pillar of world cup cybersecurity capabilities.

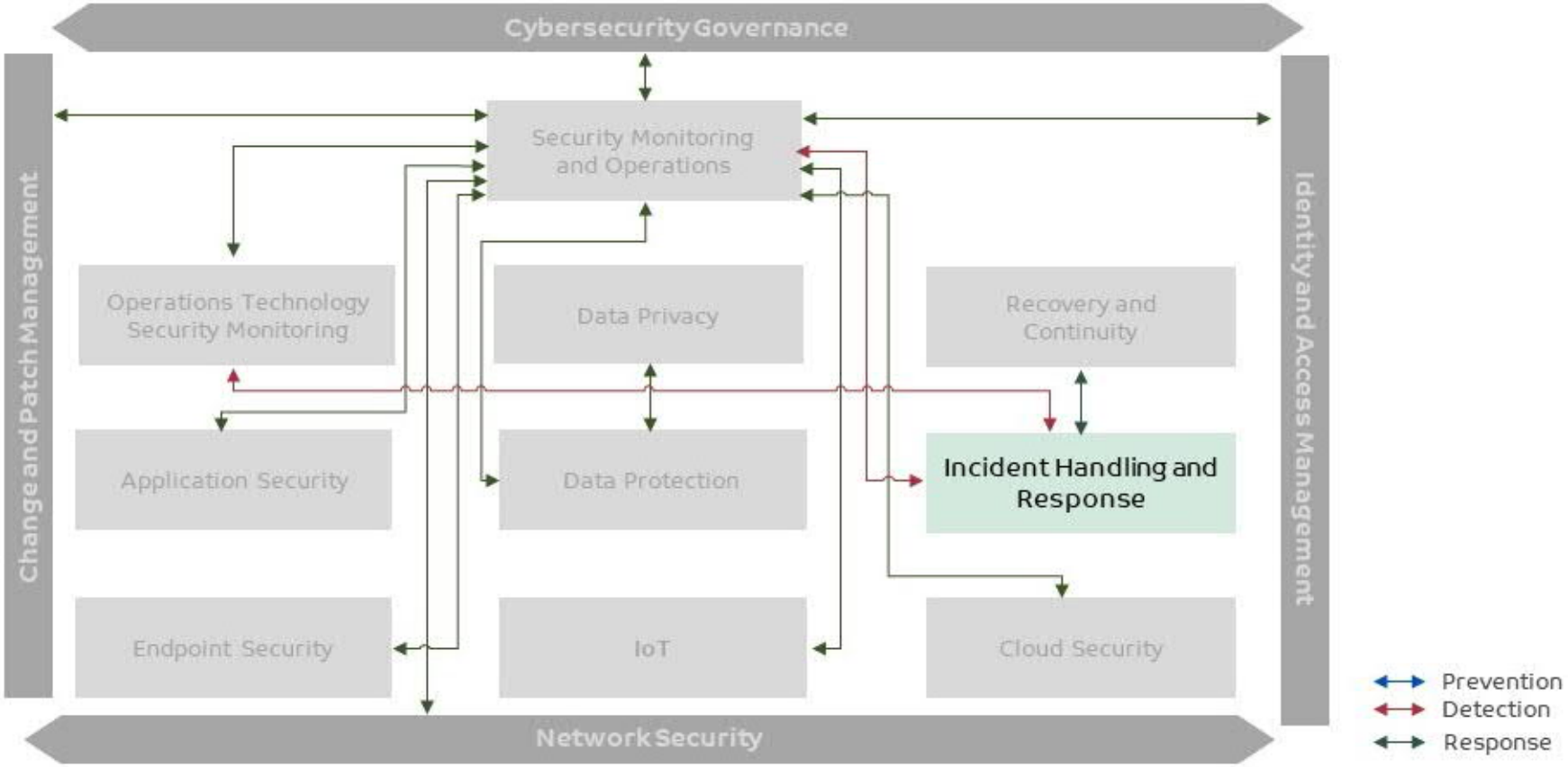
Figure 64: Cybersecurity capabilities – Incident Handling and Response



The team responsible for 'Incident Handling and Response' activities must work closely with teams responsible for 'Security Monitoring and Operations' and 'Operations Technology Security Monitoring' activities. Teams responsible for security monitoring activities DETECT the anomalous activities, categorize those activities in incident/breach and based on that process flow of 'Incident Handling and Response' is being triggered which RESPONSE to DETECTED events.

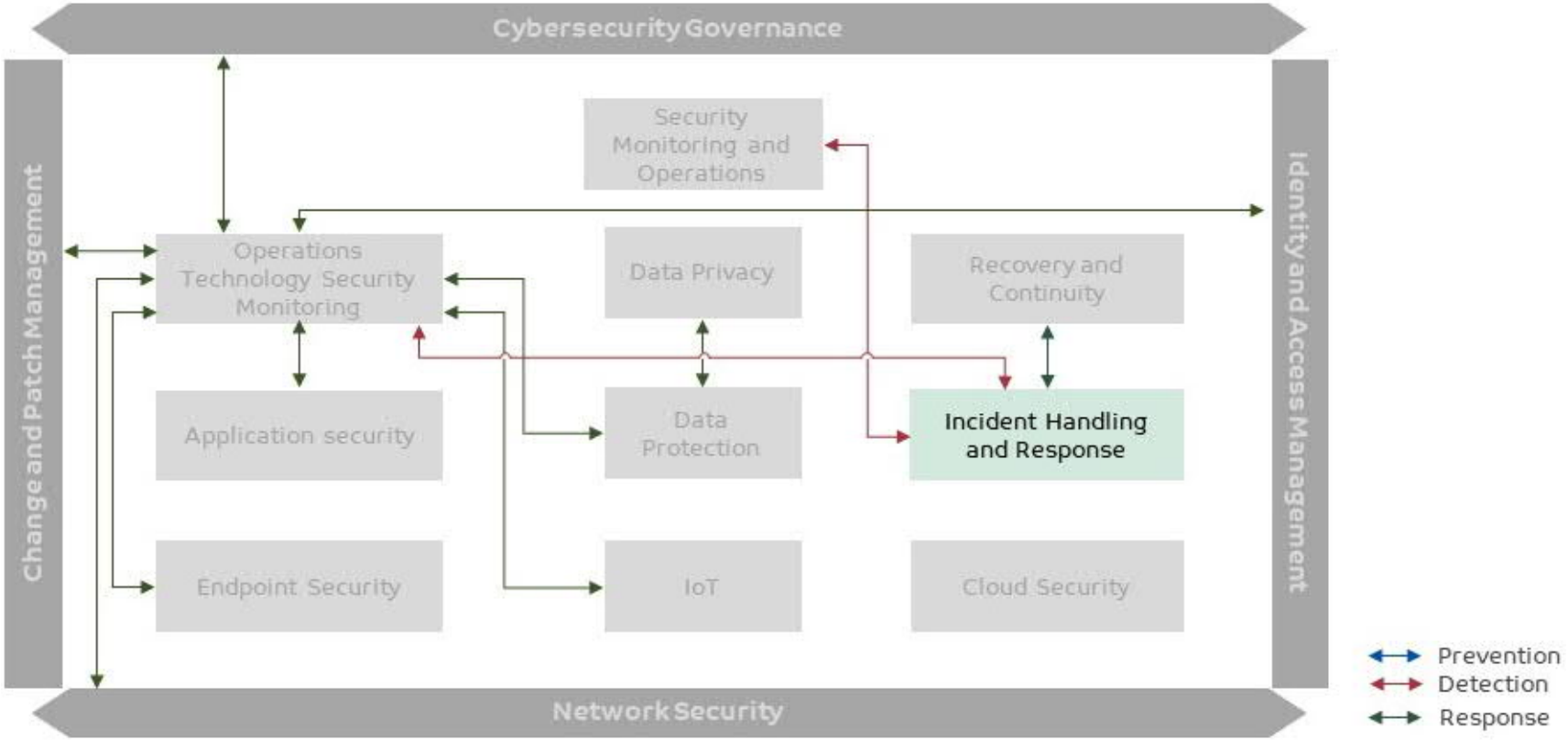
Following figure depicts linkage of Incident Handling and Response with other cybersecurity capabilities defined in the framework when the process flow is being triggered through ‘Security Monitoring and Operations’.

Figure 65: Incident Handling and Response linkage with other capabilities when process is triggered through Security Monitoring and Operations



Following figure depicts linkage of Incident Handling and Response with other cybersecurity capabilities defined in the framework when the process flow is being triggered through ‘Operations Technology Security Monitoring’.

Figure 66: Incident Handling and Response linkage with other capabilities when process is triggered through Operations Technology Security Monitoring



10.1 Prerequisites

Following are the prerequisites which are required to be accomplished for incident handling and response capability:

- Security audit logs have been collected on central logging server and analysed regularly (refer to security monitoring and operations capability chapter)
- Events are monitored & analysed to understand attack targets and methods including external vendors, partners and service provider activity
- Events are being monitored for third-party vendors
- Incident Response communication networks are protected (refer to network security capability chapter)
- Systems used by incident response team for incident communications are hardened (refer to endpoint security, data protection and data privacy capability chapter)
- SLAs have been defined with third-party vendors or service providers from service availability, support management and security requirements perspective
- Any changes to be implemented on information assets as response activities must go through change and patch management service (refer Change and Patch Management capability chapter)
- Security risks identified for the infrastructure, endpoints and applications during the risk assessment have been communicated team responsible for 'Incident Handling and Response'
- Out-of-band communication channels have been implemented for use in event if normal communication channels are presumed to be compromised

10.2 Various services under Incident Handling and Response capability

From world cup perspective, following sections describes cybersecurity services that have been defined under this capability and respective activities that needs to be conducted for each service. However, from planning viewpoint, following steps must be completed:

- Establish formal policies, procedures and guidelines
- Define program scope
- Define severity classification and acceptance standards
- Deploy/configure appropriate solutions and tools to align with establish standards
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Deploy and train team members to support
- Identify opportunities of automation where applicable
- Define services levels for remediation activity
- Define rules of engagement which will be followed
- Continually improve policy, procedure & guidelines with changing risks and lessons learned

10.2.1 Incident Handling and Response service

Following table describes activities established for Incident Handling and Response Service under this capability

Table 59: Incident Handling and Response Service

Service Name: Incident Handling and Response	
Description	A reactive capability that addresses and manages effects of an attack or anomalous activity. It is an essential capability required to respond all incidents occur with respect to world cup services.
Process Phases	**Activities/Controls**
Preparation	• Incident Response plans are prepared, in place and managed • Personnel know their roles and order of operations when a response is needed • Prepare Incident Response Contact List which should include contact information (phone numbers, mobile numbers, emergency contact numbers, email addresses, public keys etc.) of all internal and external stakeholders • Define a secure way of communication such as encryption software (Rights Management Servers/PGP Keys/Digital Certificates) for communication among stakeholders, especially external • Response plans are tested • Response planning and testing are conducted with critical suppliers/providers
Detection and Analysis	• Events are reported consistent with established criteria • Notifications from detection systems are investigated and triage is conducted • Incident Response plan is executed during or after an event • Incidents are categorized and assigned a criticality level consistent with response plans [refer **Error! Reference source not found.**] • The impact of the incident is understood [refer **Error! Reference source not found.**] • Malicious code is detected which have been identified as a part of analysis • Forensics are performed, where required, after getting authorization approval from management • Newly identified vulnerabilities are mitigated or documented as accepted risks • Information is shared consistent with response plans • Mechanisms shall be put in place to monitor, track and quantify the types and volumes of cyber security incidents • Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
Containment, Eradication and Recovery	• Incidents are contained • Incidents are mitigated • Coordination with stakeholders occurs consistent with response plans • Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

Service Name: Incident Handling and Response	
	• Recovery plan is executed during or after an event • Recovery activities are communicated to internal stakeholders and executive and management teams
Post-incident Activity	• Response plans incorporate lessons learned • Response strategies are updated • Recovery plans incorporate lessons learned • Recovery strategies are updated • Public relations are managed • Reputation after an event is repaired

10.2.1.1 Response plan testing

Response plan testing is an important step to verify defined procedures. Such testing activities can be conducted during the preparation phase which help entities to ascertain their readiness. It can also be conducted as post-incident activity as a part of response plan improvement.

The objective to conduct testing activities is to address identified gaps in defined response plans. Response plan testing should include all the stakeholders involved in execution of incident handling and response activities. It should update the following, but not limited to:

- Communication list of internal and external stakeholders
- Any team structure changes with respective responsibilities assigned
- Any procedural changes required

Following exercises will help to attain above mentioned objectives:

- **Table-top Exercise** — it is a paper-based exercise where participants' plays specific role and perform specific action given in simulated incident scenario following defined response plan
- **Cyber Drill Exercise** — it is a simulation-based exercise where controlled attack traffic is generated on specific targets. The participating teams must detect the attack, apply mitigations following defined response plan. There are national level cyber drill exercises conducted by QCERT, entities can take advantage of such exercises by participation
  - **Red Team/Blue Team Exercise** – This exercise comprises of two teams namely Red Team and Blue Team. Red Team uses real-world attacker techniques to compromise the environment, and a Blue Team, the responders use existing tools to identify, assess and respond to the intrusion
  - Entities can organize such exercises for their environment to check effectiveness of response plan implemented by them
- **Lessons learned meeting** — meeting with stakeholders involved in response activities post incident or breach, in which any gaps identified during the execution of activities should be discussed and addressed by improving the response plan

10.2.2 Digital Forensic Service

Following table describes activities established for Digital Forensics Service under Incident Handling and Response capability. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal policies, standards and guidelines
- Define program scope and identify target assets
- Define and assign roles and responsibilities
- Deploy and train team members to support
- Identify opportunities of automation where applicable
- Define services levels for remediation activity
- Define rules of engagement which will be followed

Table 60: Digital Forensics Service

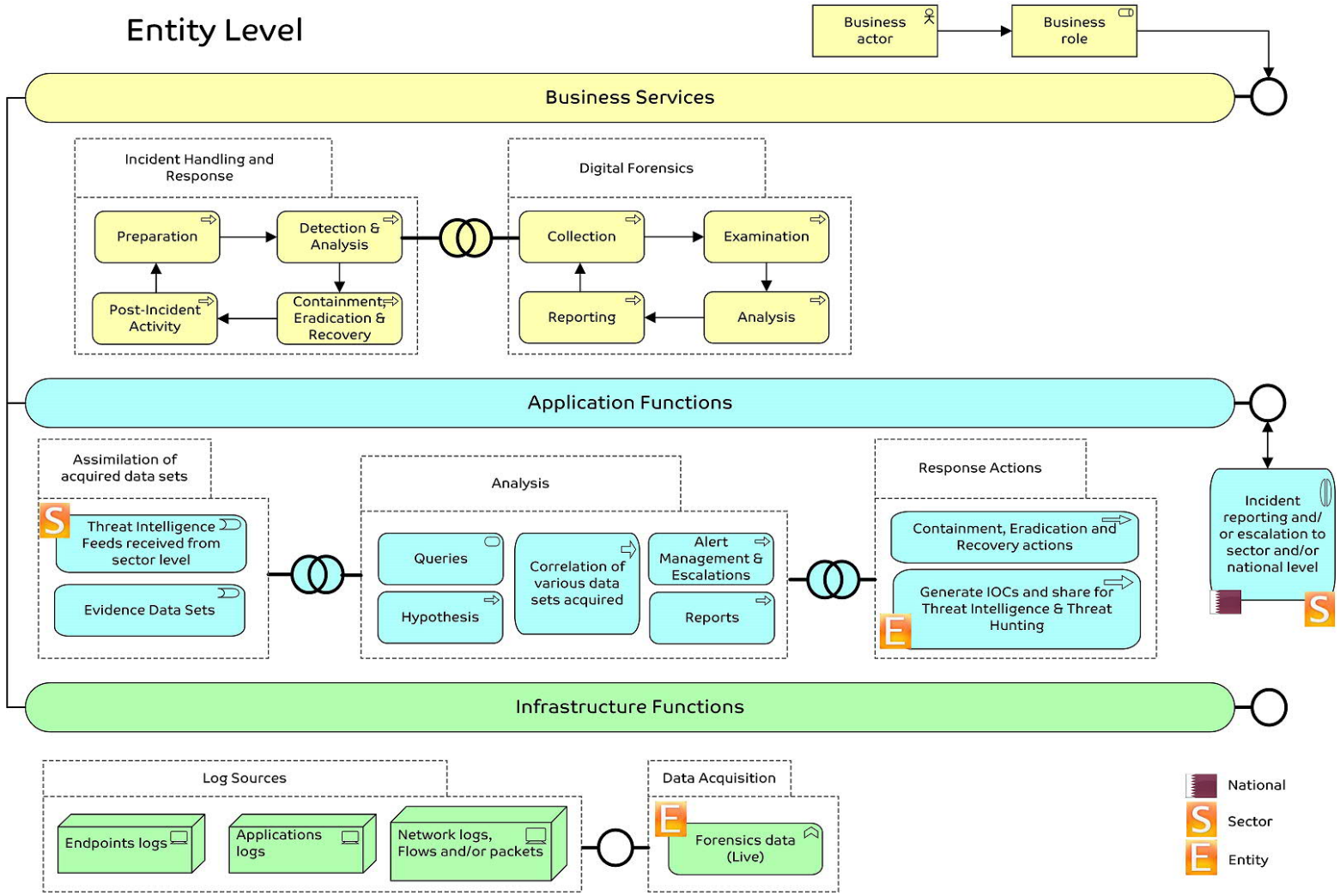
Service Name: Digital Forensics	
Description	Digital Forensics is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data This process has become an integral part of incident response while responding to the incidents. Data collection and analysis highly reliant on the procedures followed in this process. Primarily following two categories have been outlined to collect artefacts: • **Live Forensics**: Artefacts are being collected from running live and functional system. Typically followed to respond active adversary • **Post-Mortem Forensics**: Forensic Images are being created generally taking after system shutdown and analysis is being done on duplicate image which takes time: - Said procedure is generally followed when the evidences must be presented in court of law - In case, said procedure is followed, it is utmost important to follow chain of custody procedure ▪ Chain of custody refers to chronological documentation that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence ▪ For all such cases where post-mortem forensics must be conducted, entity will assist and follow instructions provided by either sector level or national level
Process Phases	**Activities/Controls**
Collection	• Identifying from the possible sources of relevant data • Acquiring data from identified sources • Label and record acquired data

Service Name: Digital Forensics	
Examination	• Forensically process collected data using a combination of automated and manual methods • Assess and extract data of interest
Analysis	• Analyse the results of the examination, using legally justifiable methods and techniques • Derive useful information that addresses the questions that were the impetus for performing the collection and examination
Reporting	• Report the results of the analysis, which may include description the actions used • Explain how tools and procedures were selected • Determine what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls) • Provide recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process

10.3 Incident Handling and Response Capability Model

Following figure illustrates an architecture model of various functions established for Incident Handling and Response capability at entity level:

Figure 67: Incident Handling and Response Capability Model



Above figure defines the Security Monitoring and Operations capability model in layered approach:

- **The Business service layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- **The Application Functions layer** supports the business layer with application services which are realized by (software) application components.
- **The Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

10.4 Information Flow in various levels

Cybersecurity services defined under this capability are tightly coupled with the similar services running at sector and national level. All identified incidents and breaches targeting at the world cup services and associated information assets, must be shared with sector and national level.

10.4.1 Incident information that should be shared (Reference Q-CERT Incident Information Form)

Following table describes the Incident Information Form defined by Q-CERT

Table 61: Incident Information required to be shared with Sector/National Level

Point of Contact Details	
Full Name (First Name Last Name)	
Designation	
Email	
Office Phone	
Mobile Phone	
Fax	
Incident Details	
Organization	
Sector	

Domain	
Incident Category	
Date of Incident	
Incident Priority	
Incident Description	
Affected Machine Name	
Affected Machine Time Zone	
Affected Machine Usage [Services provided]	
Determine Attack Source	
Attack Machine Name	
Attack Machine Time Zone	

10.4.2 Incident Categories Definitions (Reference Q-CERT)

During the Identification of the Incident Response work flow, once an event is categorized as incident, next step is to categorize it. Incident categorization is important from incident management and tracking perspective.

Following table defines the categorization of incident i.e. based on the nature of the incident it will be categorized in following defined categories.

Table 62: Incident Categories Definitions

Incident Categories	Incident Definition	Incident Types
Abusive Content	Refers to any illegal attempt that impacts loss of productivity or criminal activity	SPAM
		Harassment
		Child Abuse
Malicious Code	Refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or the confidentiality, integrity, and availability of the victim's data, applications, or operating system. Like a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host	Virus
		Worm
		Trojan
		Spyware
		Botnet
Information gathering	Refers to any attack that intercept and access information during transmission to be used in a subsequent attack	Scanning

Incident Categories	Incident Definition	Incident Types
		Sniffing
		Social Engineering
Intrusion attempts	Refers to any attempt trying to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardized identifier such as a CVE name (e.g., buffer overflow, backdoors, cross side scripting, etc.)	Exploiting known Vulnerability
		New Attack Signature
Intrusions	Refers to any unauthorized attempt to use of a computer account by someone other than the account owner	Account Compromise
		Web Compromise
Availability	Refers to any attack that makes a resource unavailable by initiating large numbers of incomplete connection requests. This type of attack overwhelms capacity, typically preventing new connections from being made	DOS Denial of Service Attacks
Information Security	Refers to any unauthorized access incident occurs when a person gains access to resources that the person was not intended to have. Unauthorized access is typically gained through the exploitation of operating system or application vulnerabilities, the acquisition of usernames and passwords, or social engineering	Unauthorized Access
		Unauthorized Modification
Fraud	Refers to any attempt for using resources for unauthorized purposes, including profit-making ventures (e.g., the use of e-mail to participate in illegal chain letters for profit or pyramid schemes). Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez). Or defines any type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it	Unauthorized use of resource
		Copyright
		Masquerade
Others	Refers to non-malware threats that are often associated with malware like phishing and virus hoaxes. Both phishing and virus hoaxes rely entirely on social engineering, which is a general term for attackers trying to trick people into revealing sensitive information or performing certain actions. Phishing refers to criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication	Phishing

10.4.3 Incident Criticality Classification (Reference NIA 2.0)

During the Identification phase of the Incident Response work flow, once an event is categorized as incident, incident is categorized as per table mentioned above, next step is to classify it as per severity level. Incident classification as per severity level is important from prioritization perspective, the process is called Triage. More severe the incident is, higher the priority should be given for mitigations.

Following table defines the criticality classification of incident i.e. based on the severity of the incident it will be classified in following defined categories.

Table 63: Incident Criticality Classification

Category	Typical Incident Categories
C1	• Denial of service • Compromised Asset (critical) • Internal Hacking (active) • External Hacking (active) • Virus/Worm (outbreak) • Destruction of property (critical)
C2	• Internal Hacking (not active) • External Hacking (not active) • Unauthorized access. • Policy violations • Unlawful activity. • Compromised information. • Compromised asset. (non-critical) • Destruction of property (non-critical)
C3	• Email • Forensics Request • Inappropriate use of property • Policy violations

As per NIA, there is a condition where entities must notify about incidents to Q-CERT in specified time limit based on its criticality. Use ***Table 64: Incident Matrix*** and ***Table 65: Response Matrix*** to define that stage.

Following table defines incident matrix which needs to be followed while defining the criticality of an incident and notifying to Q-CERT.

Table 64: Incident Matrix

Incident Matrix	C3	C2	C1
CSO+CII	CL1	CL1	CL3
CSO + Non CII	CL1	CL2	CL3
Non CSO + CII	CL1	CL2	CL3
Non CSO + Non CII	CL3	CL3	CL3

* CSO — Critical Sector Organization as defined in CIIP Law
* CII — Critical Information Infrastructure as defined in CIIP Law
* Entities categorized to provide world cup services as per SCDL identification of world cup entities

Following table defines initial response times which needs to be followed based on the criticality identified while following ***Table 64: Incident Matrix***

Table 65: Response Matrix

Response Matrix	Initial Response Times	Remarks
Criticality Level 1 CL1	60 minutes	
Criticality Level 2 CL2	Reporting not required	Employee investigations that are time sensitive should typically be classified at this level
Criticality Level 3 CL3	Reporting not required	May include: • Incident or employee investigations that are not time sensitive • Long-term investigations involving extensive research

* Initial Response Time – This specifies the maximum amount of time that should elapse before an Agency notifies Q-CERT.

10.4.4 Services expected at each level

Following table describes services expected at each level of world cup ecosystem:

Table 66: Services expected at each level – Incident Handling and Response

Entity	Sector	National
• Incident Handling and Response • Live Forensics	• Incident Handling and Response • Forensics (Live + Post Mortem)	• Incident Handling and Response • Forensics (Live + Post Mortem)

* Entities which do not fall under any sector should forward their information to national level security monitoring team

10.5 Milestones

Following milestones have been defined for incident handling and response:

- Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events
- Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies
- Analysis is conducted to ensure adequate response and support recovery activities
- Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident
- Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities

10.6 Type of tools or software that should be used for collection of artefacts

Following table define features of incident analysis tools which will help during incident analysis.

Table 67: Tools and its features required during incident analysis

Type of Tool	Features Required from Incident Response perspective
Packet Capture	• Read and write to packet capture files • Distil packet capture files to other formats for more practical analysis. This offers, fast analysis against the distilled source data, while retaining the original packet capture file for in-depth analysis and extraction
Flow Based Collections	• Collect, parse and represent the collected flow-based data • Provide query-based search for specific investigations • Provision to save specific duration of flow-based data either local or on network location. • Provision to export such data
Network logs	• Network based services and appliances should be able to support log formats which organization is using for central logging. At minimum they should support syslog log format

Type of Tool	Features Required from Incident Response perspective
	• Provision to export specific duration of log data
Operating System Based artefacts	• Collect and parse memory dump, file system and current network communications artefacts • Sort artefacts with time of event for timeline analysis • Provision to export to other formats for more practical analysis
Server Logs	• Provision to export log data to central logging server • Provision to export specific duration of logs
Workstation Logs	• Provision to export log data to central logging server • Provision to export specific duration of logs
Incident Tracking system	• Provide tracking of all incidents handled by the team • Provision to save raw artefacts collected related to the incident • Provision to save analysis reports related to the incident
Forensics Tools	• Disk and data capture • File viewers • File analysis • Registry analysis • Internet analysis • Email analysis • Mobile devices analysis • Mac OS analysis • Network forensics • Database forensics
SIEM	• A centralized log aggregator and correlation engine • Capable of understanding and inspecting various networking protocols • Capable of collecting various log from different network-based services and appliances • Support syslog log format • Provision to export specific duration log data • Provision to query and search raw log data

10.7 Criteria to categorize Event/Alert/Incident/Breach

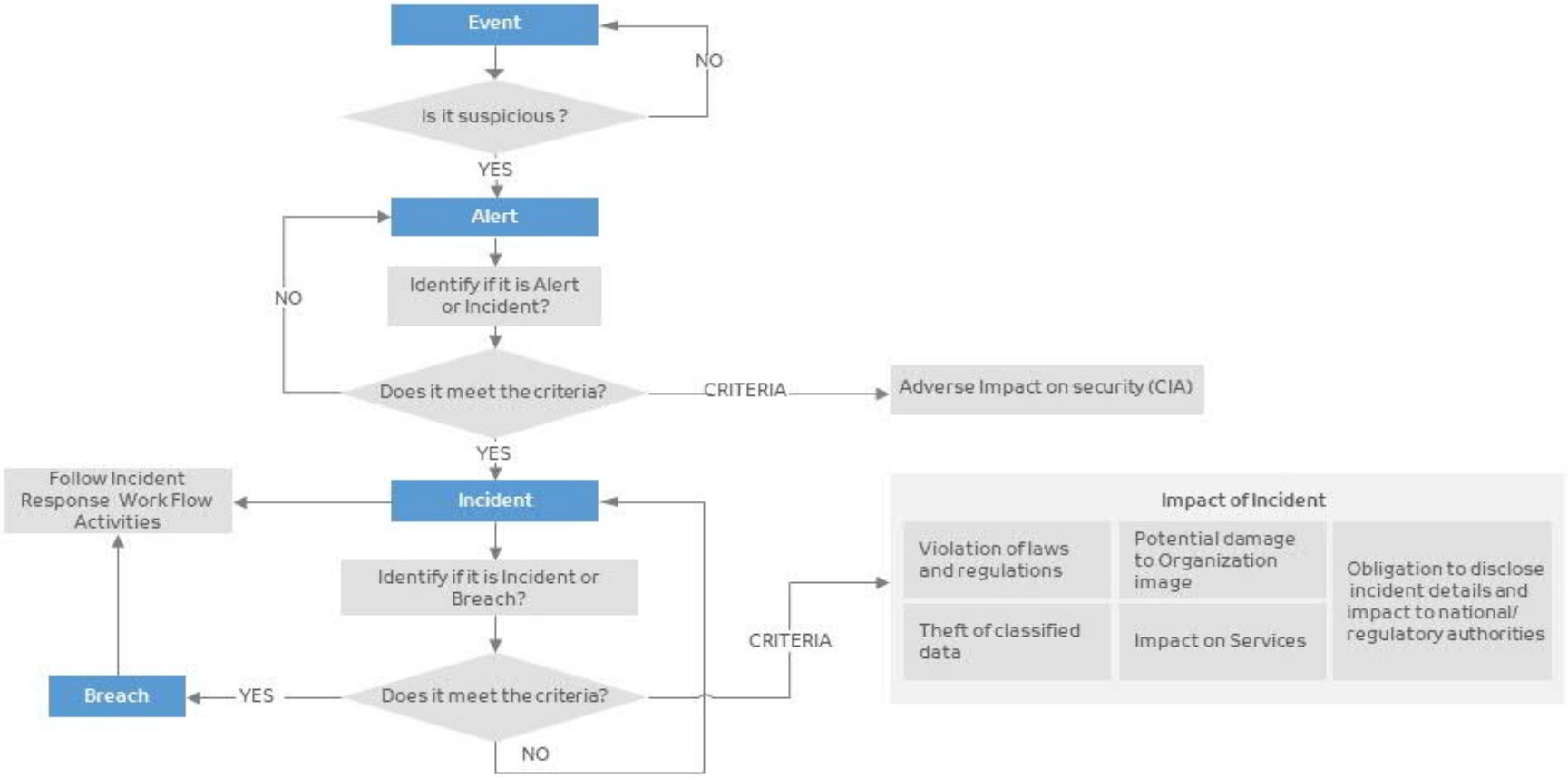
Following are some the important definitions that needs to be considered while defining the categorization criteria:

- **Event:** An action marked, logged to a point in time that may require additional assessment

- **Alert:** a notification that change is observed to the normal behaviour of a system/environment/process/workflow
- **Incident:** an adverse event that compromises Confidentiality, Integrity or Availability of an information asset, and has been verified as a potential threat
- **Breach:** an incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party.

Following figure defines the criteria that needs to be followed for categorization among alert/event/incident/breach

Figure 68: Criteria to categorize Event and Incident



10.8 Criteria to trigger Recovery and Continuity

Following criteria can used to trigger process flow of Recovery and Continuity

Table 68: Recovery and Continuity process flow triggering criteria

Security Needs	0	Low	Medium	High
Confidentiality	Public information	Information for internal use only, any disclosure can lead to minor damages on the system or its objectives	Information for internal use only, any disclosure can lead to severe damages on the system or its objectives	Secret information can impact the viability of the system or of the activity
Integrity	No specific need of integrity	Compromise of the data can lead to minor malfunctions	Compromise of the asset can lead to severe malfunction of a critical process	Compromise of the asset can impact the viability of the process or of the activity
Availability	T > 1 day of unavailability can lead to severe damages for the system or its objectives	T > 6 hours of unavailability can lead to severe damages for the system or its objectives	T > 1 hour of unavailability can lead to severe damages for the system or its objectives	T > 1 min of unavailability can lead to severe damages for the system or its objectives

10.9 Skills required for Incident Handling and Response

Following are the skills expected from personnel executing Incident Handling and Response activities:

- Perform incident analysis by correlating data from various sources
- Possess knowledge on network forensics, endpoint forensics, threat intelligence and as well as the functioning of applications or underlying IT infrastructure
- Competent to create custom signature/rules for detection and prevention technologies being used in organization
- Ability to create customized scripts for automation as well as for analysis
- Closely involved in developing, tuning and implementing threat detection analytics, security sensors and SOC Infrastructure
- Advise on remediation
- Perform Incident coordination and response
- Provide support for new analytic methods for detecting threats
- Suggested professional certifications which can help personnel to attain skills for the services defined under security monitoring and operations:
  - EC-Council Certified Incident Handler (ECIH)
  - EC-Council Certified Computer Hacking Forensic Investigator (CHFI)

- SANS GIAC Certified Incident Handler (GCIH)
- SANS GIAC Certified Forensic Examiner (GCFE)
- SANS GIAC Certified Forensic Analyst (GCFA)
- SANS GIAC Network Forensic Analyst (GNFA)
- SANS GIAC Advanced Smartphone Forensics (GASF)
- SANS GIAC Reverse Engineering Malware (GREM)

10.10 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards

Table 69: Incident Handling and Response activities mapping industry cyber security standards – Part I of II

Service Name — Incident Handling and Response						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Preparation	Incident Response plans are prepared, in place and managed					
Preparation	Personnel know their roles and order of operations when a response is needed	IM1 BC1	8.2.2	19	4.3.4.5.2 4.3.4.5.3 4.3.4.5.4	
Preparation	Prepare Incident Response Contact List which should include contact information (phone numbers, mobile numbers, emergency contact numbers, email addresses, public keys etc.) of all internal and external stakeholders					
Preparation	Define a secure way of communication such as encryption software (Rights Management Servers/PGP Keys/Digital Certificates) for communication among stakeholders					

Service Name — Incident Handling and Response						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Preparation	Response and recovery plans are tested			19 20	4.3.2.5.7 4.3.4.5.11	SR 3.3
Preparation	Response planning and testing are conducted with critical suppliers/providers			19	4.3.2.5.3 4.3.4.5.1	
Detection and Analysis	Events are reported consistent with established criteria	IM5		19	4.3.4.5.5	
Detection and Analysis	Notifications from detection systems are investigated and conduct triage is conducted			4 6 8 19	4.3.4.5.6 4.3.4.5.7 4.3.4.5.8	SR 6.1
Detection and Analysis	Incident Response plan is executed during or after an event		8.2.1	19	4.3.4.5.1	
Detection and Analysis	Incidents are categorized and assigned a criticality level consistent with response plans	IM6		19	4.3.4.5.6	
Detection and Analysis	The impact of the incident is understood		9.2.1		4.3.4.5.6 4.3.4.5.7 4.3.4.5.8	
Detection and Analysis	Malicious code is detected which have been identified as a part of analysis					
Detection and Analysis	Forensics are performed, where required, after getting authorization approval from management					SR 2.8 SR 2.9 SR 2.10 SR 2.11 SR 2.12 SR 3.9 SR 6.1

Service Name — Incident Handling and Response						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Detection and Analysis	Newly identified vulnerabilities are mitigated or documented as accepted risks			4 19		
Detection and Analysis	Information is shared consistent with response plans			19	4.3.4.5.2	
Detection and Analysis	Mechanisms shall be put in place to monitor and quantify the types and volumes of cyber security incidents					
Detection and Analysis	Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)			4 19		
Containment, Eradication and Recovery	Incidents are contained			19	4.3.4.5.6	SR 5.1 SR 5.2 SR 5.4
Containment, Eradication and Recovery	Incidents are mitigated			4 19	4.3.4.5.6 4.3.4.5.10	
Containment, Eradication and Recovery	Coordination with stakeholders occurs consistent with response plans	IM4 IM8	8.2.3	19	4.3.4.5.5	
Containment, Eradication and Recovery	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	IM7		19		
Containment, Eradication and Recovery	Recovery plan is executed during or after an event		9.2.1	10 19		

Service Name — Incident Handling and Response						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Containment, Eradication and Recovery	Recovery activities are communicated to internal stakeholders and executive and management teams					
Post-incident Activity	Response plans incorporate lessons learned				4.4.3.4	
Post-incident Activity	Response strategies are updated					
Post-incident Activity	Recovery plans incorporate lessons learned	BC4			4.4.3.4	
Post-incident Activity	Recovery strategies are updated	BC4				
Post-incident Activity	Public relations are managed					
Post-incident Activity	Reputation after an event is repaired					

Table 70: Incident Handling and Response activities mapping industry cyber security standards – Part II of II

Service Name — Incident Handling and Response							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Preparation	Incident Response plans are prepared, in place and managed						
Preparation	Personnel know their roles and order of operations when a response is needed	A.6.1.1 A.7.2.2 A.16.1.1	CP-2 CP-3 IR-3 IR-8	12.10	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii)	SEF-03	
Preparation	Prepare Incident Response Contact List which should include contact information (phone numbers, mobile numbers, emergency contact numbers, email addresses, public keys etc.) of all internal and external stakeholders						
Preparation	Define a secure way of communication such as encryption software (Rights Management Servers/PGP Keys/Digital						

Service Name — Incident Handling and Response							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
	Certificates) for communication among stakeholders						
Preparation	Response and recovery plans are tested	A.17.1.3	CP-4 IR-3 PM-14	12.10.2	164.308(a)(7)(ii)(D)		
Preparation	Response planning and testing are conducted with critical suppliers/providers	A.16.1.1 A.17.1.1 A.17.1.2 A.17.1.3	CP-2 CP-7 CP-12 CP-13 IR-7 IR-8 IR-9 PE-17	11.1.2 12.5.3 12.10	164.308(a)(6) 164.308(a)(7) 164.310(a)(2)(i) 164.312(a)(2)(ii)		
Detection and Analysis	Events are reported consistent with established criteria	A.6.1.3 A.16.1.2	AU-6 IR-6 IR-8	12.10	164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii)	SEF-03	
Detection and Analysis	Notifications from detection systems are investigated and conduct triage is conducted	A.12.4.1 A.12.4.3 A.16.1.5	AU-6 CA-7 IR-4 IR-5 PE-6 SI-4	10.6.3 11.5.1 12.5.2 12.10	164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.312(b)		

Service Name — Incident Handling and Response							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Detection and Analysis	Incident Response plan is executed during or after an event	A.16.1.5	CP-2 CP-10 IR-4 IR-8	12.10	164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)		
Detection and Analysis	Incidents are categorized and assigned a criticality level consistent with response plans	A.16.1.4	CP-2 IR-4 IR-5 IR-8	10.6.3 11.5.1 12.5.2 12.10	164.308(a)(6)(ii)		
Detection and Analysis	The impact of the incident is understood	A.16.1.4 A.16.1.6	CP-2 IR-4	10.6.3 11.5.1 12.5.2 12.10	164.308(a)(6)(ii) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E)	BCR-09	
Detection and Analysis	Malicious code is detected which have been identified as a part of analysis						
Detection and Analysis	Forensics are performed, where required, after getting authorization approval from management	A.16.1.7	AU-7 IR-4	10.6.3 11.5.1 12.5.2 12.10	164.308(a)(6)	SEF-04	

Service Name — Incident Handling and Response							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Detection and Analysis	Newly identified vulnerabilities are mitigated or documented as accepted risks	A.12.6.1	CA-7 RA-3 RA-5	10.6.3 11.5.1 12.5.2 12.10	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(6)(ii)		
Detection and Analysis	Information is shared consistent with response plans	A.16.1.2 Clause 7.4 Clause 16.1.2	CA-2 CA-7 CP-2 IR-4 IR-8 PE-6 RA-5 SI-4	12.10	164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C)		
Detection and Analysis	Mechanisms shall be put in place to monitor and quantify the types and volumes of cyber security incidents					SEF-05	
Detection and Analysis	Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security		SI-5 PM-15				

Service Name — Incident Handling and Response							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
	bulletins, or security researchers)						
Containment, Eradication and Recovery	Incidents are contained	A.12.2.1 A.16.1.5	IR-4	10.6.3 11.5.1 12.5.2 12.10	164.308(a)(6)(ii)		
Containment, Eradication and Recovery	Incidents are mitigated	A.12.2.1 A.16.1.5	IR-4	10.6.3 11.5.1 12.5.2 12.10	164.308(a)(6)(ii)		
Containment, Eradication and Recovery	Coordination with stakeholders occurs consistent with response plans	Clause 7.4	CP-2 IR-4 IR-8	12.10	164.308(a)(6) 164.308(a)(7) 164.310(a)(2)(i) 164.312(a)(2)(ii)	SEF-01 SEF-03	
Containment, Eradication and Recovery	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	A.16.1.4	PM-15 SI-5		164.308(a)(6)		
Containment, Eradication and Recovery	Recovery plan is executed during or after an event	A.16.1.5	CP-10 IR-4 IR-8	12.10.6	164.308(a)(7) 164.310(a)(2)(i)		

Service Name — Incident Handling and Response							
Process Phases	**Activities/ Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Containment, Eradication and Recovery	Recovery activities are communicated to internal stakeholders and executive and management teams	Clause 7.4	CP-2 IR-4	12.10.6	164.308(a)(6)(ii) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.314(a)(2)(i)(C)		
Post-incident Activity	Response plans incorporate lessons learned	A.16.1.6 Clause 10	CP-2 IR-4 IR-8	12.10.6	164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)		
Post-incident Activity	Response strategies are updated	A.16.1.6 Clause 10	CP-2 IR-4 IR-8		164.308(a)(7)(ii)(D) 164.308(a)(8)		
Post-incident Activity	Recovery plans incorporate lessons learned	A.16.1.6 Clause 10	CP-2 IR-4 IR-8	12.10.6	164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)		
Post-incident Activity	Recovery strategies are updated	A.16.1.6 Clause 10	CP-2 IR-4 IR-8	12.10.6	164.308(a)(7)(ii)(D) 164.308(a)(8)		
Post-incident Activity	Public relations are managed	Clause 7.4			164.308(a)(6)(i)		
Post-incident Activity	Reputation after an event is repaired	Clause 7.4			164.308(a)(6)(i)		

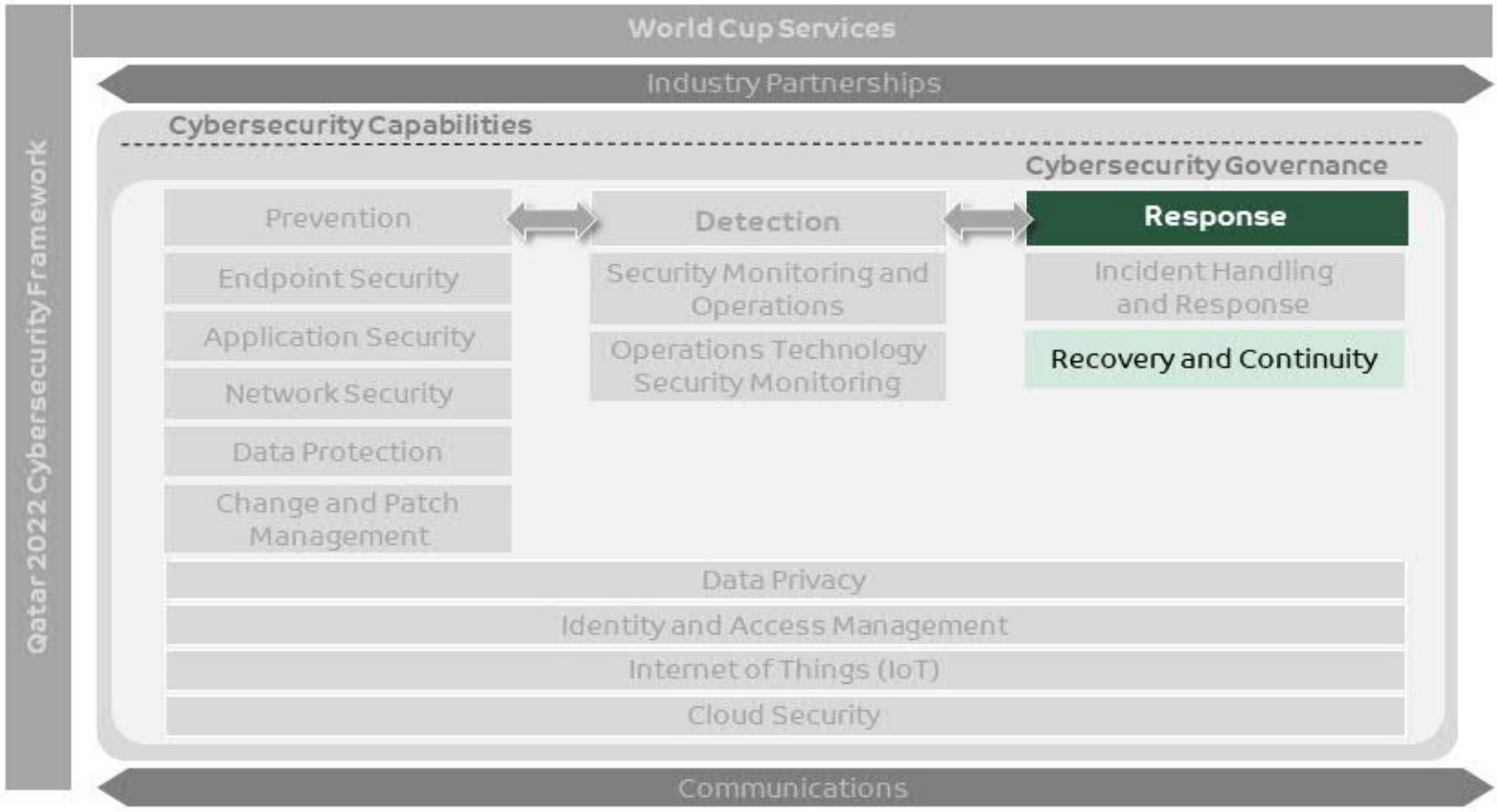
11

Recovery and Continuity

11. Capability Description – Recovery and Continuity

A capability that identifies potential threats and their impacts and builds appropriate recovery strategies and tactics accordingly. This chapter focuses on ‘Recovery and Continuity’ capability defined under the ‘Response’ pillar of world cup cybersecurity capabilities.

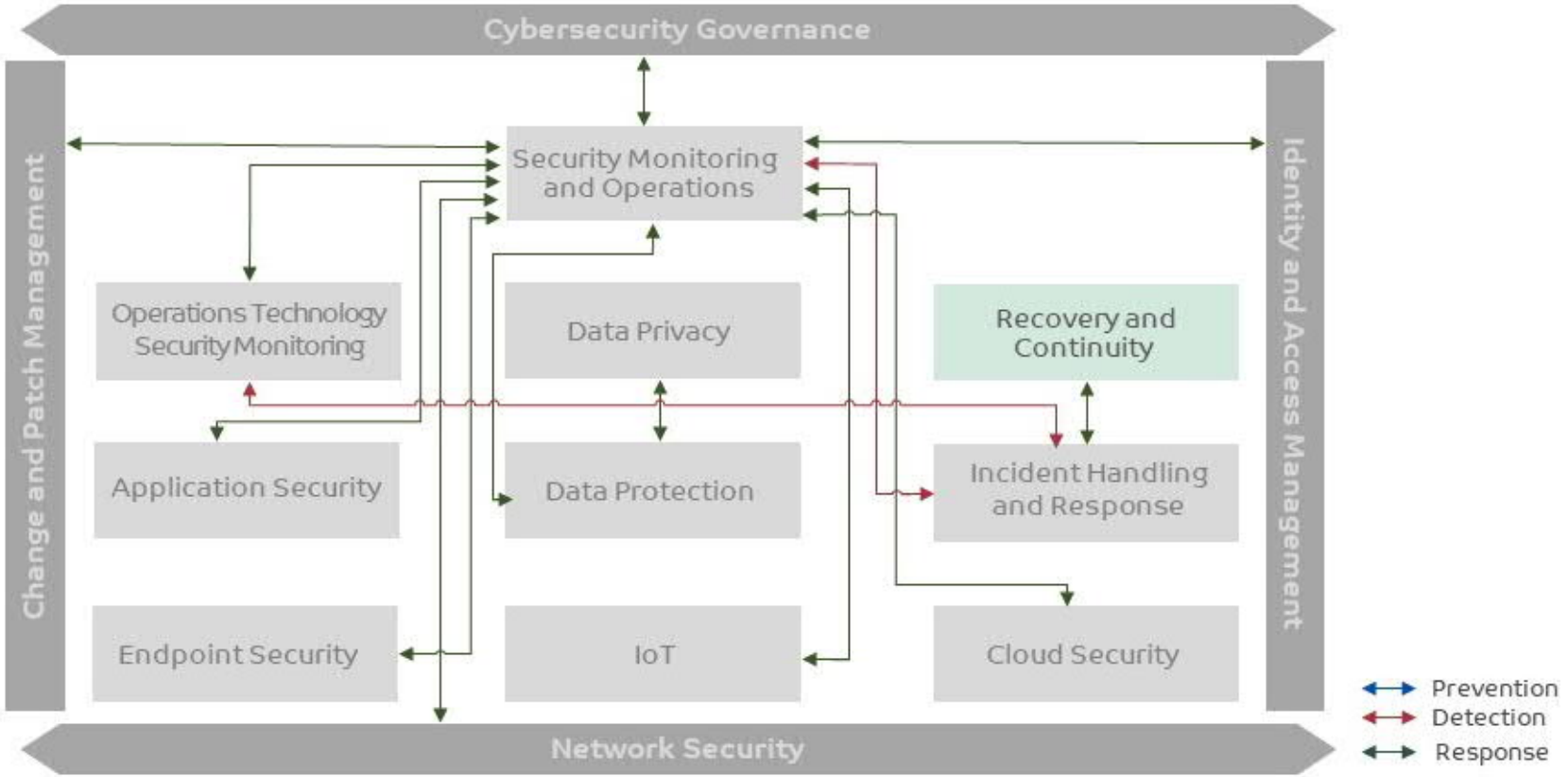
Figure 69: Cybersecurity Capabilities-Recovery and Continuity



The team responsible for executing 'Recovery and Continuity' activities must work closely with 'Incident Handling and Response' team. Moreover, the incident handling team should have defined criteria (example ***Criteria to trigger Recovery and Continuity***) to trigger recovery and continuity processes when applicable and required.

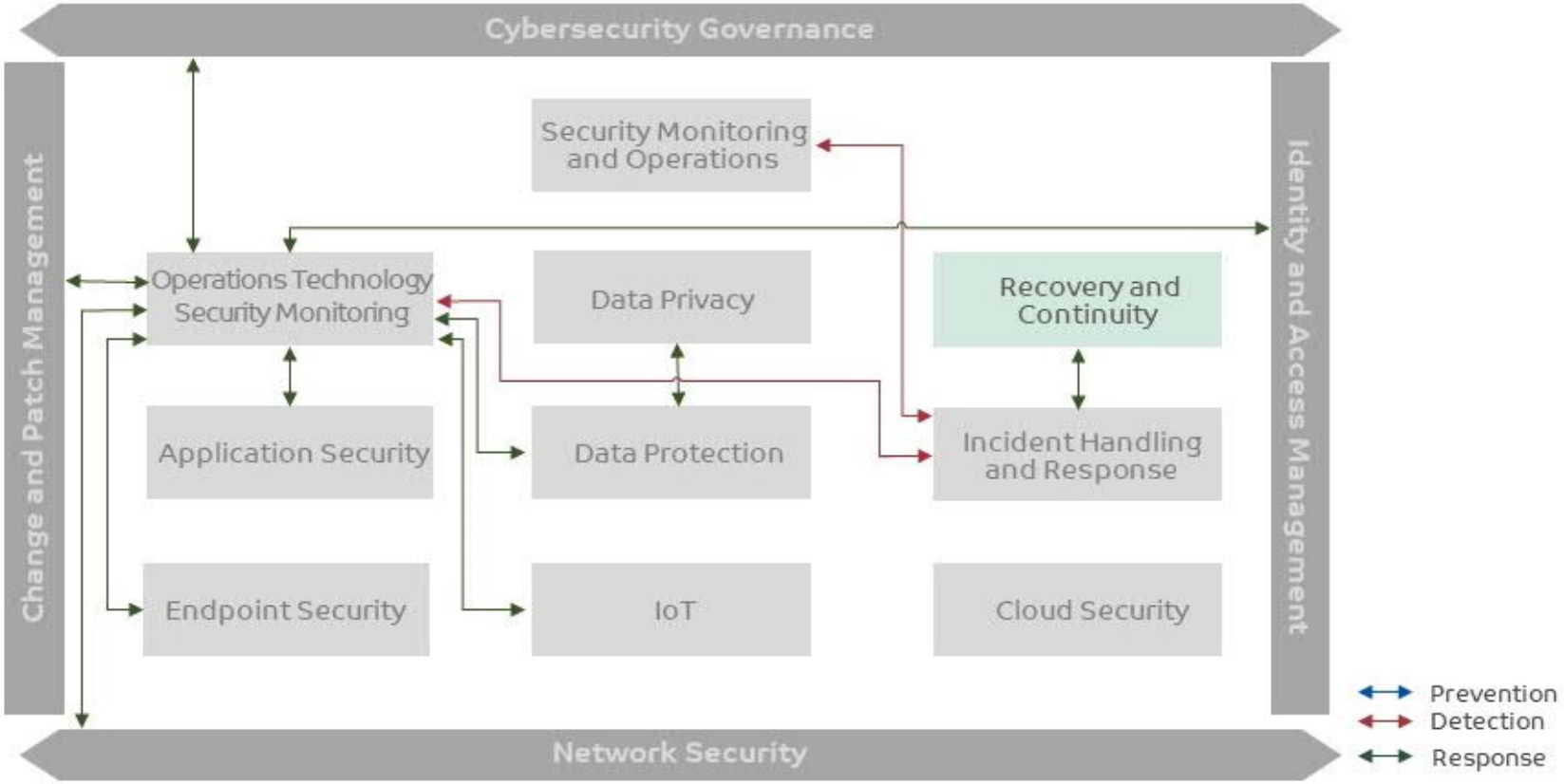
Following figure depicts linkage of Recovery and Continuity with other cybersecurity capabilities defined in the framework when the process flow is being triggered through 'Security Monitoring and Operations'.

Figure 70: Recovery and Continuity linkage with other capabilities when process is triggered through Security Monitoring and Operations



Following figure depicts linkage of Recovery and Continuity with other cybersecurity capabilities defined in the framework when the process flow is being triggered through ‘Operations Technology Security Monitoring’

Figure 71: Recovery and Continuity linkage with other capabilities when process is triggered through Operations Technology Security Monitoring



11.1 Prerequisites

Following are the prerequisites which are required to be accomplished for Recovery and Continuity:

- International, national and/or local legal, statutory and regulatory requirements have been identified
- A governance has been established and roles have been defined
- Services, business functions, processes have been identified and a service and process mapping has been performed
- Relevant methodologies have been established to enable identification of criticality and risks
- Criticality of services, business functions, processes, infrastructure and technologies have been identified
- Continuity threats and risks have been assessed and controls have been identified
- Provision for required resources (infrastructure, technology and people etc.) have been established
- Dependencies on the internal and external elements have been evaluated
- Critical 3rd party or external agency support have been identified and service agreements are established
- SLAs have been defined with third-party vendors from service availability and support management perspective
- Resilience strategies, plans and procedures development have critical dependency on the output from the impact and risk assessment exercises
- Holistic testing, exercising, training and monitoring programs have been established
- Evaluation and substance efforts are factored in for continual improvements within the programs established

11.2 Recovery and Continuity Service

From world cup perspective, the ***Table 71: Recovery and Continuity Service*** describes cybersecurity service that has been defined under this capability and respective activities that needs to be conducted for each service. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal policies, procedures and guidelines
- Define program scope and identify target assets (locations, technologies, functions, business processes)
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter)
- Define impact and risk criteria and classification
- Define minimum acceptable recovery and continuity standards
- Deploy and train resources for the execution and support
- Define service, technology and infrastructure criticality and requirements
- Identify opportunities for automation where applicable
- Continually improve policy, procedure and guidelines with changing risks and lessons learned

Table 71: Recovery and Continuity Service

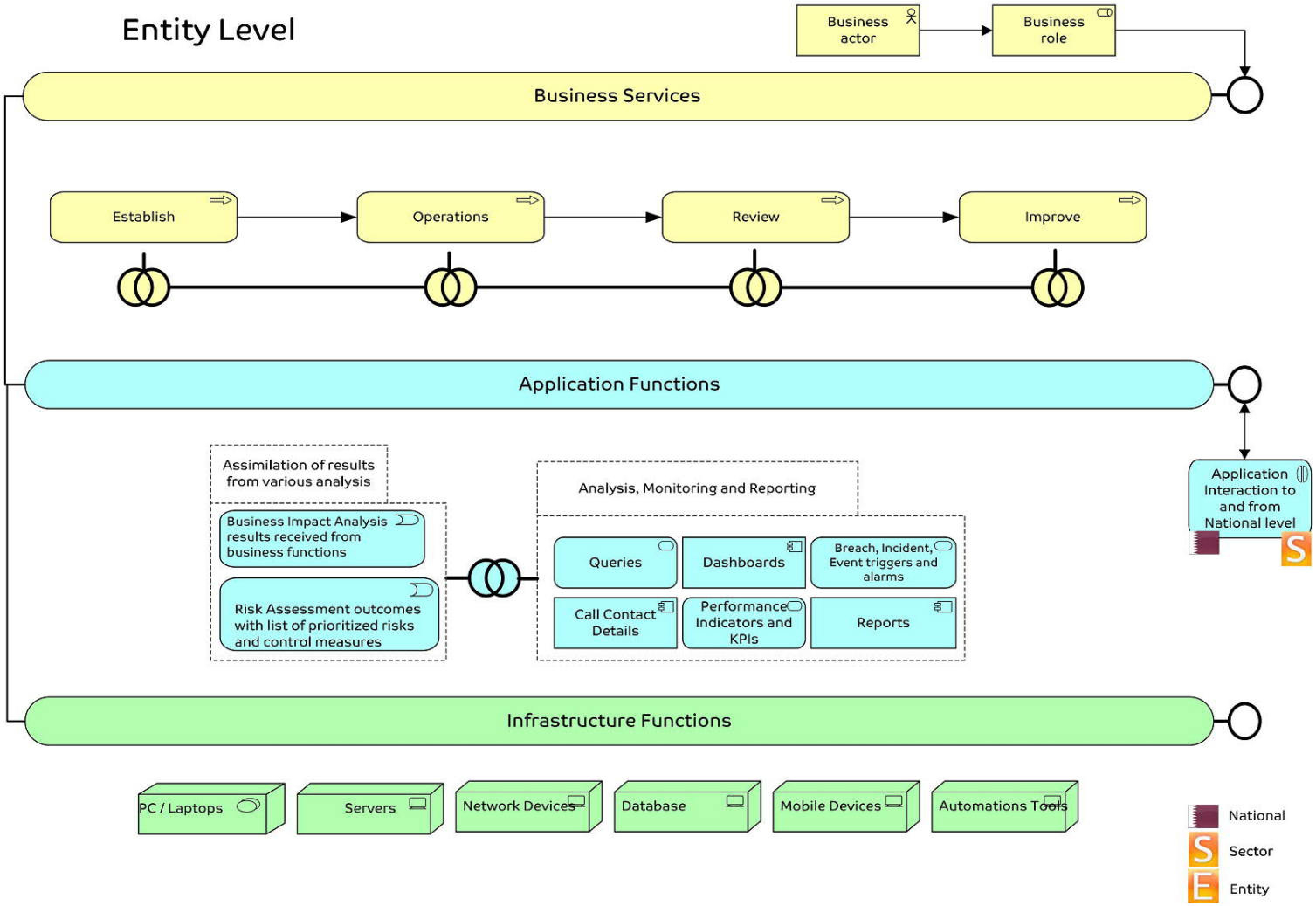
Service Name: Recovery and Continuity	
Description	A response capability that identifies potential threats and impacts to build appropriate recovery strategies /tactics.
Process Phases	**Activities/Controls**
Establish	• Design a recovery capability that enable's the entity to promptly and effectively respond to cyber security disruption's and maintain continuity of its prioritized IT/OT activities, considering all interested parties involved in performing prioritized activities • Establish the governance model to oversee the management of the recovery and continuity program at the entity, with detailed roles and responsibilities for business as usual and disruptive events. The sector level Recovery and Continuity (Resilience and/or BCMS) governance must be designed to integrate with entity level R&C governance to facilitate appropriate oversight/coordination during any disruptive incident • Identify relevant legal and regulatory framework as set by international, national and sector level standards, legislation and practices for mandatory compliance
Operations	• Frameworks governing the recovery capability is an on-going process that must be managed effectively and efficiently, that helps organizations to identify, classify, understand and prioritize the cyber recovery and continuity risks and develop plans so that the risks can be mitigated, and disruptive events can be responded in a befitting manner • Define methodology and process for conducting Business Impact Analysis (BIA) and Threat and Risk Assessment, using a combination of qualitative and quantitative metric and indicators • Risk management process, methodology and approach for the identification, evaluation and assessment of threats and risks (i.e. cyber threats, technological failures, man-made and natural disaster etc.), in alignment with Entity's Enterprise Risk management program, sector and national level standards and best practices (where available). • Identify Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), Minimum Service Levels (MSLs)and Maximum Allowable Outages (MAOs) for critical business processes, technologies and functions (or products and services, where applicable) • Appropriate strategies for stabilizing, continuing, resuming and recovering prioritized services, with the following considerations: • Data Centre and IT/OT Disaster Recovery • Alternate recovery sites • Secondary resources for all critical positions and roles • Redundancy for critical equipment • Critical vendors/suppliers/partners, in alignment with defined supply chain resiliency principles and guidelines • Emergency Command and Control Centre (ECCC) • Entity may look at Hot (Active-Active, Active-Passive), Warm or Cold options while defining the Recovery and Continuity Strategies depending on the criticality of businesses identified during Business Impact Analysis Process • Business Continuity Plans and procedures for the recovery of prioritized services, technology and supporting resources, to an acceptable level, within a predetermined timeframe

Service Name: Recovery and Continuity	
	• Emergency/crisis communication guidelines with protocols and requirements for effective internal/external communication with key stakeholders, government agencies/interested parties and customers to enable effective decision-making during a disruptive event, and to maintain alignment with national level requirements as defined by relevant government authorities (e.g. National Command Centre). • Define process and associated governance for testing and exercising the business continuity plans to ensure their effectiveness and alignment with national and sector level standards • Stimulate a culture of recovery and continuity across the entity and sector through regular awareness programs, communications and training to internal/external stakeholders
Review	• Evaluation and the identification for the improvements of recovery and continuity capability. These reviews and updates are obligatory when a change takes place in the entity (i.e. in terms of services/works or people) • Performance monitoring and reporting framework is clearly stipulated, including governance model, roles and responsibilities, and required committees and/or working groups • Compliance with the legal and regulatory framework as set by international, national and sector level standards, legislation and practices.
Improvements	• Ensuring recovery and continuity capability are valid and consistent with the National and Entity cyber resilience objectives • Review of Recovery and Continuity program against established Performance matrices and key performance indicators

11.3 Recovery and Continuity Capability Model

Following figure illustrates an architecture model of various functions established for Recovery and Continuity capability at entity level:

Figure 72: Recovery and Continuity Capability Model



Above figure defines the Recovery and Continuity capability model in layered approach:

- The **Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- The **Application Functions layer** supports the business layer with application services which are realized by (software) application components.
- The **Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

11.4 Information Flow at various levels

Entities need to collaborate with sector and national level to check the preparedness and communications under recovery & continuity service.

11.4.1 Services expected at each level

Recovery and continuity service will be applicable to all the world cup services used irrespective of the level (i.e. Entity/Sector/National) it is being used.

11.5 Milestones

Following milestones have been defined for Recovery and Continuity:

- Personnel are trained and rehearsed to respond effectively to any disruption
- Incident and crisis management capability should be enabled at the organization and National levels
- Regulations from government authorities and emergency service operators (i.e. civil defence) are properly developed, understood and documented
- Timely recovery and continuity business critical services and national critical infrastructure in the event of a disruption
- Compliance of the organization with its legal and regulatory is maintained
- Interested parties' requirements are well understood and factored in while designing and implementing the service
- The organization understands its prioritized activities, processes, services and/or functions.
- Protection of the organization's resources, reputation, finances and assets
- Adequate communication and support to staff and public in general in the event of a disruption

11.6 Functional Domains of Recovery and Continuity Service

Figure 73: Recovery and Continuity functional domains

Continuity and Recovery Framework defines the requirements for the establishment of the relevant governance, processes, plans and procedures that will underpin entity and national level resilience capabilities. The framework must a balanced approach to evaluate key resilience components at the entity level by defining the minimum levels recovery and continuity that each individual entity must comply with:

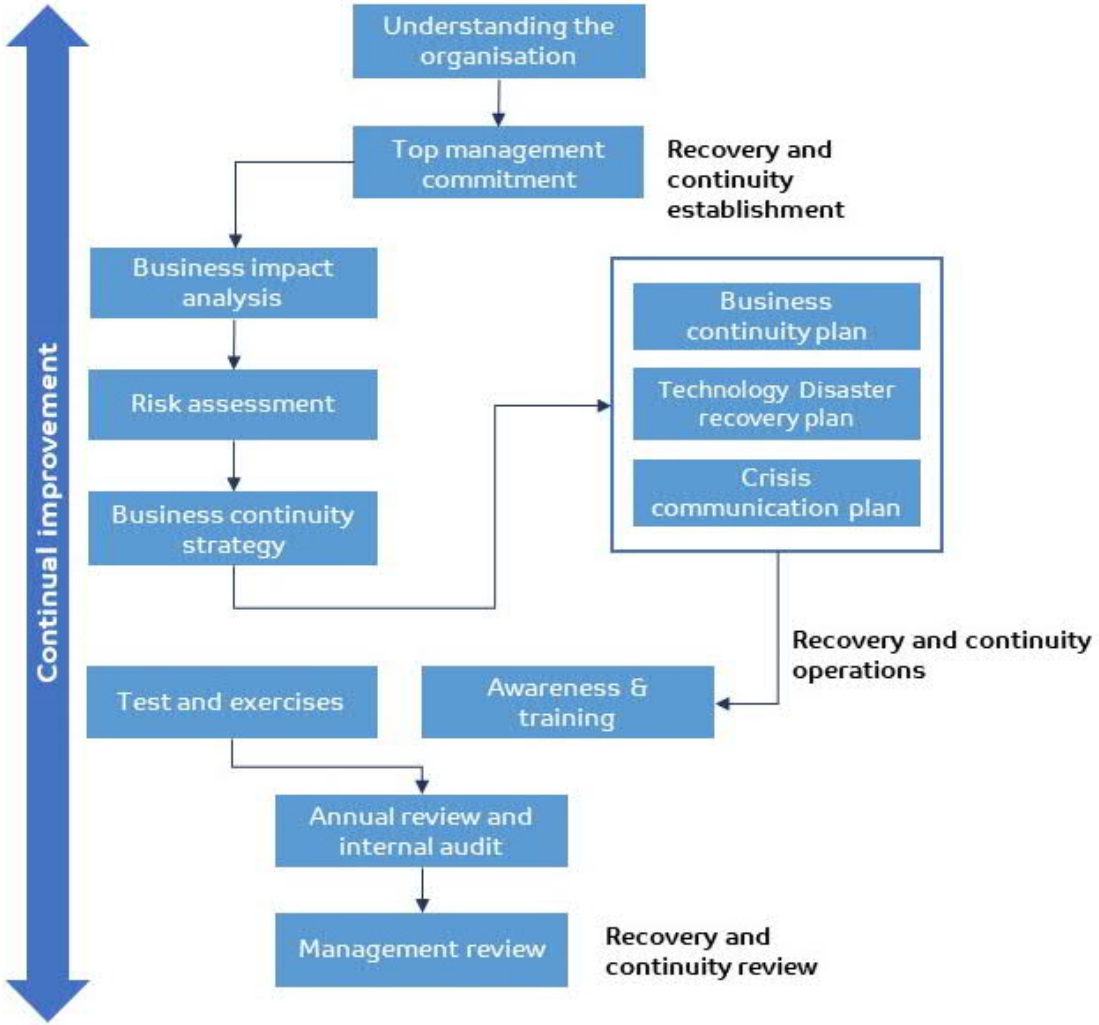
- Potential threats and associated risks that may impact the key business operations. The framework must consider the process for identification and assessment of these threats and risks and define the necessary controls to be put in place for management of potential threats and risks, as well as associated ownership for these controls
- Integrated coordination and crisis management capability, through the establishment of an entity level Emergency Command and Control Centres and aligning efforts with the National Command Centre (where applicable)
- Emergency response and crisis management protocols for effective management of national, sector and entity level events impacting the business operations
- Integrated crisis communication protocols for internal/external stakeholders and interested parties in the occurrence of a disruptive event
- Testing and Exercising Program regime which will be used to regularly check the viability of the Recovery and Continuity Framework
- Appropriate capabilities, facilities and processes to facilitate effective responses to known and unknown disasters and potential disruptive events across the entity and sector
- The framework specifies and is aligned to relevant international and national regulations and standards applicable to entity and sector level Recovery and Continuity Programs

Following key benefits of the above functional domains of the Recovery and Continuity service:

- Enables timely response to recover from cybersecurity disruptions with the aim of reducing the impact and cost of anomalous activities
- Ensures coordination with stakeholders to make available right resources in least time lagging
- Facilitates recovery Information sharing with sector-level or national-level authorities to alert them and help them to get understanding of bigger picture
- Enables use threat intelligence received from sector-level or national-level authorities and prepare themselves with better responsibilities to recover and continue operations
- Ensures government organizations and its sector partners should effectively handle recovery from disruptions in a well-coordinated manner to fully recover from such situations. Service delivery should be maintained at minimum required level and should not be disrupted when a disruption occurs until recovery is complete
- Systemically build business continuity capability before, during and after an emergency, disaster or crisis. All these initiatives are aimed at ensuring ongoing performance of prioritized activates in both public and private sectors, for enhancing Qatar’s national stability

11.7 Recovery and Continuity process flow across functional domains

Figure 74: Recovery and Continuity process flow



The key activities aligned to Recovery and Continuity capability workflows are described below:

11.7.1 Business Impact Analysis

- To determine the prioritized activities and their time frames for resuming
- To assess and analyse the requirements of prioritized activities for their recovery and continuity
- To assess and analyse the impacts of not performing the prioritized activity
- To evaluate the time span after the occurrence of an incident in which an activity or product should be restored or resources and assets should be regained.
- To evaluate the maximum interruption/downtime the organization can tolerate

11.7.2 Risk Assessment

- Risk Assessment provides a mechanism for the identification of the risks that represent opportunities as well as the risks that represent potential pitfalls.
- It enables the organizations to have a clear idea of variables to which they may be exposed, whether internal or external, retrospective or forward-looking

11.7.3 Business Continuity Strategies

The organization must define appropriate strategy options for:

- The protection of prioritized activities;
- Reducing, and managing the impacts;
- Recovery and resumption of prioritized activities considering key strategies – as identified below:

- Back-up Sites (Split/ multiple site operations)
- Alternative Sites
- Outsourcing
- Post-Event Procurement
- Insurance
- Manual Workaround
- Cross-training
- Resilient IT Architecture
- Occupational Health and Safety and Environment (OHSE)
- Third party Review

11.7.4 Business Continuity Plans (BCP)

- Have a defined purpose and scope.
- Be communicated to all personnel that needs to be aware of it, and to personnel with specific roles and responsibilities for review and update.
- Be consistent with the BCM strategy and incident response plan, capabilities and requirements of interested parties.
- Be accessible to and understood

11.7.5 Training and Testing

- Build awareness on BCM policy and objectives
- Establish a methodology for evaluating its effectiveness;
- Spread BC capability and awareness;
- Ensure continual improvement of BCM Program; and
- Ensure personnel are aware of their roles and responsibilities in BCM Program

11.8 Criteria to trigger Recovery and Continuity

Following availability criteria can used to trigger process flow of Recovery and Continuity

Table 72: Recovery and Continuity process flow triggering criteria

Security Needs	0	Low	Medium	High
Confidentiality	Public information	Information for internal use only, any disclosure can lead to minor damages on the system or its objectives	Information for internal use only, any disclosure can lead to severe damages on the system or its objectives	Secret information can impact the viability of the system or of the activity
Integrity	No specific need of integrity	Compromise of the data can lead to minor malfunctions	Compromise of the asset can lead to severe malfunction of a critical process	Compromise of the asset can impact the viability of the process or of the activity
Availability	T > 1 day of unavailability can lead to severe damages for the system or its objectives	T > 6 hours of unavailability can lead to severe damages for the system or its objectives	T > 1 hour of unavailability can lead to severe damages for the system or its objectives	T > 1 min of unavailability can lead to severe damages for the system or its objectives

11.9 Skills required for Recovery and Continuity

Following are the skills expected from personnel executing Recovery and Continuity activities:

- Perform process, service and technology analysis by identifying the impact of unavailability
- Possess knowledge and experience establishment of resilience programs and framework
- Competent to establish and operate Business Continuity, Crisis Management and Disaster recovery activities as part of Recovery and Continuity efforts within the organization
- Establish risk assessment program for proactive identification of threats and risk exposures
- Ability to prepare and communicate periodic dashboard on Recovery and Continuity activities to relevant stakeholders
- Ability to understand and maintain technological recovery and continuity requirements
- Facilitate in development and maintenance of required strategies, plans, procedures and supporting documentations
- Facilitate internal role-based trainings and awareness sessions for Recovery and Continuity governance on established programs
- Suggested professional certifications which can help personnel to attain skills for this capability
    - ISO22301:2012 Lead Implementer and Auditor
    - Certified Business Continuity Professional (DRII)

- Certification of the BCI (CBCI)
- Member of the BCI (MBCI)

11.10 Technology

Various Business Continuity Management, Crisis Management, Crisis Communications and Disaster Recovery automation tools are widely available. Some of the Recovery and Continuity automation tool:

Integrated business continuity management suite that offers Planning, Assessments, Incident Management/Testing, and Reporting on a single, inter-connected platform. Key features are defined below:

- BCM automation tool leverages related business continuity data and transforms it into timely, actionable information on the user's mobile device, tablet, or laptop
- Allows users to identify the “knowns” for a Disruption or test
- Using data relationships, pulls in the plans, recovery time objectives (RTOs), dependencies, tasks, and teams needed for recovery
- Gives mission-critical, up-to-the-minute visualizations of the recovery progress, supporting real-time decisions during the execution of tasks and plans

Call Notification Tool makes it easy to send notifications to any number of people at once, allowing for immediate, individual response with an automatic audit trail. Key features:

- Deliver multi-lingual text-to-speech notifications
- Premium 24/7 support and maintenance
- Access to unlimited web-based remote training
- Real-time reporting and audit logs
- Unlimited notification templates

11.11 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards

Table 73: Recovery and Continuity activities mapping industry cyber security standards – Part I of II

Service Name — Recovery & Continuity						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference— CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Establish	Design a recovery capability that enable's the entity to promptly and effectively respond to cyber security disruption's and maintain continuity of its prioritized IT/OT activities, considering all interested parties involved in performing prioritized activities	IM2, IM3, IM9, BC2, BC3, BC8	8.2.1, 9.2.1		4.3.2.5.3, 4.3.2.5.7, 4.3.4.5.1, 4.3.4.5.11	SR 2.8, SR 3.3, SR.6.1 SR 7.3, SR 7.4
Establish	Establish the governance model to oversee the management of the recovery and continuity program at the entity, with detailed roles and responsibilities for business as usual and disruptive events. The sector level governance must be designed to integrate with entity level governance to facilitate appropriate oversight/coordination during any disruptive incident	IM2, IM3, IM9, BC2, BC3, BC8	8.2.1, 9.2.1		4.3.2.5.3, 4.3.2.5.7, 4.3.4.5.1, 4.3.4.5.11	SR 2.8, SR 3.3, SR.6.1 SR 7.3, SR 7.4
Establish	Identify relevant legal and regulatory framework as set by international, national and sector level standards, legislation and practices for mandatory compliance	1. IM2, IM3, IM9, BC2, BC3, BC8	8.2.1, 9.2.1		4.3.2.5.3, 4.3.2.5.7, 4.3.4.5.1, 4.3.4.5.11	SR 2.8, SR 3.3, SR.6.1 SR 7.3, SR 7.4

Service Name — Recovery & Continuity						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference— CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Operations	Frameworks governing the recovery capability is an on-going process that must be managed effectively and efficiently, that helps organizations to identify, classify, understand and prioritize the cyber recovery and continuity risks and develop plans so that the risks can be mitigated, and disruptive events can be responded in a befitting manner	IM1, IM4, IM5, IM7, IM8, BC1	8.2.2, 8.2.3		4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5	
Operations	Define methodology and process for conducting Business Impact Analysis (BIA) and Threat and Risk Assessment, using a combination of qualitative and quantitative metric and indicators	IM1, IM4, IM5, IM7, IM8, BC1	8.2.2, 8.2.3	CSC 4	4.2.3, 4.2.3.9, 4.2.3.12	
Operations	Risk management process, methodology and approach for the identification, evaluation and assessment of threats and risks, in alignment with Entity's Enterprise Risk management program, sector and national level standards and best practices (where available)	IM1, IM4, IM5, IM7, IM8, BC1	8.2.2, 8.2.3	CSC 4	4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12	

Service Name — Recovery & Continuity						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference— CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Operations	Appropriate strategies for stabilizing, continuing, resuming and recovering prioritized services, with the following considerations: • Data Centre and IT/OT Disaster Recovery • Alternate recovery sites • Secondary resources for all critical positions and roles • Redundancy for critical equipment • Critical vendors/suppliers/partners, in alignment with defined supply chain resiliency principles and guidelines • Emergency Command and Control Centre (ECCC)	IM1, IM4, IM5, IM7, IM8, BC1	8.2.2, 8.2.3		4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5	
Operations	Business Continuity Plans and procedures for the recovery of prioritized services, technology and supporting resources, to an acceptable level, within a predetermined timeframe	IM1, IM4, IM5, IM7, IM8, BC1	8.2.2, 8.2.3		4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5	
Operations	Emergency/crisis communication guidelines with protocols and requirements for effective internal /external communication with key stakeholders, government agencies/interested parties and customers to enable effective decision-making during a disruptive event, and to maintain alignment with national level requirements as defined by relevant government authorities (e.g. National Command Centre)	IM1, IM4, IM5, IM7, IM8, BC1	8.2.2, 8.2.3	CSC 19	4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5, 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8	

Service Name — Recovery & Continuity						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference— CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Operations	Define process and associated governance for testing and exercising the business continuity plans to ensure their effectiveness and alignment with national and sector level standards	IM1, IM4, IM5, IM7, IM8, BC1	8.2.2, 8.2.3		4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5	
Operations	Stimulate a culture of recovery and continuity across the entity and sector through regular awareness programs, communications and training to internal/external stakeholders	IM1, IM4, IM5, IM7, IM8, BC1	8.2.2, 8.2.3		4.3.4.5.10, 4.4.3.4	
Review	Evaluation and the identification of the improvements of recovery and continuity capability. These review's and updates are obligatory when a change takes place in the entity (in terms of services /works or people)	IM6	9.2.1		4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8	SR 2.8, SR 2.9, SR 2.10 SR 2.11, SR 2.12, SR 3.9, SR 6.1
Review	Performance monitoring and reporting framework is clearly stipulated, including governance model, roles and responsibilities, and required committees and/or working groups	IM6	9.2.1		4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8	SR 2.8, SR 2.9, SR 2.10 SR 2.11, SR 2.12, SR 3.9, SR 6.1

Service Name — Recovery & Continuity						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference— CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Review	Compliance with the legal and regulatory framework as set by international, national and sector level standards, legislation and practices	IM6	9.2.1		4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8	SR 2.8, SR 2.9, SR 2.10 SR 2.11, SR 2.12, SR 3.9, SR 6.1
Improvements	Ensuring recovery and continuity capability are valid and consistent with the National and Entity cyber resilience objectives				4.3.4.5.10, 4.4.3.4	
Improvements	Review of Recovery and Continuity program against established Performance matrices and key performance indicators				4.3.4.5.10, 4.4.3.4	

Table 74: Recovery and Continuity activities mapping industry cyber security standards – Part II of II

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Establish	Design a recovery capability that enable's the entity to promptly and effectively respond to cyber security disruption's and	A.16.1.1, A.16.1.5, A.17.1.1, A.17.1.2, A.17.1.3	CP-2, CP-4, CP-10, IR-3 IR-4, IR-6, IR-	12.10	164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B)	SEF-02, BCR-01, BCR-02	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
	maintain continuity of its prioritized IT/OT activities, considering all interested parties involved in performing prioritized activities		8, IR-9 PM-14		164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)		
Establish	Establish the governance model to oversee the management of the recovery and continuity program at the entity, with detailed roles and responsibilities for business as usual and disruptive events. The sector level governance must be designed to integrate with entity level governance to facilitate appropriate oversight / coordination during any disruptive incident	A.16.1.1, A.16.1.5, A.17.1.1, A.17.1.2, A.17.1.3	CP-2, CP-4, CP-10, IR-3 IR-4, IR-6, IR-8, IR-9 PM-14	12.10	164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)	SEF-02, BCR-01, BCR-02	
Establish	Identify relevant legal and regulatory framework as set by international, national and sector level standards, legislation and practices for mandatory compliance	A.16.1.1, A.16.1.5, A.17.1.1, A.17.1.2, A.17.1.3	CP-2, CP-4, CP-10, IR-3 IR-4, IR-6, IR-8, IR-9 PM-14	12.10	164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)	SEF-02, BCR-01, BCR-02	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Operations	Frameworks governing the recovery capability is an on-going process that must be managed effectively and efficiently, that helps organizations to identify, classify, understand and prioritize the cyber recovery and continuity risks and develop plans so that the risks can be mitigated, and disruptive events can be responded in a befitting manner	A.6.1.1, A.6.1.3, A.16.1.1, A.16.1.2	CP-2, CP-3, IR-3, IR-8 AU-6, IR-6, CA-2, CA-7, IR-4, PE-6, RA-5, SI-4 PM-15, SI-5	12.10.1, 12.10.4	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii) 164.314(a)(2)(i)(C) 164.308(a)(6) 164.308(a)(7) 164.314(a)(2)(i)	SEF-01, SEF-03	
Operations	Define methodology and process for conducting Business Impact Analysis (BIA) and Threat and Risk Assessment, using a combination of qualitative and quantitative metric and indicators	A.6.1.1, A.6.1.3, A.16.1.1, A.16.1.2	RA-2, RA-3, PM-9, PM-11, SA-14	6.1	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C)	SEF-01, SEF-03	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
					164.314(a)(2)(iii) 164.314(a)(2)(i)(C) 164.308(a)(6) 164.308(a)(7) 164.314(a)(2)(i)		
Operations	Risk management process, methodology and approach for the identification, evaluation and assessment of threats and risks, in alignment with Entity's Enterprise Risk management program, sector and national level standards and best practices (where available)	A.12.6.1, A.18.2.3	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-13, PM-16, RA-2, M-4, PM-9	6.1, 11.2, 11.3 12.2, 12.10	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii) 164.314(a)(2)(i)(C) 164.308(a)(6) 164.308(a)(7) 164.314(a)(2)(i)	SEF-01, SEF-03	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Operations	Appropriate strategies for stabilizing, continuing, resuming and recovering prioritized services, with the following considerations: * Data Centre and IT/OT Disaster Recovery * Alternate recovery sites * Secondary resources for all critical positions and roles * Redundancy for critical equipment * Critical vendors / suppliers / partners, in alignment with defined supply chain resiliency principles and guidelines * Emergency Command and Control Centre (ECCC)	A.6.1.1, A.6.1.3, A.16.1.1, A.16.1.2	CP-2, CP-3, IR-3, IR-8 AU-6, IR-6, CA-2, CA-7, IR-4, PE-6, RA-5, SI-4 PM-15, SI-5	12.10.1, 12.10.4	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii) 164.314(a)(2)(i)(C) 164.308(a)(6) 164.308(a)(7) 164.314(a)(2)(i)	SEF-01, SEF-03	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Operations	Business Continuity Plans and procedures for the recovery of prioritized services, technology and supporting resources, to an acceptable level, within a predetermined timeframe	A.6.1.1, A.6.1.3, A.16.1.1, A.16.1.2	CP-2, CP-3, IR-3, IR-8 AU-6, IR-6, CA-2, CA-7, IR-4, PE-6, RA-5, SI-4 PM-15, SI-5	12.10.1, 12.10.4	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii) 164.314(a)(2)(i)(C) 164.308(a)(6) 164.308(a)(7) 164.314(a)(2)(i)	SEF-01, SEF-03	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Operations	Emergency/crisis communication guidelines with protocols and requirements for effective internal/external communication with key stakeholders, government agencies/interested parties and customers to enable effective decision-making during a disruptive event, and to maintain alignment with national level requirements as defined by relevant government authorities (e.g. National Command Centre)	A.16.1.5, A.6.1.1, A.7.2.2, A.16.1.1, Clause 7.4, A.16.1.4, A.16.1.6	CP-2, CP-10, IR-4, IR-8, CP-3, IR-3	12.10.1, 12.10.4	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii) 164.314(a)(2)(i)(C) 164.308(a)(6) 164.308(a)(7) 164.314(a)(2)(i)	SEF-01, SEF-03	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Operations	Define process and associated governance for testing and exercising the business continuity plans to ensure their effectiveness and alignment with national and sector level standards		CP-2, CP-10, IR-4, IR-8, CP-3, IR-3	12.10.1, 12.10.4	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii) 164.314(a)(2)(i)(C) 164.308(a)(6) 164.308(a)(7) 164.314(a)(2)(i)	SEF-01, SEF-03	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Operations	Stimulate a culture of recovery and continuity across the entity and sector through regular awareness programs, communications and training to internal/external stakeholders	A.16.1.6, Clause 10	CP-2, IR-4, IR-8	12.10.1, 12.10.4	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii) 164.314(a)(2)(i)(C) 164.308(a)(6) 164.308(a)(7) 164.314(a)(2)(i)	SEF-01, SEF-03	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Review	Evaluation and the identification of the improvements of recovery and continuity capability. These review's and updates are obligatory when a change takes place in the entity (in terms of services /works or people)	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4	AU-6, AU-7, CA-7, IR-4 IR-5, IR-8, PE-6, SI-4 CP-2	A.1.4, 12.10, 12.10.5	164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.312(b) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.308(a)(6) 164.308(a)(6)(ii)	BCR-09, SEF-04, SEF-05	
Review	Performance monitoring and reporting framework is clearly stipulated, including governance model, roles and responsibilities, and required committees and/or working groups	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4	AU-6, AU-7, CA-7, IR-4 IR-5, IR-8, PE-6, SI-4 CP-2	1.4, 12.10, 12.10.5	164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.312(b) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.308(a)(6) 164.308(a)(6)(ii)	BCR-09, SEF-04, SEF-05	

Recovery & Continuity							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference - GDPR**
Review	Compliance with the legal and regulatory framework as set by international, national and sector level standards, legislation and practices	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4	AU-6, AU-7, CA-7, IR-4 IR-5, IR-8, PE-6, SI-4 CP-2	1.4, 12.10, 12.10.5	164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.312(b) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.308(a)(6) 164.308(a)(6)(ii)	BCR-09, SEF-04, SEF-05	
Improvements	Ensuring recovery and continuity capability are valid and consistent with the National and Entity cyber resilience objectives	A.16.1.6	CP-2, IR-4, IR-8	12.10.6	164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii) 164.308(a)(8)		
Improvements	Review of Recovery and Continuity program against established Performance matrices and key performance indicators	A.16.1.6	CP-2, IR-4, IR-8	12.10.6	164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii) 164.308(a)(8)		

12

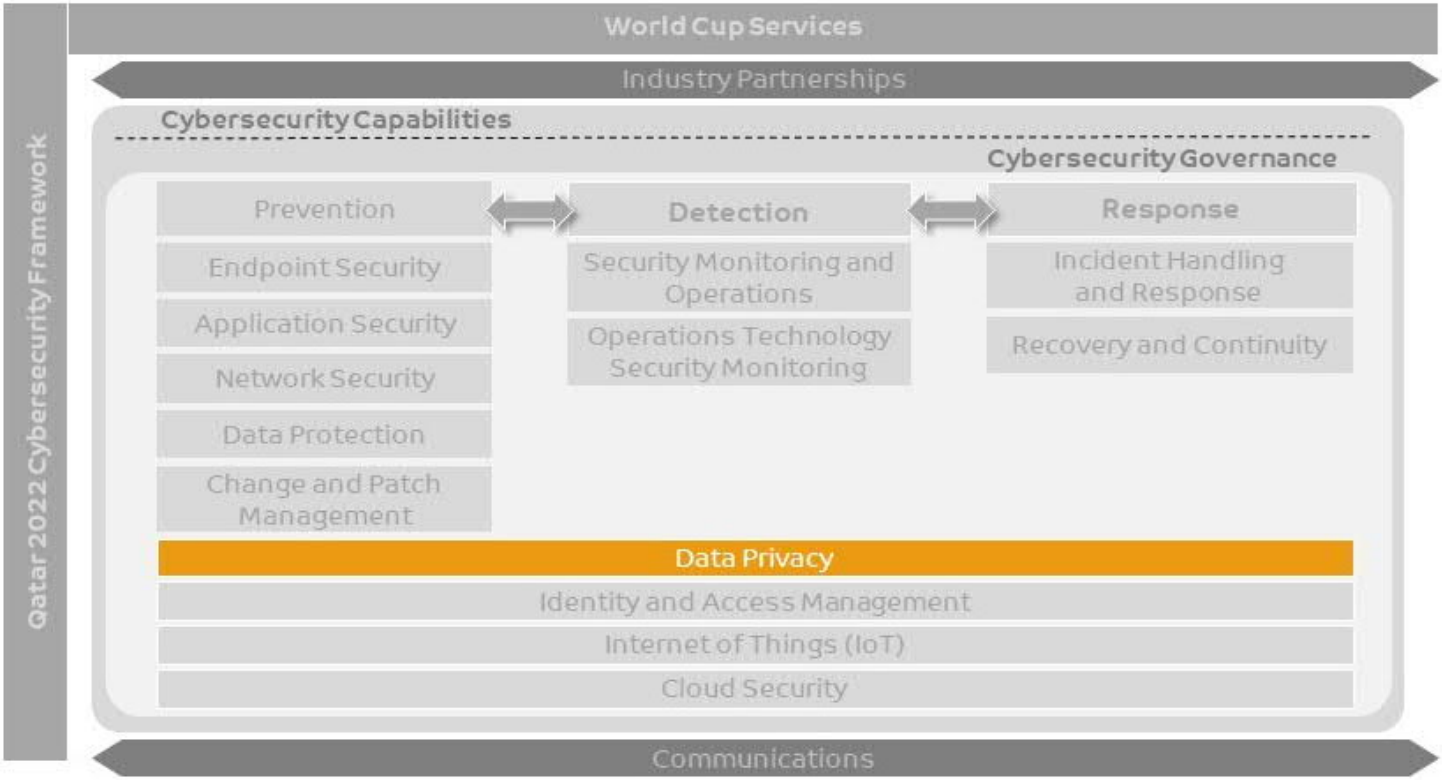
Data Privacy

12. Capability Description – Data Privacy

A capability that ensures compliance to legally binding regulation for protecting personally identifiable information as per the Qatari privacy and international regulations such as the EU General Data Privacy and Regulations (GDPR). This capability will implement the processes, controls and technologies required to build a sustainable data Privacy capability that is aligned to the business and is focused on compliance to General Data Privacy and Regulations.

This chapter focuses on 'Data Privacy', and covers all three pillars of world cup cybersecurity capabilities (Prevention, Detection and Response)

Figure 75: Cybersecurity capabilities – Data Privacy



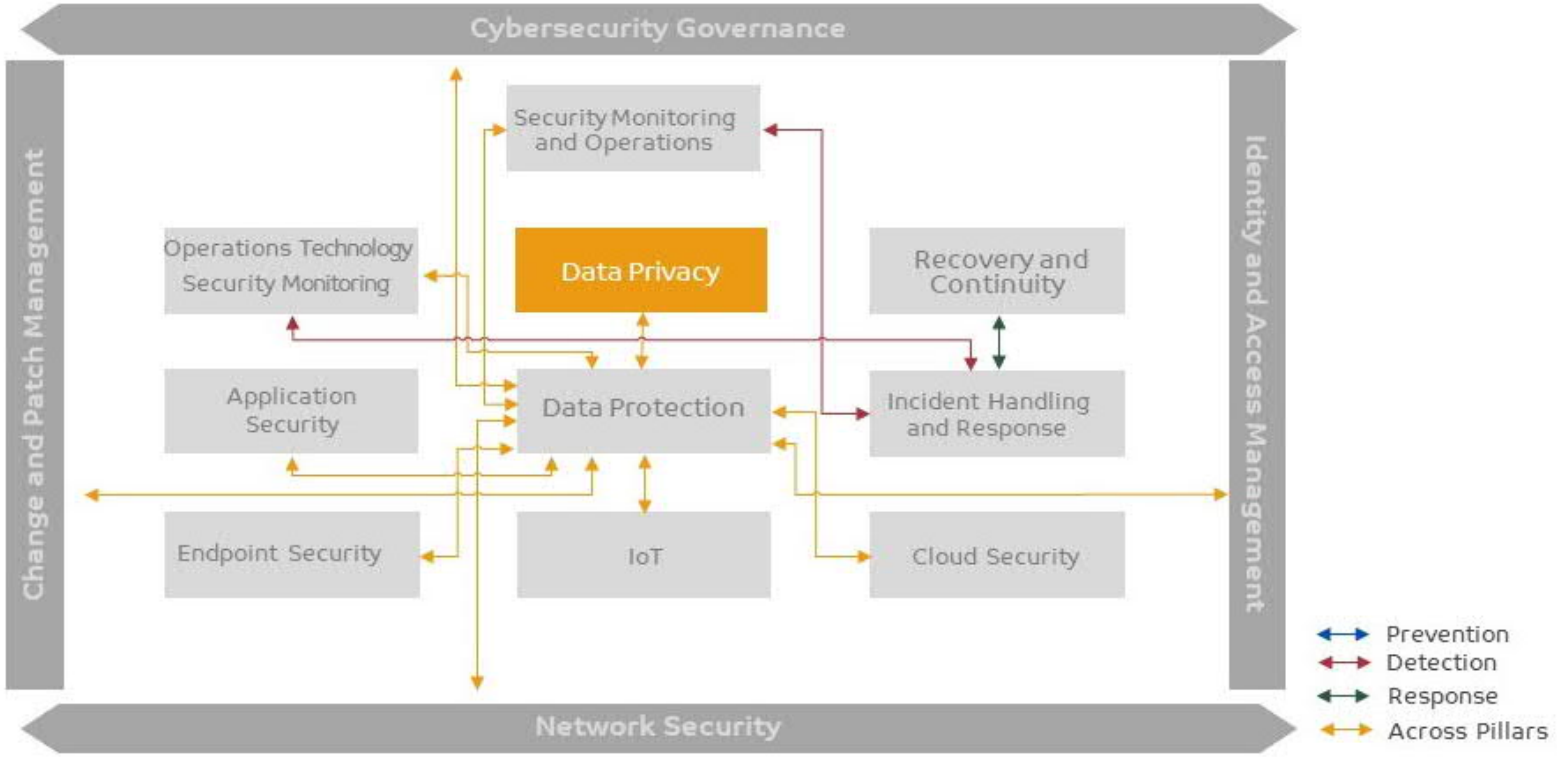
This capability is dependent on Data Protection capability (refer ***Capability Description – Data Protection*** chapter).

- Data protection refers to the processes that ensures that data is accurate, reliable, and available when those with authorized access need it and is NOT being accessed or used by unauthorized personnel
- Data privacy refers to the appropriate use of personally identifiable information to the agreed purposes

Hence, fundamentally data privacy cannot be ensured unless the data is protected.

Following figure depicts linkage of Data Privacy (through Data Protection and other cybersecurity capabilities) defined in the framework

Figure 76: Data Privacy linkage with other capabilities



12.1 Prerequisites

Following are the prerequisites which are required to be accomplished for a successful implementation of the Data Privacy capability:

- Personal identifiable Information or Data to be protected has been identified and documented
- Identified Information or Data have been classified for required security controls implementation
- Staff are educated and fully aware of the contractual, statutory or regulatory regulations and implications of any Data Privacy breaches
- Staff have access to the Data Privacy related policies and are aware of the importance of Data Privacy practices and their responsibilities for maintaining Data Privacy
- There is a process established for collection, legal usage, disclosure/ transfer, retention, archival and disposal of information or data based on the role organization will have such as information processor/controller
- Third-party(es) collecting, storing and processing personal information on behalf of the entities are identified
- Applicable regulations and contracts regarding the maintenance of Data Privacy, protection and cross border transfer of personal information are identified
- Management leadership and support to ensure compliance to Data Privacy requirements once established
- Availability of necessary resources to enforce the Data Privacy rules and regulations within the Entity
- Entity to have identified competent department/resource to monitor, report and manage noncompliance or breach to the Data Privacy regulation/laws
- Roles and responsibilities for data privacy are clearly defined in contracts, acknowledgments, terms and conditions between the entity and service providers (where applicable)
- Security risks are identified for the data privacy during the risk assessment have been communicated and considered

12.2 Data Privacy Service

From world cup perspective, ***Table 75: Data Privacy Service*** describes cybersecurity service that has been defined under this capability and respective activities that needs to be conducted for each service. However, from preparation/planning viewpoint, following steps must be completed:

- Establish formal policies, procedures and guidelines
- Define program scope and identify target assets
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and its compendium section)
- Define Data Privacy assessment classification and acceptance standards
- Deploy/configure appropriate solutions to align with establish standards
- Deploy and train team members to support personal identifiable information or other sensitive information handling
- Identify opportunities of automation where applicable
- Define services levels for remediation activity
- Define rules of engagement which will be followed
- Continually improve policy, procedure & guidelines with changing risks and lessons learned

Following table describes Data Privacy key activities established within the capability:

Table 75: Data Privacy Service

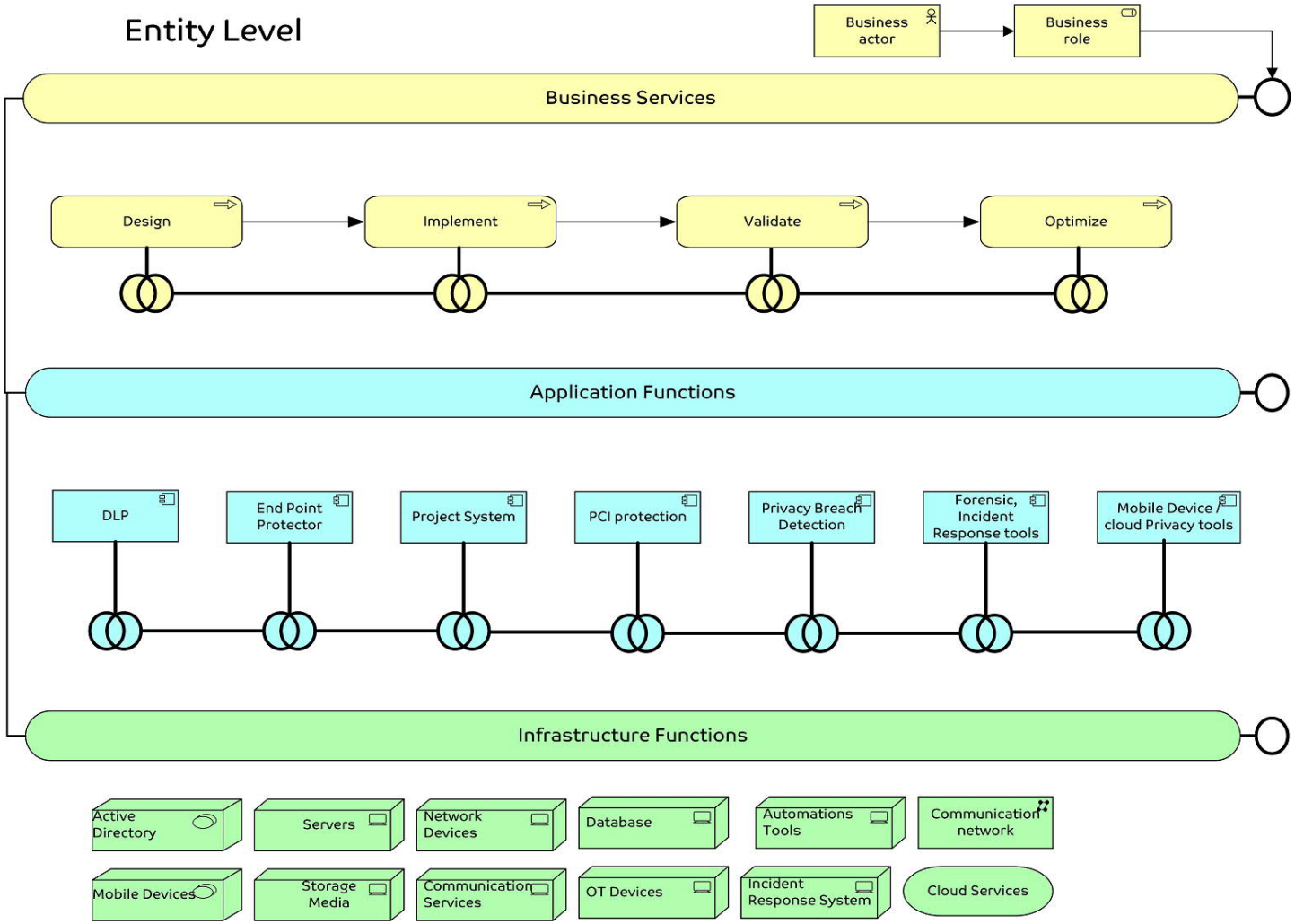
Service Name: Data Privacy	
Description	Privacy is concerned with any personal identifiable information or other sensitive information that is collected, stored, used, and finally destroyed / deleted – in digital form or otherwise. Data Privacy capability helps establish a framework that contains framework that if implemented, maintained, and improved periodically will help to protect information privacy by specifying what can and cannot be done with the personal information
Process Phases	**Activities/Controls**
Design	• Establish an overall sense of direction and principles for action with regards to protection of Data/Information in the Entity • Establish the Governance for management of Privacy Framework • Identify the privacy impact assessment methodology that is suited to the organization, and the identified privacy requirements • Provide direction and support for implementing controls to protect Data/Information, compliance with applicable laws and regulations and to implement best practice • Define purpose for collection, lawful/rightful usage, disclosure, transfer, retention, archival and disposal process of private data • Define process for handling non-compliance, breaches and dealing with rights and protection of whistle blowers
Implement	• Establish Privacy Impact Assessment (PIA) to analyse how Personally Identifiable Information (PII) is collected, used, disseminated, and maintained • PIA and implementation of controls shall be performed on those Personal Identifiable Information (PII) data elements as identified in the PII inventory • The PIA report shall identify and assess the impacts of all business functions on the privacy of personal information of customers, employees, and vendors/contractors together with the suggested remediation for treating or mitigating those impacts • Entity understands categories of the Data/Information that it processes, sand the level of risk associated to the processing of that information • Access to private data must be based on 'Need-to-know' and 'Segregation of Duties' basis • Disclosures of Data/Information to third parties or processing by any other organization are managed in compliance with data protection legislation and good practices • Keep records regarding data processing • Implement controls to protect personal data to prevent and detect data attacks and breaches

Service Name: Data Privacy	
Validate	• Establish a process for evaluating the effectiveness of privacy structure and continuously improve the composure of the Entity • Conduct periodic audits and performance reviews of the Privacy Management Framework • Review if implemented privacy and security controls are functioning as required
Optimize	• Embed Privacy within the organization's culture • Include management of Data/Information as part of organizational core values and effective management • Establish a process for evaluating the effectiveness of privacy structure and continuously improve the composure of the organization • Employees and stakeholders are aware of how they contribute to the achievement of the organization's privacy objectives and the consequences of nonconformity • Raise, enhance and maintain awareness of Privacy through an ongoing education and awareness programme for all employees and stakeholders

12.3 Data Privacy Capability Model

Following figure illustrates an architecture model of various functions established for Data Privacy capability at entity level:

Figure 77: Data Privacy Capability Model



Above figure defines the Data Privacy capability model in layered approach:

- The **Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- The **Application Functions layer** supports the business layer with application services which are realized by (software) application components.
- The **Infrastructure layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

12.4 Information Flow at various levels

There is no requirement to share data privacy service information to the sector/national level.

12.4.1 Services expected at each level

Data privacy service will be applicable to all the applications used for world cup irrespective of the level (i.e. Entity/Sector/National) it is being used.

12.5 Milestones

Following milestones have been defined for Data Privacy:

- The personal information in custody is adequately protected against threats to maintain its security
- Employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches
- The limit of the use of personal information has been established including the business purposes of the data for which it has been collected
- Awareness of privacy requirements is an integral part of the day to day operation of every staff at the Entity and all the staffs understand the importance of privacy practices and their responsibilities for maintaining privacy
- Staff are fully aware of the process required for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal information
- All the contracted third parties are collecting, storing and processing personal information on behalf of Entity provides adequate data protection
- Applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal information are adhered to

12.6 Key domains and suggested controls for enhancing Data Privacy

Following are list of samples recommended controls for various domains within Data Privacy. The controls are applicable to people, process and technology elements

Table 76: Suggested controls for enhancing Data Privacy

Domain	Sample List of Controls
Management/ Governance	• Organization has formalized a privacy policy comprising Notice, Choice and consent, Collection, Use, Retention and disposal, Access, Disclosure to third-parties, Security for privacy, monitoring, enforcement and adequately address the organization's privacy objectives. • Organization has defined and described what is considered Personally Identifiable Information (PII) • Organization has formalized a process to identify the presence of PII across its processes • Organization has defined a privacy organization structure along with the roles and responsibilities of the members • Organization has defined a Privacy Impact Assessment (PIA) and risk assessment framework and PIAs are conducted for all systems/ processes handling personal information • Organization has established a process to keep track of the applicable legal and regulatory privacy requirements and changes across the globe • Organization ensures that internal personnel or external advisors review contracts to check their consistency with organization’s requirements for privacy • Organization has formalized a process to handle any disputes or complaints with respect to handling of personal information and has defined escalation process

Domain	Sample List of Controls
	• Notify any breach of personal information or possibility of breach, immediately to organization's Privacy team/Information security team • Processes are in place to perform introductory induction training for all the new employees at the time of on-boarding. The training material includes sections on security, privacy and how to report breaches. • Organization conduct regular privacy related training and awareness sessions (including GDPR topics) for internal employees and relevant third-parties • Organization conduct specific role-based trainings for the employees working with PII • Organization has documented an Incident Management process to handle and report incidents related to privacy breach • Organization documents instances of non-compliance to privacy policies and procedures • Organization documents all the Personally Identifiable Information (PII) processing operations carried out under its responsibility • Organization established processes through which data subjects may inquire or file complaints about organization's privacy practices
Security for privacy	• Organization must ensure that it facilitate the execution of client's defined access control policy for user creation, user modification and user deletion/termination at individual and group level • Organization must ensure that client's authorization and approval matrix is practiced for providing access to view, modify or delete PII content in the client's application • Organization must ensure that unique user ID's are available for accessing the client's application • Organization conducts user ID and access level reviews periodically for the users accessing PII over client's application thereafter informing the discrepancy to the client for revoking any additional access • Organization must ensure that role-based access is assigned to the users accessing PII and any discrepancy should be immediately informed to the client • If an ID is required to be shared amongst multiple employees, then request for creation of generic ID from the client post obtaining approval from organization's Information Security team • Organization must ensure that disclosure of user ID credentials is restricted • Organization must ensure that administrative rights are restricted on local systems from where users access client's application • Organization must ensure that passwords are frequently changed on the applications as per the client's Information Security policy • Notify to client immediately, if there's an access available to personal information through reports/application/emails/any other means, without a business need • Organization notify the client and third parties (who hold personal information) in case of any amendments or deletions to a data subject's PII • Organization has a defined and documented access control policy for user creation, user modification and user deletion /termination at individual and group level • Organization has defined authorization and approval matrix for providing access to view, modify or delete • Organization create unique user ID's for accessing the application

Domain	Sample List of Controls
	• Organization conducts user ID and access level reviews periodically • Organization assigns role-based access to the users • If an ID is required to be shared amongst multiple employees, then request for a generic ID and obtain approval from organization's Information Security team. • Organization has restricted disclosure of user ID credentials • Organization has restricted administrative rights on local systems • Frequently change the password's as per the organization's Information Security policy. • Notify to organization privacy team immediately, if there's an access available to personal information through reports/application/emails/any other means, without a business need. • All applications involving PII should have capability to generate audit trails • Photo-copies of any physical document containing customer personal information is not maintained, unless required for specific business purpose • Hard copy of PII document created for any business purpose should be safely stored under lock or other access control mechanisms • Organization has restricted use of data storage and data recording devices like USB, Mobile devices, etc. In case it is required for business purposes specific approvals and exceptions are to be taken • Organization has ensured that client's data stored on organization's hard drive is encrypted • If client's data is stored on organization's file server audit trails are created for the PII • Organization maintains the list of users who have access to the datacentres where applications containing PII is hosted. The list is reviewed on a periodic basis to keep it updated
Collection	• In case when data is collected directly from data subjects, organization has a process to provide notice prior to collecting their personal information • In case when data is collected directly from data subjects, organization has a process for obtaining implicit/ explicit written consent when personal information is collected and for cases where personal information/ sensitive personal information is collected and used for purposes not previously mentioned • In case when data is collected directly from data subjects, organization seek consent from a competent person before collecting, processing and disclosing PII concerning a child • n case when data is collected directly from data subjects, organization provide notice about its privacy policies and procedures in the following scenarios: - At or before the time personal information is collected, or as soon as practical thereafter, - At or before the entity changes its privacy policies and procedures, or as soon as practical thereafter, - before personal information is used for new purposes not previously identified • In case when data is collected directly from data subjects, organization ensure that the privacy notice is conspicuous and uses clear language

Domain	Sample List of Controls

	• In case when data is collected directly from data subjects, organization has formalized a process to ensure that the personal information collected is used
	  - in conformity with the purposes identified in the privacy notice
	  - in agreement with the consent received from the individual
	  - in compliance with applicable laws and regulations"
	• In case when data is collected directly from data subjects, organization ensure that the data processing systems used to collect, and process personal data gather only necessary information required for business use
	• In case when data is collected directly from data subjects, organization communicate that they can contact the entity in case their PII needs any correction/modification

Access	• In case when data is collected directly from data subjects, organization has made provisions for data subjects to access their personal information and request or make amendments/ modifications as desired • In case data subjects approach organization for any change or modification in their PII, organization informs the client, then document and manage the changes that a data subject makes to his/her PII • In case when data is collected directly from data subjects, organization has informed them about the process they must follow to update or correct their PI records (e.g.: in writing, by phone, by e-mail, or by using organization's Web site • In case when data is collected directly from data subjects, organization verify the accuracy and completeness of PII that an individual update by means of a self-declaration form or supporting evidence provided at the time of making those changes

Use, Retention and Disposal	• Ensure that the organization only receives the minimum amount of personal data required to conduct processing as per the contractual requirements with client. Excess personal data should either be masked or not shared
	• In case when data is collected directly from data subjects, ensure that the organization only collects the minimum amount of personal data required to conduct processing as per the requirements. Excess personal data should either be masked or not shared
	• Organization review complaints/grievances to identify indications of any misuse of PI by third parties
	• Formally agree on the retention periods for which customer's personal information shall be retained by the organization
	• Organization has a formalized process to ensure that personal information is retained for no longer than necessary to fulfil the stated purposes unless a law or regulation specifically requires otherwise
	• "Dispose of the personal information of customer (including those stored in backups) in following secure ways:
	  - Permanent deletion of personal information in electronic form.
	  - Shredding off the physical hard copies of personal information."

Transfer and Disclosures	• Cross-border transfer of personal data shall only be permissible if privacy is ensured through contractual clauses or binding corporate regulations • Organization has a process in place to document and maintain the record of the PII hardcopy and media movements from the facilities • Transfer of PII from one client process to another should be over secure channels

Domain	Sample List of Controls
	• Organization do not disclose the personal information to a sub-contractor/other party in any form without prior consent from the client • If third party or sub-contractor and vendors (support/ enhancement/ troubleshooting/ administration) is aligned in the process involving PII, non-disclosure agreement (NDA) to be signed and privacy requirement to be mentioned in the contract • Conduct periodic self-assessment or reviews or due diligence of third-parties to demonstrate compliance to privacy requirements • Transfer all documentary and other materials relating to the PII of the customers promptly to the organization on termination of contract between third party/sub-contractors and Entity • Restrict forwarding of emails containing customer's personal information to IDs other than the ones required for the processing over secure channels • In case data belonging to EU citizen is shared with any third party, organization must confirm that the third party complies with GDPR

12.7 Skills required for Data Privacy

Following are the skills expected from personnel executing Data Privacy activities:

- Excellent working knowledge of data protection legislation and practices
- Knowledge of Industry or sector specific services business models and products
- Experience assessing and defining system specifications preferably in relation to compliance with data protection and privacy regulations
- Provide data privacy program and requirements subject matter expertise as key resource and point of contact to business, functions, and other key stakeholders
- Ability to conduct and evaluate privacy impact assessments (PIA) activities and/or business consulting for new product or service development, material changes to existing products or services, third party vendor privacy assessments and business consultation requests as required by the PIA standards and procedures. Analyse results of assessments to identify trends and patterns that can be used to improve review efficiencies, existing processes, and standards
- Experience in leading business level privacy assessments that results in program enhancement, mitigation and remediation activities as appropriate
- Design, direct and execute data protection and privacy operational compliance monitoring activities in collaboration and coordination with the organization's security, compliance, audit, risk management and other related corporate functions as appropriate
- Suggested professional certifications which can help personnel to attain skills for the services defined under Data Privacy:
    - The Certified Information Privacy Professional (CIPP), IAPP
    - The Certified Information Privacy Manager (CIPM), IAPP
    - The Certified Information Privacy Technologist (CIPT), IAPP

12.8 Technology

There are various data leakage prevention (DLP) technological solutions and tools available in the market to protect and enhance data privacy at the organization. Some of the key features of the DLP tools / solutions:

- **Rules-Based/Regular Expressions:** This is the most common analysis technique available in both DLP products and other tools with DLP features
- **Database Fingerprinting:** Sometimes called Exact Data Matching, this technique takes either a database dump or live data (via ODBC connection) from a database and only looks for exact matches
- **Exact File Matching:** With this technique you take a hash of a file and monitors for any files that match that exact fingerprint. Some consider this to be a contextual analysis technique because the file contents themselves are not analysed.
- **Partial Document Matching:** This technique looks for a complete or partial match to protected content. You could build a policy to protect a sensitive document, and the DLP solution will look for either the complete text of the document, or even excerpts as small as a few sentences
- **Statistical Analysis:** Use of machine learning, Bayesian analysis, and other statistical techniques to analyse a corpus of content and find policy violations in content that resembles the protected content
- **Conceptual/Lexicon:** This technique uses a combination of dictionaries, rules, and other analyses to protect nebulous content
- **Categories:** Pre-built categories with rules and dictionaries for common types of sensitive data, such as credit card numbers/PCI protection, HIPAA, etc.
- **Data Location:** covers data in motion, data at rest and data in use
- **Integration** with major IT systems - AD, email, firewalls, proxies, web portals etc.
- Supports Agent-Based Scanning, Memory-Resident Agent Scanning, Application Integration
- Once a policy violation is discovered, a DLP tool can take a variety of actions:
    - **Alert/Report**: Create an incident in the central management server just like a network violation.
    - **Warn**: Notify the user via email that they may be in violation of policy.
    - **Quarantine/Notify**: Move the file to the central management server and leave a text file with instructions on how to request recovery of the file.
    - **Quarantine/Encrypt**: Encrypt the file in place, usually leaving a plain text file describing how to request decryption.
    - **Quarantine/Access Control**: Change access controls to restrict access to the file.
    - **Remove/Delete**: Either transfer the file to the central server without notification, or simply delete it.

Other Features and Integrations - the lists above include most of the DLP Light, feature, and integration options in the market; but there are few categories that don't fit quite as neatly into some network/endpoint/storage divisions:

- **SIEM and Log Management**: All major SIEM tools can accept privacy related alerts from DLP solutions and possibly correlate them with other collected activity. Some SIEM tools also offer DLP features, depending on what kinds of activity they can collect to perform content analysis on. Log management tools tend to be more passive, but increasingly include some similar basic DLP-like features when analysing data. Most DLP users tend to stick with their DLP solutions for incident workflow, but we do know cases where alerts are sent to the SIEM for correlation or incident response, as well as when the organization prefers to manage all security incidents in the SIEM
- **Enterprise Digital Rights Management**: Multiple DLP solutions now integrate with Enterprise DRM tools to automatically apply DRM rights to files that match policies. This makes EDRM far more usable for most organizations, since one major inhibitor is the complexity of asking users to apply DRM rights. This integration may be offered both in storage and on endpoints, and we expect to see these partnerships continue to expand

- **E-mail Encryption**: Automatic encryption of emails based on content was one of the very first third-party integrations to appear on the market, and a variety of options are available. This is most frequently seen in financial and healthcare organizations (including insurance) with strict customer communications security requirements

12.9 Mapping with Industry Standards

Table 77: Data Privacy activities mapping industry cyber security standards – Part I of II

Service Name — Data Privacy						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Design	Establish an overall sense of direction and principles for action with regards to protection of Data/Information in the Entity	6.2 PS 3				
Design	Establish the Governance for management of Privacy Framework	6.2 PS 3				
Design	Identify the privacy impact assessment methodology that is suited to the organization, and the identified privacy requirements					
Design	Provide direction and support for implementing controls to protect Data/Information, compliance with applicable laws and regulations and to implement best practice	10.2 SM 6	A.10.2.1	CIS CSC 19		
Implement	Establish Privacy Impact Assessment (PIA) to analyse how Personally Identifiable Information (PII) is collected, use, disseminated, and maintained		AR-2, DM 1, P-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1			
Implement	Privacy impact assessment and implementation of controls shall be performed on those Personal		AR-2			

Service Name — Data Privacy						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
	Identifiable Information (PII) data elements as identified in the PII inventory					
Implement	The PIA report shall identify and assess the impacts of all business functions on the privacy of personal information of customers, employees, and vendors/contractors together with the suggested remediation for treating or mitigating those impacts		DM 1, P-1, AP-2, AR-4, IP-1, SE-1, SI-12, TR-1, AC-2, AP-1, TR-1, TR-2			
Implement	Entity understands categories of the Data/Information that it processes, and the level of risk associated to the processing of that information		AR-8, IP-3, TR-1, TR-2, AR-1, AR-4, AR-5, AT-1, DM-1, PM-5			
Implement	Disclosures of Data/Information to third parties or processing by any other organization are managed in compliance with data protection legislation and good practices		AR-1, AR-5, SA-4, AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1			
Implement	Keep records regarding data processing					
Implement	Implement controls to protect personal data to prevent and detect data attacks and breaches	10.2 SM 6, 11 DR 3	A.10.2.1, DM-3			
Validate	Establish a process for evaluating the effectiveness of privacy structure and continuously improve the composure of the Entity	10.2 SM 3	AR-6, IP-3			
Validate	Conduct periodic audits and performance reviews of the Privacy Management Framework		A.12.4.1, A.16.1.2,			

Service Name — Data Privacy						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
			A.16.1.4 A.12.4.1, A.16.1.7, AR-6, IP-3			
Validate	Review if implemented privacy and security controls are functioning as required	10.2 SM 3	AR-4, AR-6, AR-7, AU-1, AU-2, AU-3, AU-6, AU-12, CA-7, TR-1, UL-2			
Optimize	Embed Privacy within the organization's culture		AR-5, AR-3, AT-2, AT-3, TR-1			
Optimize	Include management of Data/Information as part of organizational core values and effective management					
Optimize	Employees and stakeholders are aware of how they contribute to the achievement of the organization's privacy objectives and the consequences of nonconformity		AR-5, AR-3, AT-2, AT-3, TR-1			
Optimize	Raise, enhance and maintain awareness of Privacy through an ongoing education and awareness programme for all employees and stakeholders		AR-5, AR-3, AT-2, AT-3, TR-1			

Table 78: Data Privacy activities mapping industry cyber security standards – Part II of II

Service Name — Data Privacy							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Design	Establish an overall sense of direction and principles for action with regards to protection of Data/Information in the Entity				164.308(a)(1) 164.308(b)		Arts 5, 24, 25, 26, 28, 32, 33 and 34 Rec 74, 77, 78, 83-86
Design	Establish the Governance for management of Privacy Framework				164.308(a)(1)(i) 164.316, 164.308(a)(1)(i) 164.308(a)(2) 164.308(a)(3) 164.308(a)(4) 164.308(b) 164.314		Art 24, 37-39, 55-59 Rec 97
Design	Identify the privacy impact assessment methodology that is suited to the organization, and the identified privacy requirements						Art 25, 35 Rec 74, 78, 83, 84, 89-95
Design	Provide direction and support for implementing controls to protect Data/Information, compliance with applicable laws and regulations and to implement best practice	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5	NIST SP 800-53 Rev. 4	PCI DSS v3.2 3.1, 9.8, 12.10	164.306 164.308 164.310 164.312 164.314 164.316		Arts 5, 24, 25, 26, 28, 32, 33 and 34 Rec 74, 77, 78, 83-86
Implement	Establish Privacy Impact Assessment (PIA) to analyse how Personally Identifiable Information	A.18.1.1, A.18.1.2, A.18.1.3,					Art 25, 35 Rec 74, 78, 83, 84, 89-95

Service Name — Data Privacy							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
	(PII) is collected, used, disseminated, and maintained	A.18.1.4, A.18.1.5					
Implement	Privacy impact assessment and implementation of controls shall be performed on those Personal Identifiable Information (PII) data elements as identified in the PII inventory	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5					Art 25, 35 Rec 74, 78, 83, 84, 89-95
Implement	The PIA report shall identify and assess the impacts of all business functions on the privacy of personal information of customers, employees, and vendors/contractors together with the suggested remediation for treating or mitigating those impacts	A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5					Art 25, 35 Rec 74, 78, 83, 84, 89-95
Implement	Entity understands categories of the Data/Information that it processes, and the level of risk associated to the processing of that information						Art 9
Implement	Disclosures of Data/Information to third parties or processing by any other organization are managed in compliance with data protection legislation and good practices				164.308(a)(6)		Art 44, 45,46,47,48,49,50
Implement	Keep records regarding data processing						Art 28,29,30, 32

Service Name — Data Privacy							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Implement	Implement controls to protect personal data to prevent and detect data attacks and breaches						Art 32,33,34
Validate	Establish a process for evaluating the effectiveness of privacy structure and continuously improve the composure of the Entity	A.18.2.1, A.18.2.2					Art 10
Validate	Conduct periodic audits and performance reviews of the Privacy Management Framework	A.18.2.1, A.18.2.2			164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C) 164.310(a)(2)(iv) 164.310(d)(2)(iii) 164.312(b)		
Validate	Review if implemented privacy and security controls are functioning as required	A.18.2.1					
Optimize	Embed Privacy within the organization's culture						
Optimize	Include management of Data/Information as part of organizational core values and effective management						
Optimize	Employees and stakeholders are aware of how they contribute to the achievement of the organization's privacy objectives and the consequences of nonconformity				164.308(a)(2) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(4) 164.310(a)(2)(iii)		

Service Name — Data Privacy							
Process Phases	**Activities/Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference — HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
					164.312(a)(1) 164.312(a)(2)(ii)		
Optimize	Raise, enhance and maintain awareness of Privacy through an ongoing education and awareness programme for all employees and stakeholders						

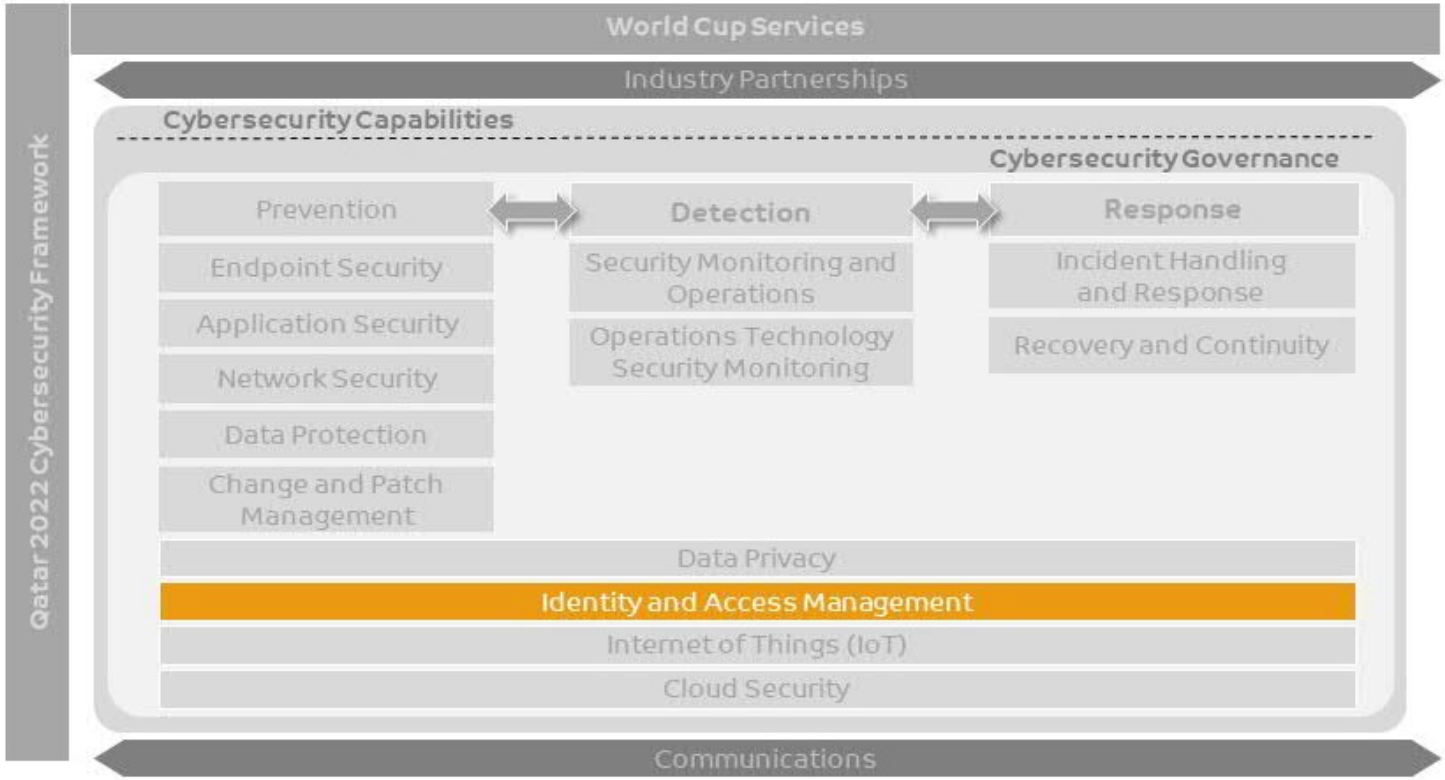
13 Identity and Access Management

13. Capability Description – Identity and Access Management

A capability that manage the right individuals to access the right resources at the right times for the right reasons. Identity and access management (IAM) addresses the mission-critical need to ensure appropriate access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices with respect to services provided for the world cup.

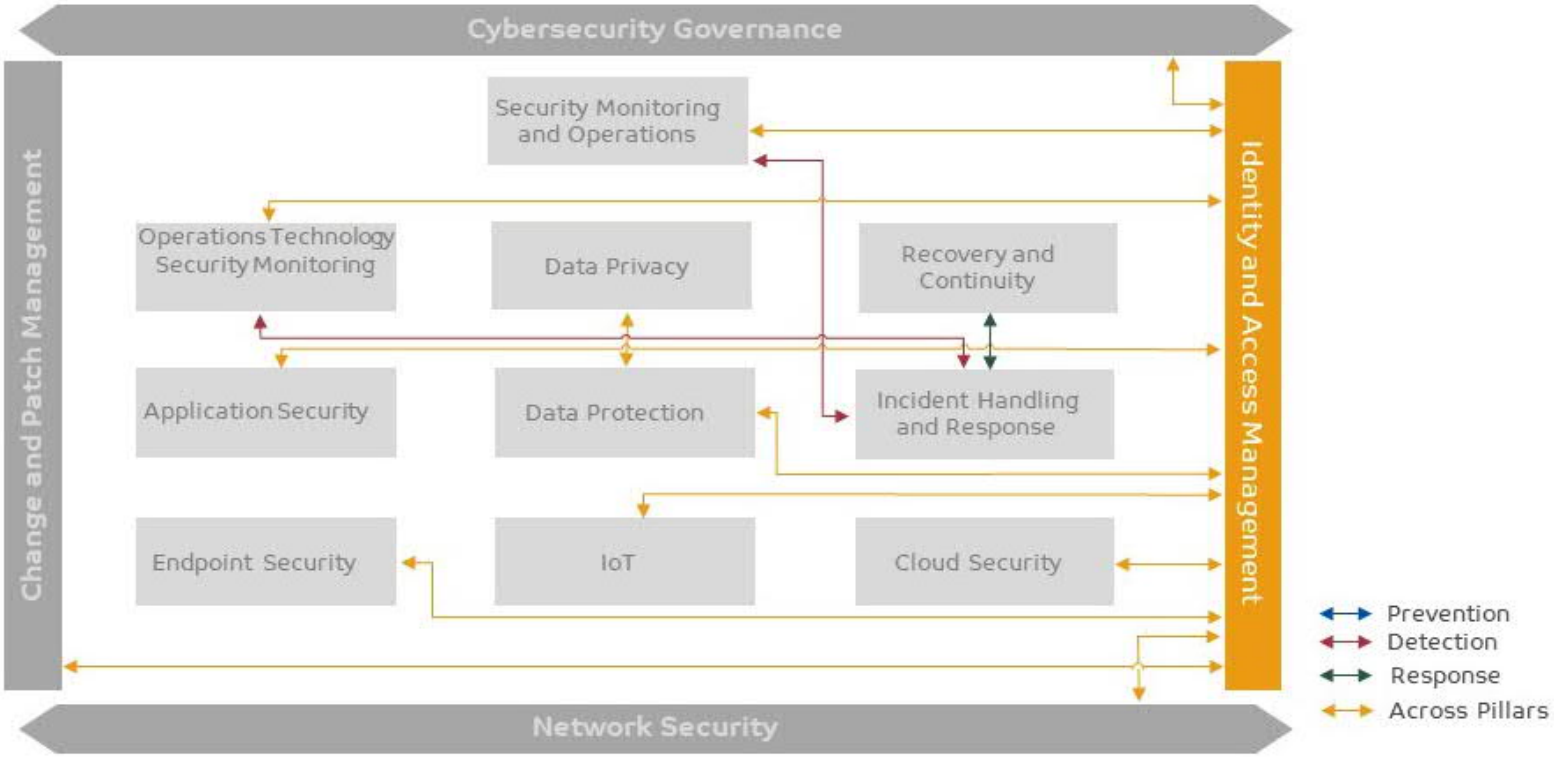
This chapter focuses on 'Identity and Access Management' capability, and covers all three pillars of world cup cybersecurity capabilities (Prevention, Detection and Response)

Figure 78: Cybersecurity Capability – Identity and Access Management



Following figure depicts linkage of Incident Handling and Response with other cybersecurity capabilities defined in the framework

Figure 79: Identity and Access Management linkage with other capabilities



13.1 Prerequisites

Following are the prerequisites, which are required to be accomplished for identity and access management capability:

- Directory services have been implemented
- Unique, Digital identities have been identified including people (internal employees, contractors, external constituents or business partners), systems, and services.
- Remote access logins are considered while defining strategy for identity and access management
- Assets to be protected have been identified including endpoint, network, application, data and cloud devices or services (refer to cybersecurity governance, risk assessment, endpoint security, application security, network security, data protection, data privacy and cloud security capability chapters)

- Appropriate logs have been enabled on identified information assets for collection and analysis (endpoint security, network security and application security capability chapters)
- The Operations/IT team should be notified for any change management activities (refer to change and patch management capability chapter)
- Consider mobility and cloud as future drivers for how IAM could be enforced having a maturity self-measurement mechanism
- Security risks have been identified for identities and its access rights during the risk assessment

13.2 Identity and Access Management Service

From world cup perspective, the ***Table 79: Identity and Access Management Service*** describes respective activities that needs to be conducted for the identity and access management (IAM) capability. From preparation/planning viewpoint, the following steps must be considered:

- Establish formal IAM policies, procedures and guidelines
- Define IAM program scope
- Establish governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Define acceptance standards
- Deploy/configure appropriate solutions to align with established policies and standards
- Deploy and train team members to support IAM processes
- Identify opportunities of automation where applicable
- Define acceptable IAM services levels for remediation activity
- Continually improve IAM policy, procedure and guidelines with changing risks and lessons learned

Table 79: Identity and Access Management Service

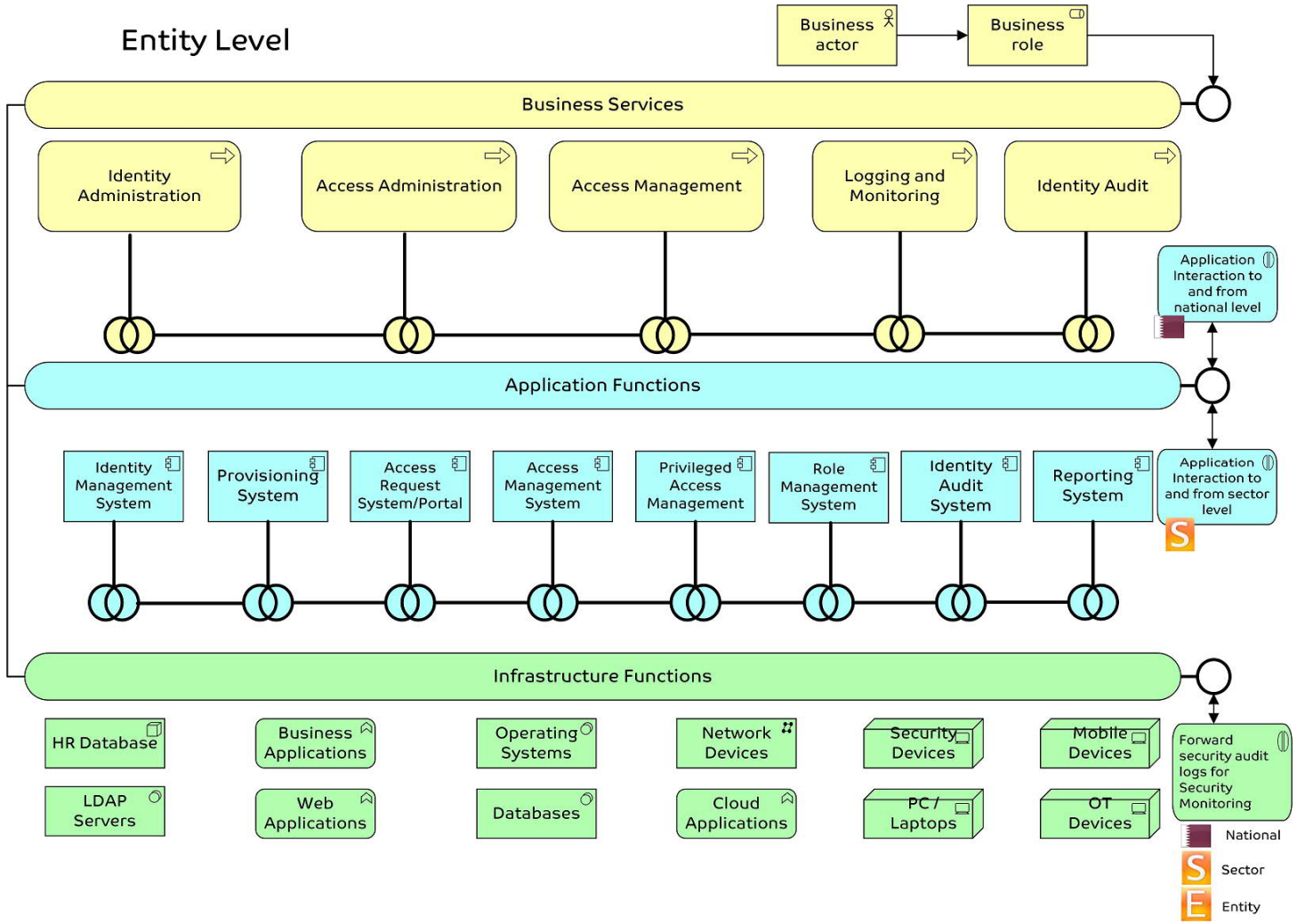
Service Name: Identity and Access Management	
Description	It is the combination of processes, technologies and people used by an organization to manage identities access to services, systems, data and resources including IT, Cloud OT and IoT systems.
Process Phases	**Activities/Controls**
Identity Administration	• Establish processes and tools to manage identities of users during onboarding, transfer, and off-boarding across platforms and applications - Unique ID generation - Identity profile management - Authoritative source data management
Access Administration	• Establish processes and tools to create, modify, delete and monitor user accounts and entitlements - Provisioning workflow - Privileged access management

Service Name: Identity and Access Management	
	- Credential management - Role management - Fine-grained access policy administration
Access Control	• Processes and tools used to control users' access to protected resources by various authentication and authorization mechanisms such as multi-factor authentication. - Shared authentication service - Single sign-on - Identity federation - Fine-grained access policy enforcement
Logging and Monitoring	• Establish processes and tools used to capture, aggregate, and correlate IAM specific logs for proactive and reactive analysis - Log consolidation and analysis - Identity and access reporting - Privileged access monitoring
Identity Audit	• Establish processes and tools to understand the health of the various IAM components - Identify opportunities for improvement in processes - Provide evidence for access reviews, audit activities, - Demonstration of compliance to policies, standards, and regulations. - Access and review certification - Policy compliance monitoring - Role and definition certification

13.3 Identity and Access Management Capability Model

Following figure illustrates an architecture model established for Identity and Access management capability at Entity level:

Figure 80: Identity and Access Management Capability Model



Above figure defines the Identity and Access Management capability model in layered approach:

- The **Business Services layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- The **Application Functions layer** supports the business layer with application services which are realized by (software) application components.

- The **Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

13.4 Information Flow in various levels

Identity information related to access control based on federated identity such as Government IDs, national level PKI etc. must be shared among all levels (i.e. National, Sector and Entity).

13.4.1 Services expected at each level

Following table describes services expected at each level of world cup ecosystem:

Table 80: Services expected at each level

Entity	Sector	National

• Identity Administration
• Access Administration
• Access Control
• Logging and Monitoring
• Identity Audit
	• Access Control
	  - Identity Federation (for example in Government section)
	• Logging and monitoring
	  - Log consolidation and analysis
	  - Reporting
		• Access Control
		  - Identity Federation (i.e. National PKI)
		• Logging and monitoring
		  - Log consolidation and analysis
		  - Reporting

Compendium – Identity and Access Management

13.5 Milestones

Following milestones have been defined for Identity and Access Management:

- Approval processes capable of supporting IAM approver notifications, delegation, and escalations to approve within SLA
- Configurable IAM approval, provisioning, and de-provisioning workflows

- Centralized access and enforcement for access requests
- Reporting and continuous access use monitoring
- Configurable processes that support user life cycle event triggered access reviews and certifications

13.6 Identity Lifecycle

Figure 81: Identity and Access Management Lifecycle

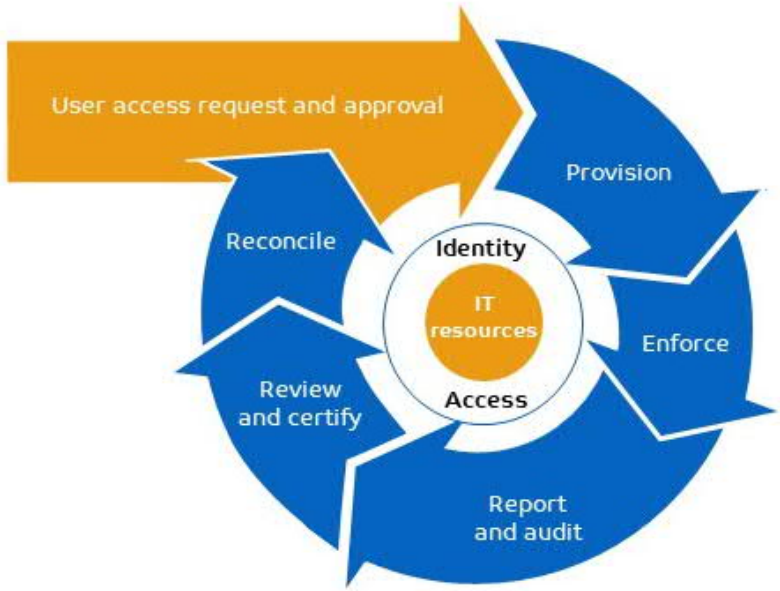


Figure shows graphical representation of the identity lifecycle among various activities of Identity and Access Management capability.

An identity lifecycle starts from the moment when the user's access is requested and approved. Examples of identities are an employee account, IT administrator account, a citizen's identity as a national of a country.

Following table describes results expected at each phase of identity lifecycle:

Table 81: Identity lifecycle phases

Phases	Definition
User access request and approve	Gaining access to the applications, systems and data required
Provision/de-provision	Granting users appropriate entitlements and access in a timely manner Revoking access in a timely manner when no longer required due to termination or transfer
Enforce	Enforcing user access to applications and systems using authentication and authorization Enforcing compliance with access management policies and requirements
Report and audit	Defining business-relevant key performance indicators (KPIs) and metrics

Phases	Definition
	Auditing user access
Review and certify	Reviewing user access periodically to realign it with job function or role
Reconcile	Enforcing that access within the system, matching approved access levels

13.7 Skills required for Identity and Access Management

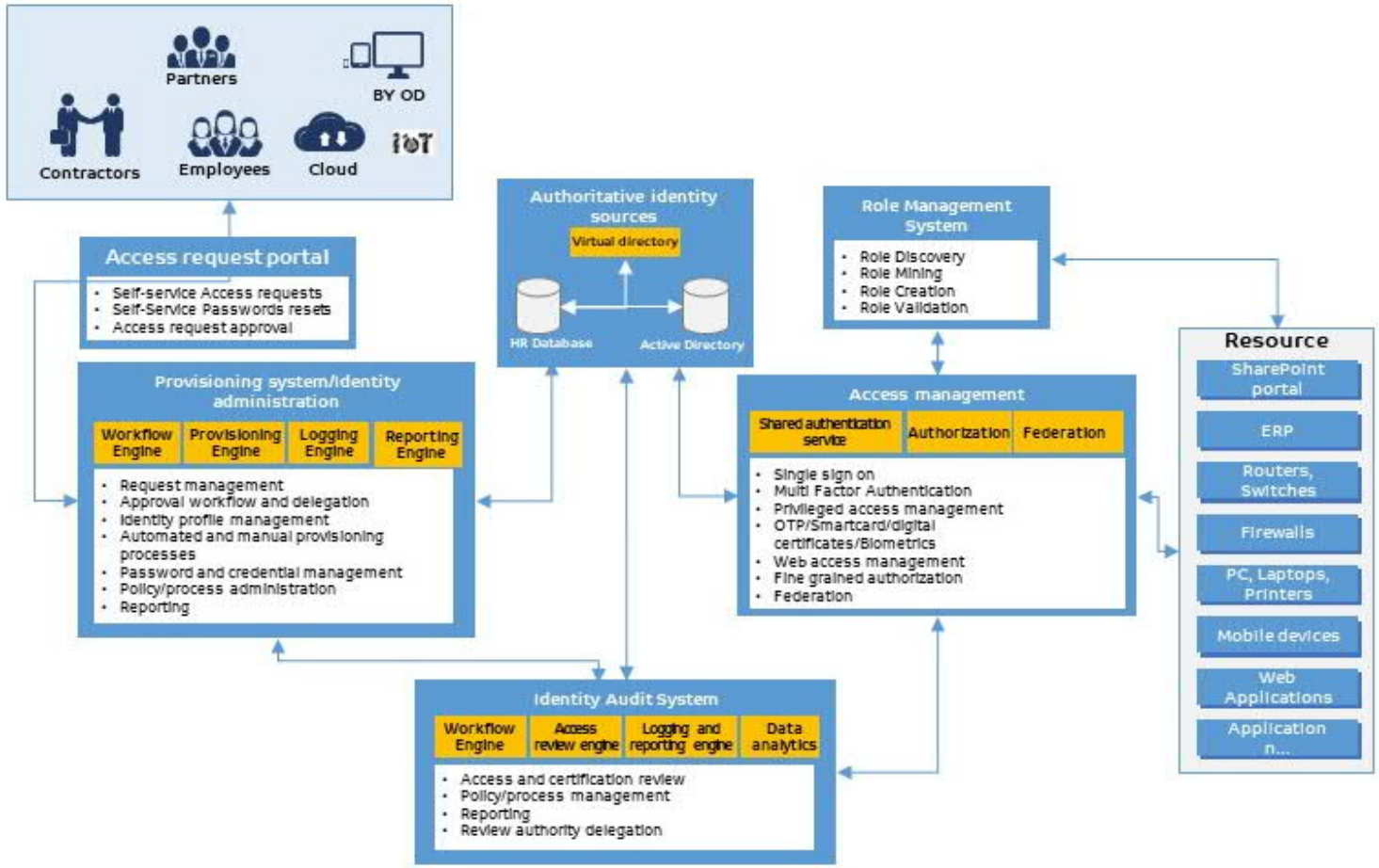
Following are the skills expected from personnel executing Identity and Access Management activities:

- Analyse and specify the business/functional requirements for IAM to all system workflows
- Ensure business and functional processes meet operational needs
- Analyse, design and develop the required identity management processes and workflows
- Ability to issue new identities, check and proof identities
- Resolve identity duplicates and conflicts
- Perform provision and integrate new systems with the IAM structure
- Manage the data feeds into IAM and distribution to target systems
- Administration, support and ongoing system configuration of the IAM solution
- Management of the Single Sign-On, federation, authentication and authorization systems
- Ability to collect, correlate and report on IAM contributions to compliance, security and overall IAM performance
- Analyse and review legal and compliance requirements

13.8 Technology

Following figure shows which technologies are vital and should be considered for a successful implementation of identity and access management capability

Figure 82: IAM Conceptual Architecture



IAM functions are typically built using solution components that include the following features:

- **Identity & Access Administration:** provides users with the capability to request access rights and allows self-service profile and password management. Identity Management also provides delegated administration capability that allows business units or partners to manage their own user communities
- **Access Control:** provides user identification, authentication, secure session management, and authorization services to applications. Authentication includes reduced/single sign-on to reduce the number of user IDs and passwords to manage.

- **Provisioning**: automates the administration of user identities and resource access rights. Provisioning also provides workflow capabilities so that change requests can be routed for approval as required. Through Identity & Access Reconciliation, Provisioning also provides a consolidated repository view of organizational, user identity, and access rights information
- **Role Management:** provides the capability to mine (discover) enterprise and business-level roles, define roles as mappings of entitlements to resource access rights, update role definitions as the business changes and manage the relationship between roles and users
- **Entitlement Management:** enables fine-grained authorization by centralizing authorization policies and providing a shared service for applications to query to determine if a requested action should be allowed
- **Access Logging and Monitoring:** provides the capability to aggregate access usage logs from disparate applications and systems, enabling detection of potentially significant security events that require correlation of access use across multiple systems
- **Identity Audit:** provides the capability to effectively review user's current access to determine if it is appropriate based on their job function. Identity audit also provides the ability to apply access policies (e.g., Segregation of Duties) to the entitlement data under review

13.9 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards

Table 82: Identity and Access Management activities mapping industry cyber security standards – Part I of II

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identity Administration	Processes and tools to manage identities of users during onboarding, transfer, and off-boarding across platforms and applications	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identity Administration	Unique ID generation	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
Identity Administration	Identity profile management	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-20 AM-21 AM-22 AM-29 AM-30				
Identity Administration	Authoritative source data management	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
Access Administration	Establish processes and tools to create, modify, delete and monitor user accounts and entitlements	PS-9 NS-1 NS-2 AM-1 AM-2 AM-3 AM-4	7.3.2 7.3.3	16	4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4	SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-9 AM-15 AM-24 AM-28 AM-29 AM-31 AM-5 AM-32 AM-33 NS-8 SS-31 NS-2 AM-27 AM-26				
Access Administration	Provisioning Workflow (On-Board, Move/Update, Revoke)	PS-9 NS-1 NS-2 AM-1 AM-2 AM-3 AM-4 AM-9 AM-15 AM-24 AM-28 AM-29 AM-31 AM-5	7.3.2 7.3.3	16	4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4	SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-32 AM-33 NS-8 SS-31 NS-2 AM-27 AM-26				
Access Administration	Privileged access management	PS-9 NS-1 NS-2 AM-1 AM-2 AM-3 AM-4 AM-9 AM-15 AM-24 AM-28 AM-29 AM-31 AM-5 AM-32 AM-33 NS-8 SS-31 NS-2 AM-27 AM-26	7.3.2 7.3.3	16	4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4	SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Access Administration	Credential management (Password Management)	PS-9 NS-1 NS-2 AM-1 AM-2 AM-3 AM-4 AM-9 AM-15 AM-24 AM-28 AM-29 AM-31 AM-5 AM-32 AM-33 NS-8 SS-31 NS-2 AM-27 AM-26	7.3.2 7.3.3	16	4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4	SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1
Access Administration	Role management: managing access based on job functions/responsibilities and related permissions.	PS-9 NS-1 NS-2 AM-1 AM-2 AM-3 AM-4	7.3.2 7.3.3	16	4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4	SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-9 AM-15 AM-24 AM-28 AM-29 AM-31 AM-5 AM-32 AM-33 NS-8 SS-31 NS-2 AM-27 AM-26				
Access Administration	Fine-grained access policy administration	PS-9 NS-1 NS-2 AM-1 AM-2 AM-3 AM-4 AM-9 AM-15 AM-24 AM-28 AM-29 AM-31 AM-5	7.3.2 7.3.3	16	4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4	SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-32 AM-33 NS-8 SS-31 NS-2 AM-27 AM-26				
Access Control	Processes and tools used to control users' access to protected resources by various authentication and authorization mechanisms	PS-9 NS-1 NS-8 AM-1 AM-2 AM-3 AM-15 AM-28 AM-31 AM-24 AM-5 AM-32 AM-33 NS-8 SS-31	6.6.19 7.2.1 7.2.3	3, 5, 12, 14, 15, 16, 18	4.3.3.7.3	SR 2.1
Access Control	Shared authentication service	PS-9 NS-1 NS-8 AM-1 AM-2 AM-3	6.6.19 7.2.1 7.2.3	3, 5, 12, 14, 15, 16, 18	4.3.3.7.3	SR 2.1

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-15 AM-28 AM-31 AM-24 AM-5 AM-32 AM-33 NS-8 SS-31				
Access Control	Single Sign-On	PS-9 NS-1 NS-8 AM-1 AM-2 AM-3 AM-15 AM-28 AM-31 AM-24 AM-5 AM-32 AM-33 NS-8 SS-31	6.6.19 7.2.1 7.2.3	3, 5, 12, 14, 15, 16, 18	4.3.3.7.3	SR 2.1
Access Control	Identity federation	PS-9 NS-1 NS-8 AM-1	6.6.19 7.2.1 7.2.3	3, 5, 12, 14, 15, 16, 18	4.3.3.7.3	SR 2.1

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-2 AM-3 AM-15 AM-28 AM-31 AM-24 AM-5 AM-32 AM-33 NS-8 SS-31				
Access Control	Fine-grained access policy enforcement	PS-9 NS-1 NS-8 AM-1 AM-2 AM-3 AM-15 AM-28 AM-31 AM-24 AM-5 AM-32 AM-33 NS-8 SS-31	6.6.19 7.2.1 7.2.3	3, 5, 12, 14, 15, 16, 18	4.3.3.7.3	SR 2.1

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Logging and Monitoring	Establish processes and tools used to capture, aggregate, and correlate IAM specific logs for proactive and reactive analysis			1, 3, 5, 6, 14, 15, 16	4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
Logging and Monitoring	Log consolidation and analysis			1, 3, 5, 6, 14, 15, 16	4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
Logging and Monitoring	Identity and access monitoring			1, 3, 5, 6, 14, 15, 16	4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
Logging and Monitoring	Privileged access monitoring	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identity Audit	Processes and tools to understand the health of the various IAM components	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
Identity Audit	Identify opportunities for improvement in processes	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-21 AM-22 AM-29 AM-30				
Identity Audit	Provide evidence for access reviews, audit activities	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
Identity Audit	Demonstration of compliance to policies, standards, and regulations.	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
		AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30				
Identity Audit	Access and review certification	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identity Audit	Policy compliance monitoring	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

Service Name — Identity and Access Management						
Process Phases	**Activities/Controls**	**Controls Reference — NIA (Qatar National Information Assurance Policy 2.0)**	**Controls Reference — NICS (National ICS Security Standard v3.0)**	**Controls Reference — CSC**	**Controls Reference — ISA 62443-2-1:2009**	**Controls Reference — ISA 62443-3-3:2013**
Identity Audit	Role and definition certification	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

Table 83: Identity and Access Management activities mapping industry cyber security standards – Part II of II

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Identity Administration	Processes and tools to manage identities of users during onboarding, transfer, and off-boarding across platforms and applications	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-02, IAM-05, IAM-12, IVS-12, AIS-01, AAC-03, GRM-06, GRM-09	
Identity Administration	Unique ID generation	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Identity Administration	Identity profile management	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Identity Administration	Authoritative source data management	CM-4 NS-33 NS-48 NS-60 NS-61 GS-4 AM-2 AM-4 AM-8 AM-9 AM-19 AM-20 AM-21 AM-22 AM-29 AM-30	7.2 7.3.3 7.4.3	1, 5, 15, 16	4.3.3.5.1	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Access Administration	Establish processes and tools to create, modify, delete and monitor user accounts and entitlements	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	7.1, 7.2, 8.1 (all), 8.2.2	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-02, IAM-05, IAM-12, IVS-12, AIS-01, AAC-03, GRM-06, GRM-09	
Access Administration	Provisioning Workflow (On-Board, Move/Update, Revoke)	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	7.1, 7.2, 8.1 (all), 8.2.2	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-02, IAM-05, IAM-12, IVS-12, AIS-01, AAC-03, GRM-06, GRM-09	
Access Administration	Privileged access management	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	7.1, 7.2, 8.1 (all), 8.2.2	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii)	IAM-02, IAM-05, IAM-12, IVS-12, AIS-01, AAC-03, GRM-06, GRM-09	

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
					164.312(a)(2)(iii) 164.312(d)		
Access Administration	Credential management (Password Management)	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	7.1, 7.2, 8.1 (all), 8.2.2	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-02, IAM-05, IAM-12, IVS-12, AIS-01, AAC-03, GRM-06, GRM-09	
Access Administration	Role management: managing access based on job functions/responsibilities and related permissions.	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	7.1, 7.2, 8.1 (all), 8.2.2	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-02, IAM-05, IAM-12, IVS-12, AIS-01, AAC-03, GRM-06, GRM-09	

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Access Administration	Fine-grained access policy administration	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	7.1, 7.2, 8.1 (all), 8.2.2	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-02, IAM-05, IAM-12, IVS-12, AIS-01, AAC-03, GRM-06, GRM-09	
Access Control	Processes and tools used to control users' access to protected resources by various authentication and authorization mechanisms	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	PCI DSS v3.2 6.4.2, 7.1, 7.2	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii)	IAM-02, IAM03, IAM-05, IAM-06, IAM-07, DSI-01, GRM-11, IVS-09	
Access Control	Shared authentication service	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	PCI DSS v3.2 6.4.2, 7.1, 7.2	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii)	IAM-02, IAM03, IAM-05, IAM-06, IAM-07, DSI-01, GRM-11, IVS-09	

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Access Control	Single Sign-On	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	PCI DSS v3.2 6.4.2, 7.1, 7.2	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii)	IAM-02, IAM03, IAM-05, IAM-06, IAM-07, DSI-01, GRM-11, IVS-09	
Access Control	Identity federation	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	PCI DSS v3.2 6.4.2, 7.1, 7.2	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii)	IAM-02, IAM03, IAM-05, IAM-06, IAM-07, DSI-01, GRM-11, IVS-09	
Access Control	Fine-grained access policy enforcement	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	PCI DSS v3.2 6.4.2, 7.1, 7.2	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii)	IAM-02, IAM03, IAM-05, IAM-06, IAM-07, DSI-01, GRM-11, IVS-09	
Logging and Monitoring	Establish processes and tools used to capture, aggregate, and correlate IAM specific logs for	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	AU Family	10.1, 10.2, 10.3, 10.6.1, 10.6.2	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C) 164.310(a)(2)(iv) 164.310(d)(2)(iii) 164.312(b)	IAM-01, IAM-07, IVS-01, SEF-04, SEF-05,	

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
	proactive and reactive analysis						
Logging and Monitoring	Log consolidation and analysis	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	AU Family	10.1, 10.2, 10.3, 10.6.1, 10.6.2	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C) 164.310(a)(2)(iv) 164.310(d)(2)(iii) 164.312(b)	IAM-01, IAM-07, IVS-01, SEF-04, SEF-05,	
Logging and Monitoring	Identity and access monitoring	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	AU Family	10.1, 10.2, 10.3, 10.6.1, 10.6.2	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C) 164.310(a)(2)(iv) 164.310(d)(2)(iii) 164.312(b)	IAM-01, IAM-07, IVS-01, SEF-04, SEF-05,	
Logging and Monitoring	Privileged access monitoring	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-01, IAM-07, IAM-10, AAC-01, IVS-06	
Identity Audit	Processes and tools to understand the health of the various IAM components	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7,	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B)	IAM-01, IAM-07, IAM-10, AAC-01, IVS-06	

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
			IA-8, IA-9, IA-10, IA-11		164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)		
Identity Audit	Identify opportunities for improvement in processes	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-01, IAM-07, IAM-10, AAC-01, IVS-06	
Identity Audit	Provide evidence for access reviews, audit activities	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-01, IAM-07, IAM-10, AAC-01, IVS-06	

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Identity Audit	Demonstration of compliance to policies, standards, and regulations.	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-01, IAM-07, IAM-10, AAC-01, IVS-06	
Identity Audit	Access and review certification	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-01, IAM-07, IAM-10, AAC-01, IVS-06	
Identity Audit	Policy compliance monitoring	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii)	IAM-01, IAM-07, IAM-10, AAC-01, IVS-06	

Service Name — Identity and Access Management							
Process Phases	**Activities / Controls**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
					164.312(a)(2)(iii) 164.312(d)		
Identity Audit	Role and definition certification	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.1, 8.2, 12.3	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)	IAM-01, IAM-07, IAM-10, AAC-01, IVS-06	

14

Internet of Things (IoT)

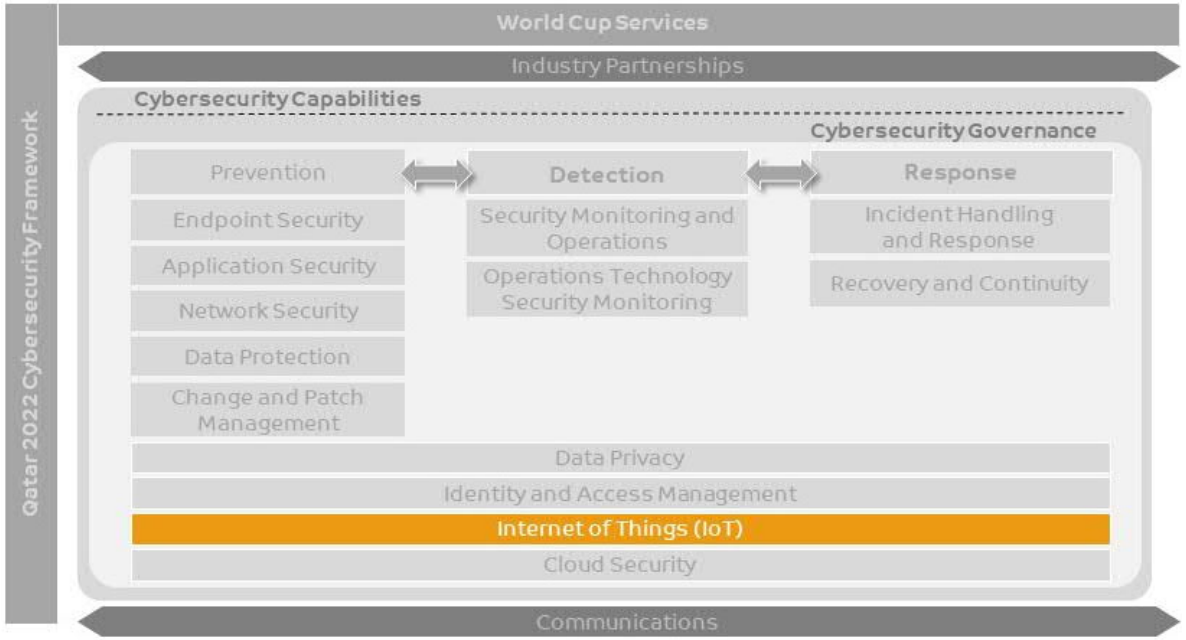
14. Capability Description – Internet of Things (IoT)

The Internet of Things (IoT) connects smart sensing devices such as everyday consumer devices and industrial equipment to enterprise networks, enabling information gathering and management of these devices via software to increase efficiency, enable new services or achieve other health, safety or environmental benefits. IoT solution deployments enable improved services to the public through the deployment of Smart sensors and provide rich data creation and marketing opportunities and new experiences for consumer-based areas such as wearable's and Smart stadiums.

These architectures push smarter devices closer to business and consumers for real-time data analysis and processing. Ensuring the Protection of these smart systems and endpoints is still emerging and organizations are finding it extremely challenging due to the sheer number of devices expected to be deployed and the extension of corporate services and Critical Infrastructure into The Cloud. IoT devices which is actively being deployed also presents many opportunities for cyber-attackers to exploit globally.

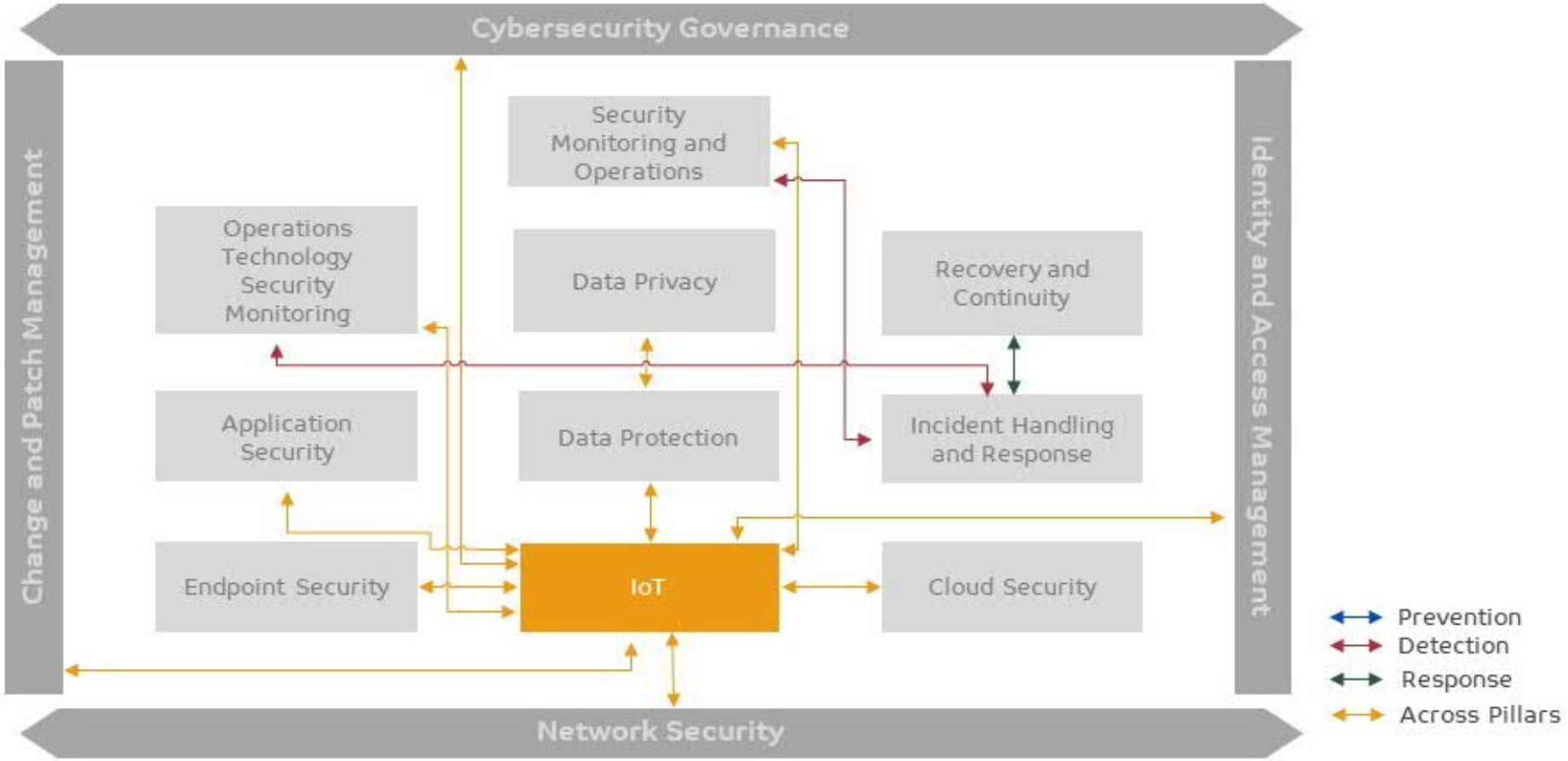
This chapter focuses on 'IoT Security" capability, and covers all three pillars of world cup cybersecurity capabilities (Prevention, Detection and Response):

Figure 83: Cybersecurity Capabilities-Internet of Things (IoT)



Following figure depicts linkage of Internet of Things (IoT) with other cybersecurity capabilities defined in the framework

Figure 84: Internet of Things (IoT) linkage with other capabilities



14.1 Prerequisites

Following are the prerequisites, which are required to be accomplished for a successful IoT Security capability:

- IoT assets to be protected have been identified (refer to other capability chapters Cybersecurity Governance, data protection, application security, network security, data privacy, and cloud security)
- The capability to automatically discover and account for connected IoT
- Standard information security policies are applied
- Embedded sensor devices meet security best practices and World Cup Cybersecurity Framework requirements, if any
- IoT assets must meet industry safety and cyber security compliance requirements before field deployment (Passed Site Acceptance Testing – SAT)
- Appropriate logs and events have been enabled on identified assets for collection and analysis (refer to other capability chapters such as application security, network security, data protection and cloud security)
- Information protection regulations and industry compliance requirements are identified
- The IoT Security team should be notified for any change management activities (refer to change and patch management capability)
- Security risks identified for IoT devices during the risk assessment have been communicated and considered

14.2 IoT Security Service

The IoT Security capability is the ability to securely design and deploy secure Smart systems and sensing solutions across complex systems like Building Management Systems (BMS), UAV's, Smart stadiums and Smart Energy Solutions as follows:

- Ensuring there is an IoT vision and strategy are defined at the entity level with the appropriate security and safety components
- IoT Solution Design and implementation is based on industry standards
- Establish IoT security governance and define roles & responsibilities (refer organization structure in Cybersecurity Governance chapter)
- IoT security architecture is accounted, designed and implemented for completing systems such as cloud solutions, enterprise IT, and /or OT domains
- IoT solutions used for Critical Infrastructure are Protected in line with Qatari Security Standards as a minimum
- Advanced Security Monitoring solutions are implemented to detect cyber-attacks on IoT endpoints
- IoT legal and compliance aspects are considered when capturing private/citizen data
- IoT is a broad discipline, and IoT security should fall under the existing IT or Technology Department governance structure already in place
- IoT security governance is an extension of the existing IT program and must have the same Governance, Risk and Compliance controls applied
- Policies and procedures for IoT security must be developed in line with the standards
- IoT design and security requires regular vulnerability assessment and penetration testing to be performed on enterprise, cloud and embedded device assets. Standard testing frameworks (e.g. PTES, IEC: 62443-4) can be used be assure IoT solution deployments have been carried out according to the Qatar 2022 Cybersecurity policies and procedures and in collaboration of the other capabilities of the framework
- Continually improve policy, procedure and guidelines with changing risks and lessons learned

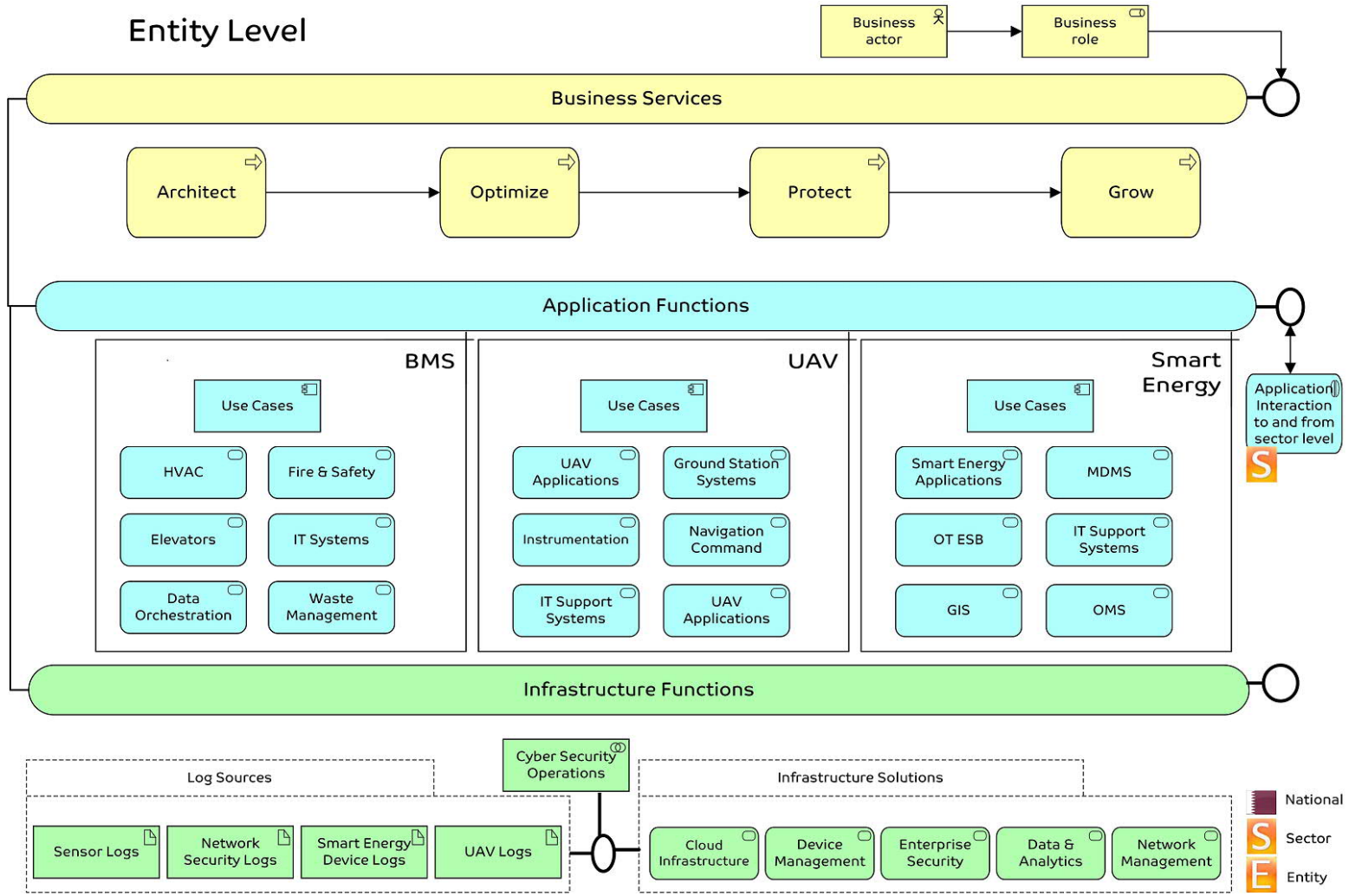
Table 84: IoT Security Service

Service Name: IoT Security	
Description	The IoT Security capability is the ability to design and secure Smart systems and endpoint sensing solutions across Building Management Systems, UAV's and Smart Energy Solutions.
Process Phases	**Activities/Controls**
Architect	• The technology vision and strategy embrace the potential of IoT • All levels of architecture accommodating IoT concepts, processes, data and components are considered and security is embedded • The governance and operating models must allow for seamless coexistence of operations and information technologies • Entities deploying IoT solutions must support the inclusion of game-changing aspects of human-machine integration • The sensing/controlling periphery of systems become natural extension of the IT core • Omnipresent data sources creating data driven decisions and value opportunities in line with the security and privacy considerations
Optimize	• New sources and results of processing of information enables improvement of established businesses and can contribute to the intelligence gathering • Ensure design supports high availability and resilience principals • Proactive, condition-based maintenance improves
Protect	• IoT security architecture is one of the pillars of IoT strategy • IoT components with trust mechanisms (i.e. with Block Chain) is capable to perform transactions -trusted digital • Supports artificial intelligence cyber security, as attacks on Critical Infrastructure can be detected based on measured work parameters analysed by Machine Learning algorithms in real-time. • IoT assets are hardened and certified (if possible) • IoT instrumentation can provide information on conditions (environmental, external infrastructure) as well as on actions (inspection and monitoring events) widening the oversight of security operations • IoT is contributing with new data sources for the entity's Security Operation Centre (SOC) to provide deeper awareness and enriched context to decision makers • Supports intelligent, automated or decision-making systems to minimize Incident response time
Grow/Enrich	• Near-real-time information coming from practically unlimited sources will create new to enrich the cyber security visibility • Always ensure alignment with citizens' and users' privacy rights • New operating models and new cyber security use cases for monitoring based on sensor information are constantly created and revisited • Convergence of monitoring of physical access and digital/IoT is implemented • Adding of digital identity to physical IoT assets

14.3 IoT Security Capability Model

Following figure illustrates an architecture model established for IoT Security capability at Entity level:

Figure 85: IoT Security Capability Model



The above figure defines the IoT Security capability model in layered approach:

- The **Business service layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- The **Application Functions Layer** supports the business layer with application services which are realized by (software) application components.
- The **Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

14.4 Information Flow in various levels

Upon analysis and following confirmation that certain threats and risks are targeting the world cup specific services and associated IoT systems, this should be shared with the sector/national levels as world cup specific risks and threats via the security monitoring team and utilizing vehicles such as STIX/TAXII as mentioned in the security monitoring capability. This will help in implementing unified mitigating/compensating control across the world cup ecosystem. Services expected at each level.

14.4.1 Services expected at each level

IoT security service will be applicable to all IoT systems used for world cup irrespective of the level (i.e. Entity/Sector/National) it is being used.

Table 85: IoT Security services expected at each level

Entity	Sector	National
• IoT Vision, Strategy and Governance • IoT solution design and implementation • IoT human aspects • IoT Security Architecture and solutions • Critical infrastructure protection controls implementation • IoT legal aspects • IoT rogue device detection and prevention	• Critical infrastructure protection controls requirements • National Level escalation process	• Critical infrastructure protection controls • National level logging and monitoring (i.e. national PKI is used to authenticate IoT assets) • National level incident response

14.5 Milestones

Following milestones have been defined for IoT Security:

- Cybersecurity has been considered as a design principal in the IoT architecture
- Optimize business processes to support cyber security requirements
- Protect information and sensor device assets
- Support next generation automation and artificial intelligence to be used in cybersecurity

14.6 Skills required for IoT Security

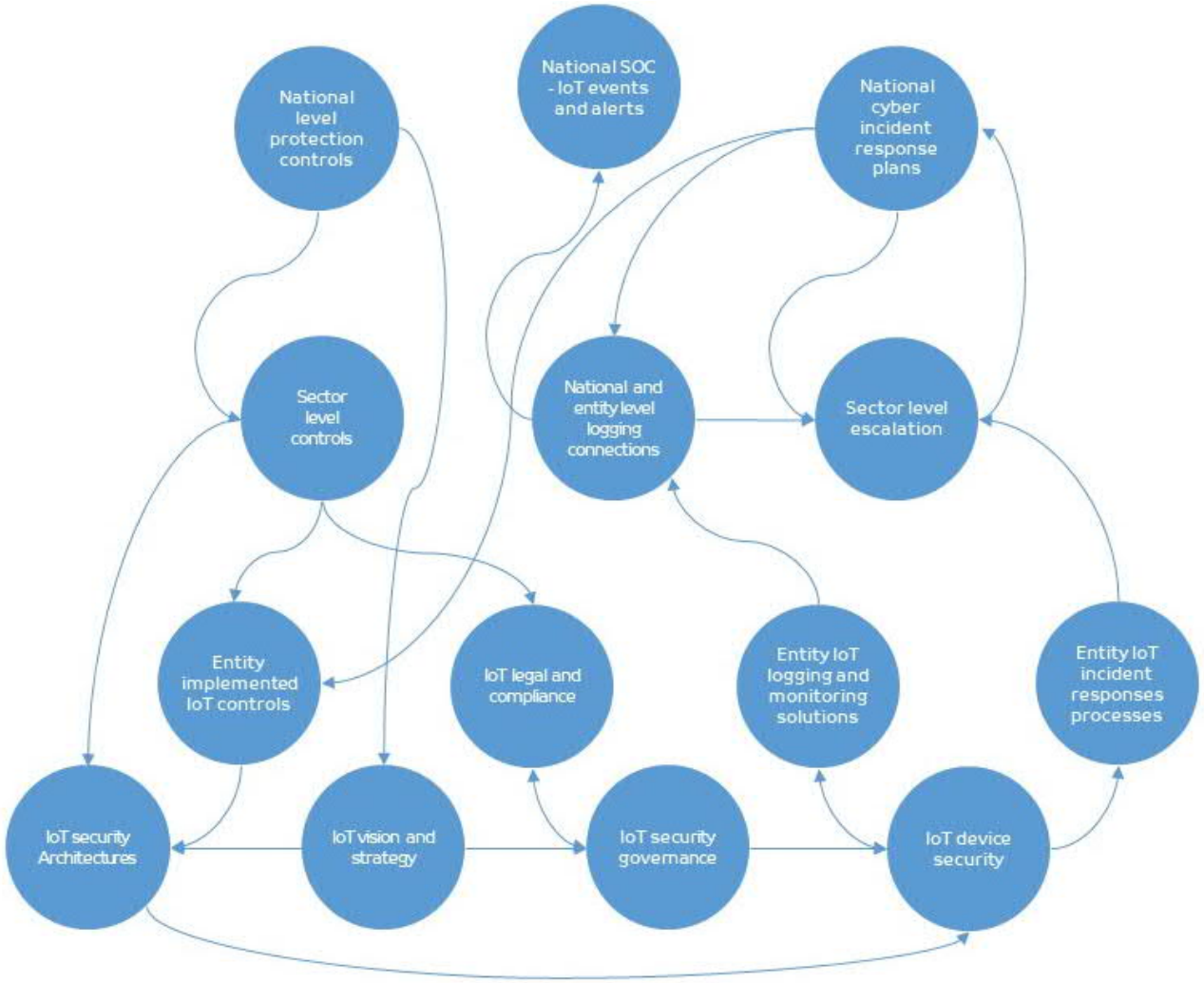
Following are the skills expected from personnel executing IoT Security activities:

Skills Required -

- Bachelor's degrees such as Business Information Systems & Analytics, Computer Science, Electrical Engineering and Electronics Engineering include the appropriate skills to understand, design and deploy and secure IoT solutions.
- Solid knowledge of the IoT security domains and secure design principals
- Capable of evaluating the cyber risks to IoT systems architectures for instance BMS, AMI/AMRs
- Solid knowledge of Industrial networking protocols security such as DNP3, Modbus, Profinet, ZigBee, IEC 104 etc.
- Knowledge of IoT capable SIEM, security events logging and monitoring technologies
- Awareness of IoT network monitoring technology platforms
- Performing event analysis by correlating data from various sources
- Competent to create custom signature/rules for detection and prevention technologies being used in the IoT environment
- Ability to create various use cases based on environment for better detection of anomalies
- Ability to conduct IoT and embedded systems vulnerability assessments
- Provide support to incident response teams for collecting evidences and in motoring of mitigation steps
- Ability to identify gaps in detection processes

14.7 Conceptual IoT Service Level Data Flows

Figure 86: Conceptual IoT Security Data Model



14.8 Technology

14.8.1 Target High-Level Technical Architecture

IoT security capability for world cup entities and partners will focus on three key technology deployment domains:

- Smart stadiums - Building management systems (BMS)
- Unattended autonomous vehicles (UAV)
- Smart energy solutions - Smart Meters (SM)

These are anticipated to be core IoT deployment domains in readiness for the world cup event and beyond. The security requirements needed to secure these areas are defined in the sections below.

Figure 87: BMS Technical Domain Architecture

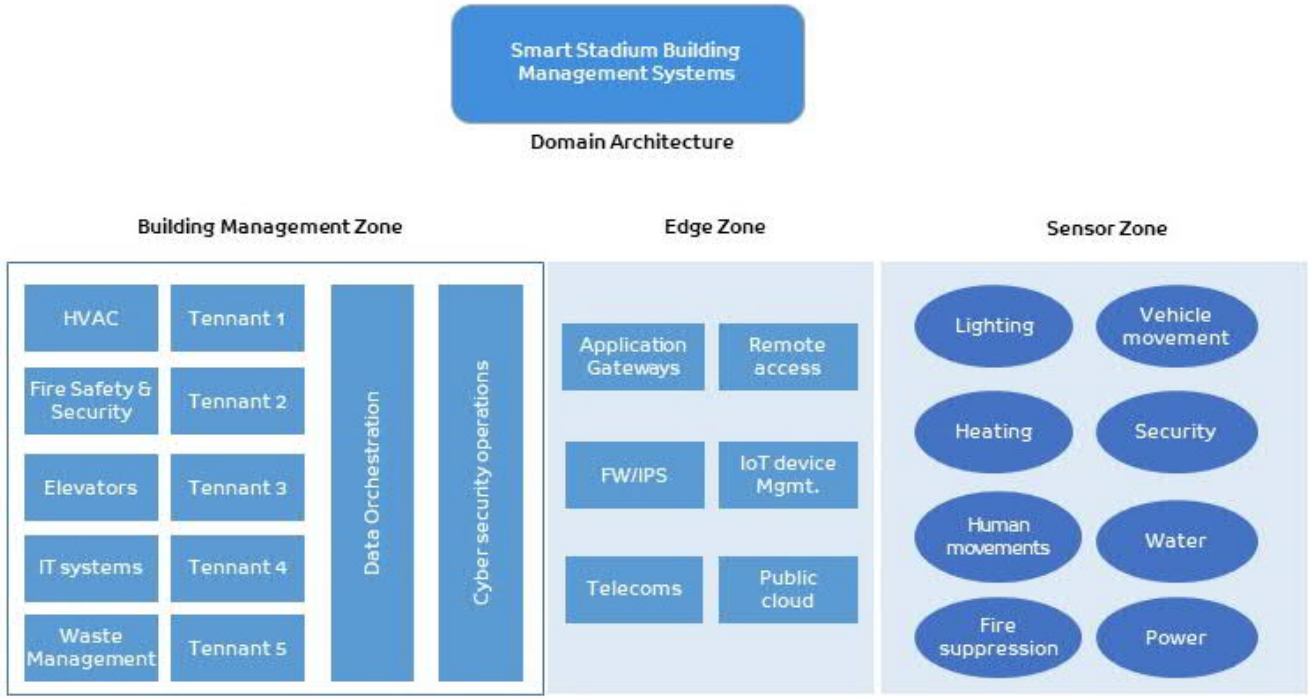


Figure 88: UAV Technical Domain Architecture

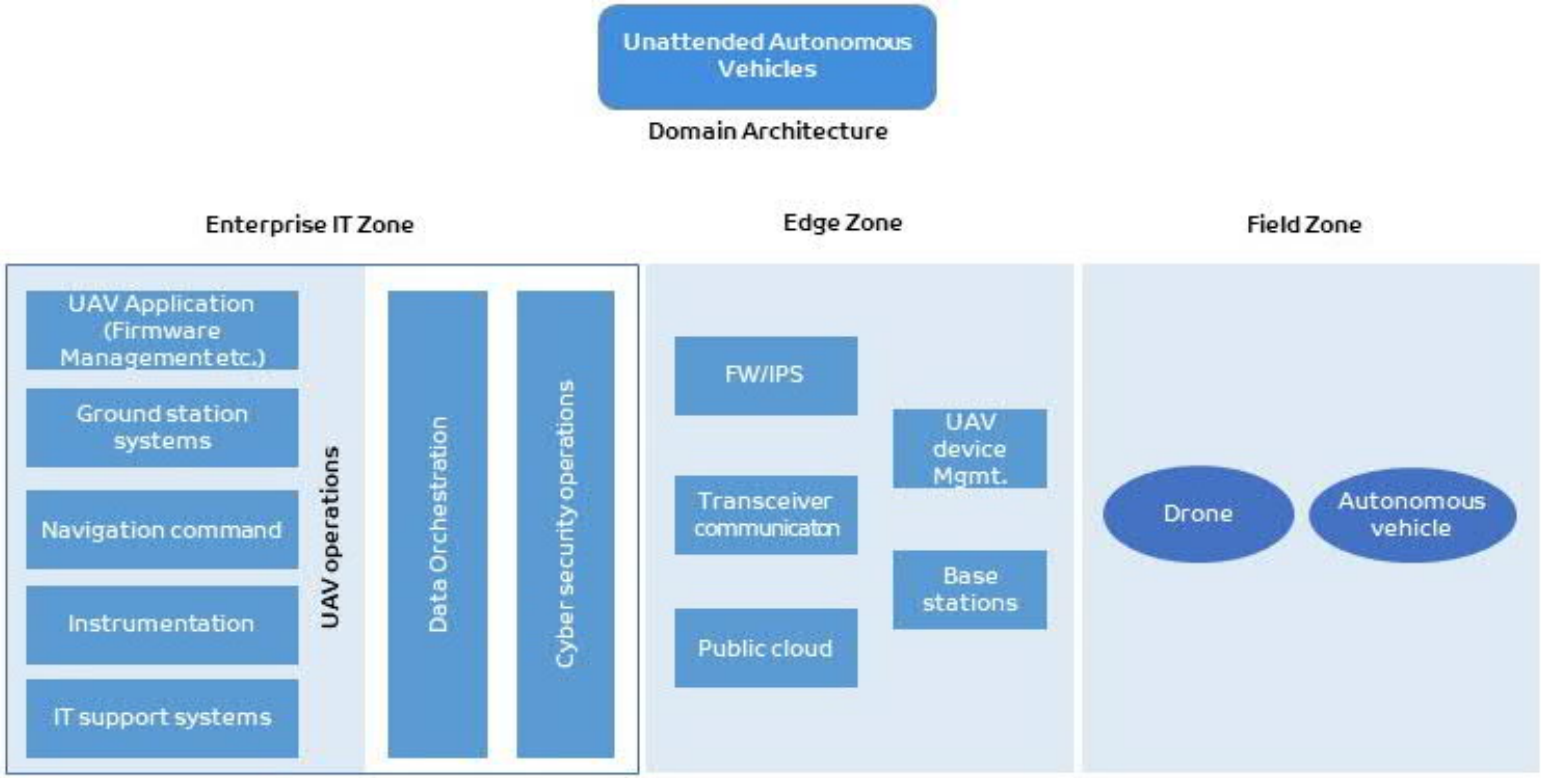
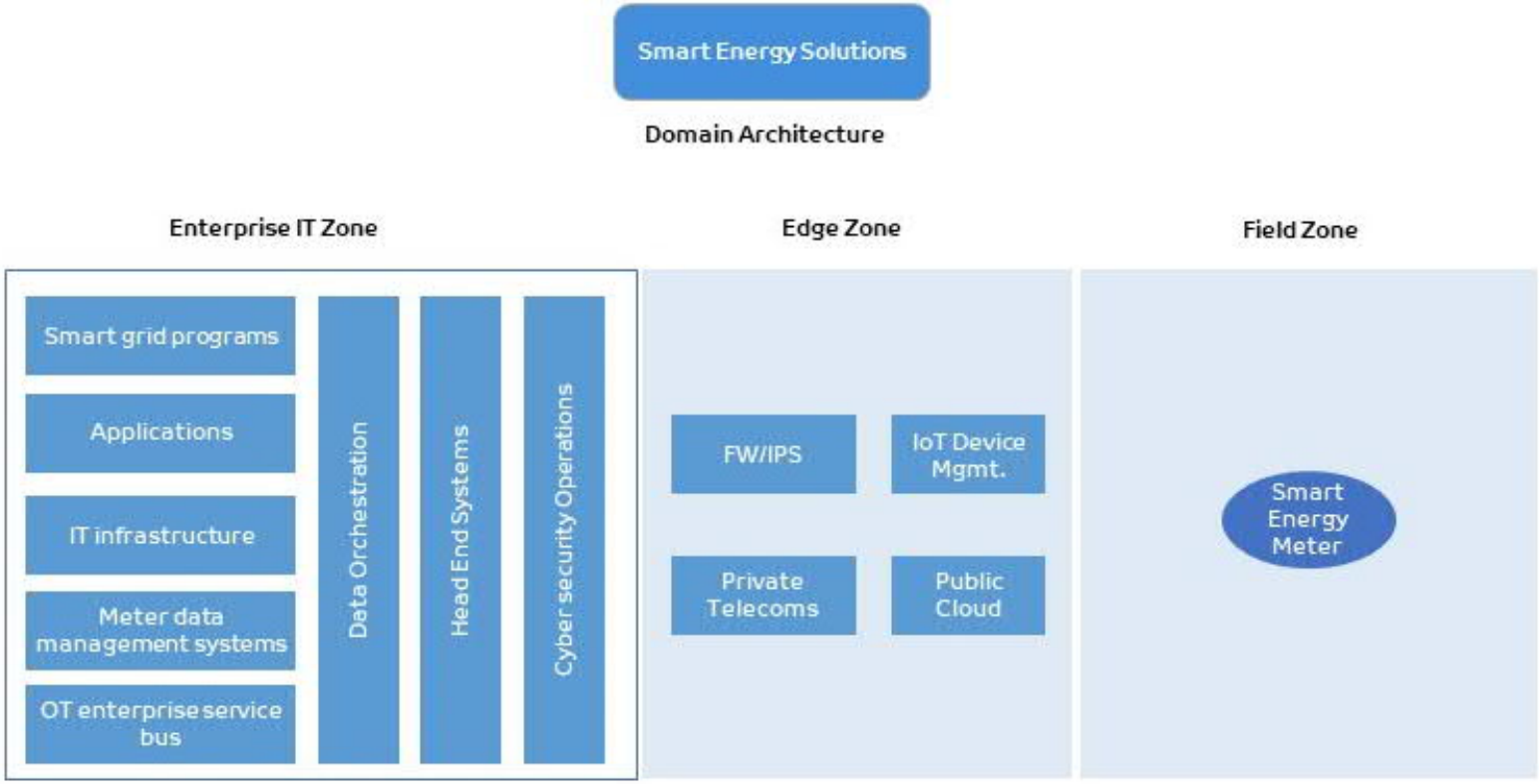


Figure 89: Smart Energy Technical Domain Architecture



14.9 Recommended IoT Security Hardening Controls

14.9.1 Recommended Protection Requirements – Cryptography

Table 86: Recommended Protection Requirements – Cryptography

Cryptographic Technique		Example Objective	Example Requirements	
Symmetric key cryptography	MACs	Message authentication: Message integrity	Securely generated, distributed and maintained, shared secret key	Secure standardized and up-to-date MAC algorithm
	Symmetric encryption	Confidentiality		Secure standardized and up-to-date encryption algorithm
Asymmetric key cryptography	Digital signatures	Authorship; Integrity; Non-repudiation	Public-key infrastructure	Standard-based securely generated, distributed and maintained, public and private keys; Standardized and up-to-date signature schemes
	Asymmetric encryption	Confidentiality		Standardized and up-to-date asymmetric encryption algorithm
	Shared secret establishment	Forward secrecy		Standardized and up-to-date shared secret establishment algorithm
Hash function		Message/data integrity		Standardized and up-to-date hashing algorithm
Random number generator		Random key and other data	Proper random seed	Standardized and up-to-date random generator

14.9.2 Recommended Protection Requirements – Integrity

Table 87: Recommended Protection Requirements – Integrity

Objective: Integrity		Example Technique/Process	Example Requirements
Endpoint integrity	Integrity for roots of trust	Protected key store	Integrity of protected storage for key management
	Integrity of endpoint identity	Identity certificate signed by trusted certificate authority	Trusted public-key infrastructure
	Hardware integrity	Side channel measurements; silicon scanning	Open, standards-based specification
	Software integrity	Code signing	Trusted public-key infrastructure
		Secure software development; Risk-based security testing; Static analysis	Secure software development methodology
		Boot process integrity	Trusted hardware manufacturer; Hardware security module or proprietary implementation of hardware backed cryptographic boot protection; Standardized OS firmware interface (e.g. UEFI)
		Secure patch management	Patch management plan
	Runtime integrity	Runtime verification	Code execution modelling, instrumentation and monitoring
	Integrity of data-at-rest	MACs, hashes/digests; Digital Signatures	Securely generated, distributed and maintained keys; Standardized and up-to-date algorithms
Integrity of communications		Mutual authentication between endpoints; use of MACs and/or digital signatures during communication	Securely generated, distributed and maintained keys; Standardized and up-to-date algorithms for mutual authentication and message exchange integrity
Integrity of management and monitoring operations		Authentication of management and monitoring assets (including workforce); Integrity verification of asset changes, asset monitoring solutions and asset Updates; Maintaining integrity of logs and reports	Endpoint integrity for management and monitoring; Communication integrity for monitoring, logging and management of assets; Security procedures for managing management and monitoring operations; Integrity of analytical algorithms; Integrity of audit or audit path

Objective: Integrity		Example Technique/Process	Example Requirements
Architectural integrity	Integrity of data-in-motion	Holistic assessment of data integrity in its lifecycle across the entire IoT system	Endpoint, communication, monitoring and management integrity in system segments
	Mutual impact of integrity controls on other key system characteristics	Architectural integrity evaluation	Holistic security evaluation methodology; Domain-specific expertise
	Mitigating impact of both insider and outsider attacks on system integrity	Enforcing principle of least privilege; Access control	Granular access control policies

14.9.3 Recommended Protection Requirements – Confidentiality

Table 88: Recommended Protection Requirements – Confidentiality

Objective: Confidentiality		Example Technique/Process	Example Requirements
Confidentiality at endpoints		Encrypted data storage	Securely generated, distributed, and maintained keys; Protective storage of sensitive key material; Standardized and up-to-date encryption algorithms
Confidentiality of communication		Encrypted communication	Securely generated, distributed, and maintained keys; Standardized and up-to-date encryption algorithms
Confidentiality of management and monitoring operations and solutions		Encrypted communication	Endpoint confidentiality and communications confidentiality
Architectural confidentiality	Confidentiality of data in its lifecycle		Endpoint confidentiality; communications confidentiality; Confidentiality of management and monitoring
	Mutual impact of confidentiality controls on other key system characteristics	Architectural confidentiality evaluation	Holistic security evaluation methodology; Domain-specific expertise
	Mitigating impact of both insider and outsider attacks on confidentiality	Enforcing principle of least privilege; Access control	Granular access control policies

14.9.4 Recommended Protection Requirements – Access Control

Table 89: Recommended Protection Requirements – Access Control

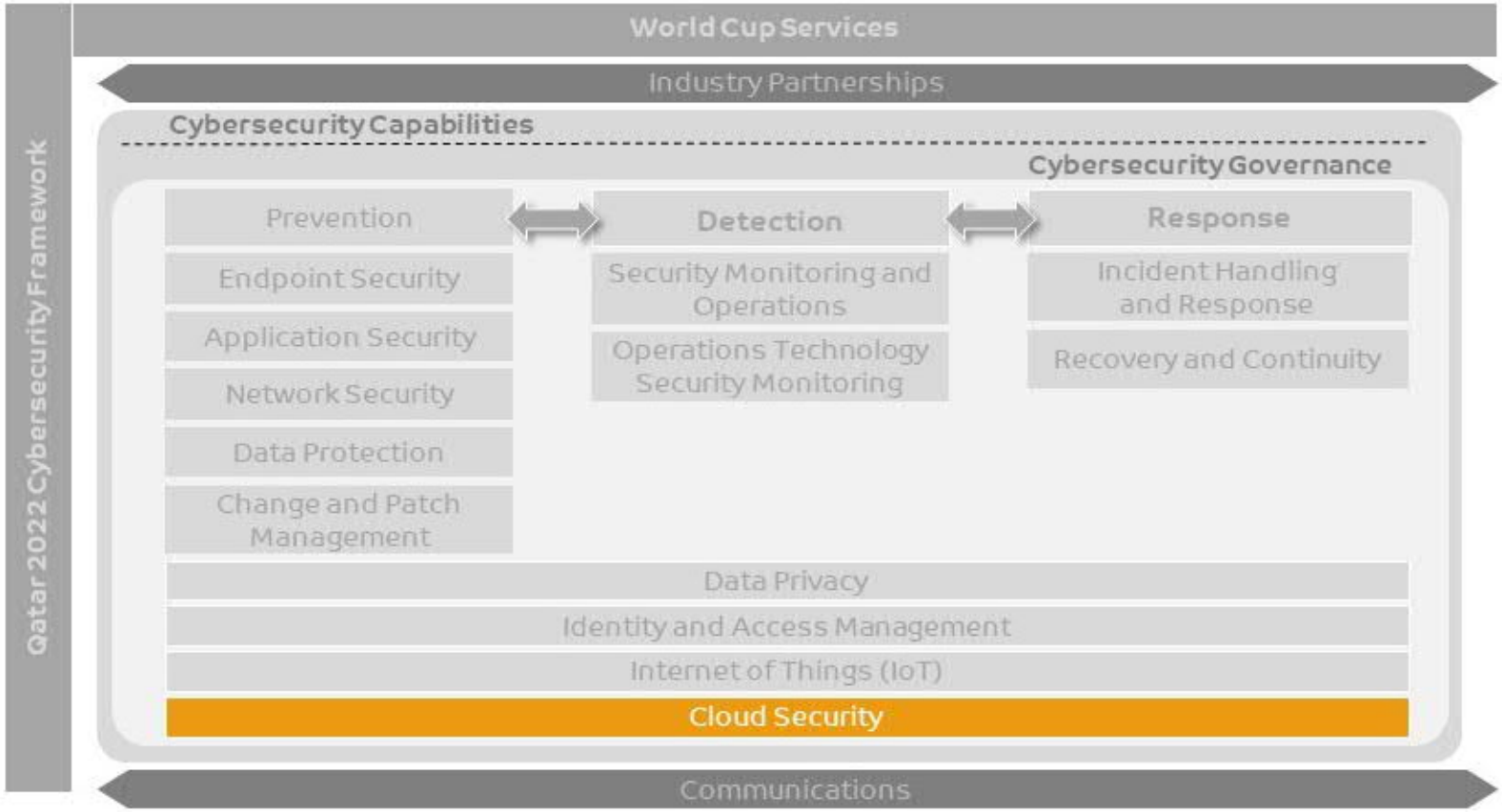
Objective: Access Control			Example Technique/Process	Example Requirements
Endpoint access control	Confinement and information flow protection within endpoint		Sandboxing (application); Fine-grained data-centric access control (middleware); Separation kernels (OS); Trusted computing environments (hardware)	Comprehensive and consistent security policies
Communications access control	Cryptographic protection of communications and connectivity		Use of protocols at different layers; Forcible disconnection of unauthorized endpoints;	Correct and trusted implementation of cryptographic techniques; Network access control for endpoints
	Information flow control		Network segmentation; Gateways and filtering; Network firewalls; Unidirectional gateways	Comprehensive and consistent security policies; Trusted manufacturing of devices
Access control for management and monitoring operations			Access control for monitoring, logging and managing assets (e.g. endpoints, communication, data, workforce); Control procedures for managing and monitoring operations; Controlling access to data that is fed into analytics solutions; Separation of duties; Role-based access control (RBAC)	
Architectural access control	Controlling access to data in its lifecycle		Access control within endpoints, communication, management and monitoring	
	Mutual impact of access controls on other key system characteristics	Architectural access control evaluation	Holistic security evaluation methodology; Domain-specific expertise	
	Mitigating impact of both insider and outsider attacks on access control	Enforcing principle of least privilege	Granular access control policies	

15 Cloud Security

15. Capability Description – Cloud Security

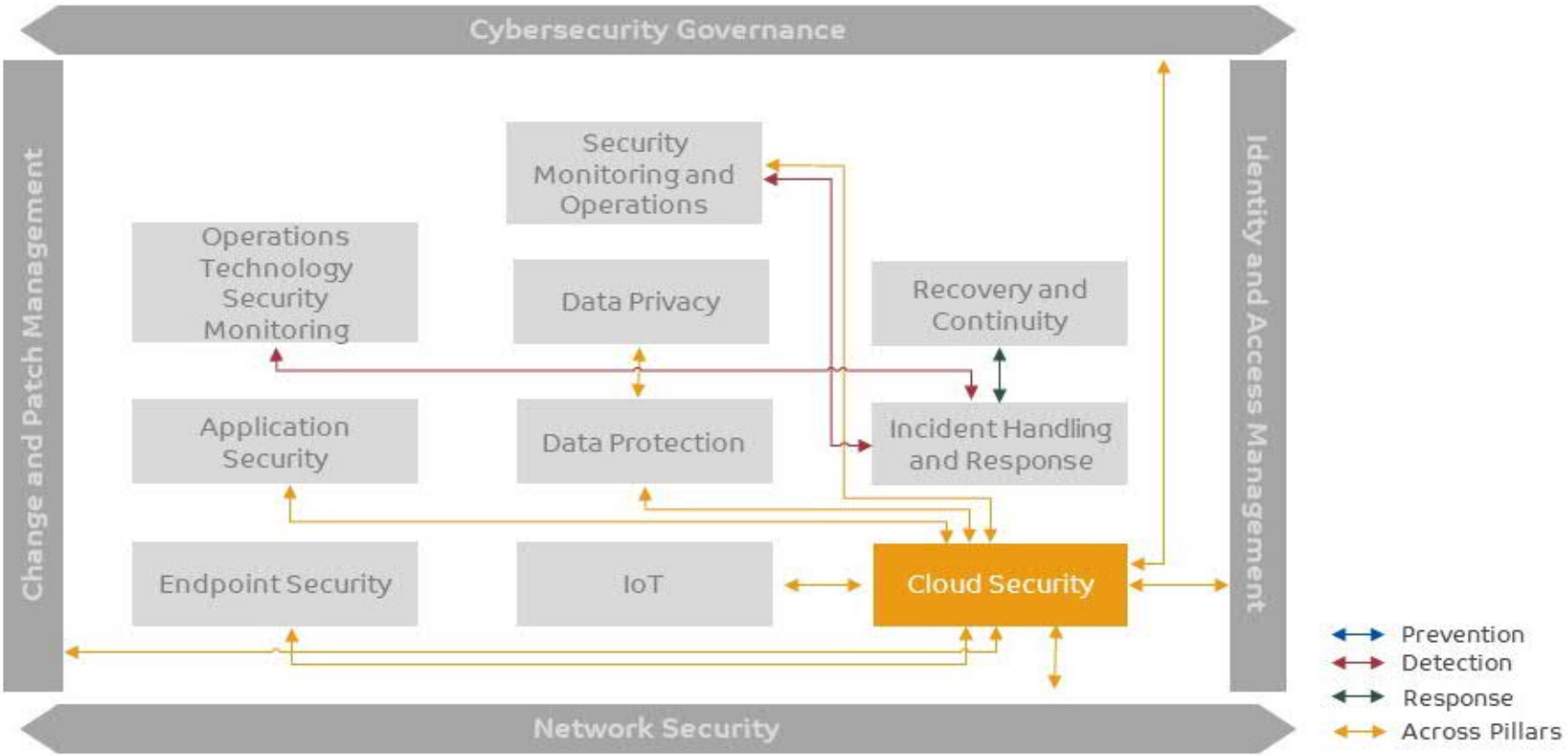
This is a proactive capability that ensures the secure operations of the entity cloud services offered by a local Cloud Service Provider (CSP) in Qatar. The capability will focus on how to ensure proper hardening for your cloud fabric, a model security architecture as well as the security requirements that should be provided by the CSP.

Figure 90: Cybersecurity capabilities – Cloud Security



Following figure depicts linkage of cloud security with other cybersecurity capabilities defined in the framework

Figure 91: Cloud Security linkage with other capabilities

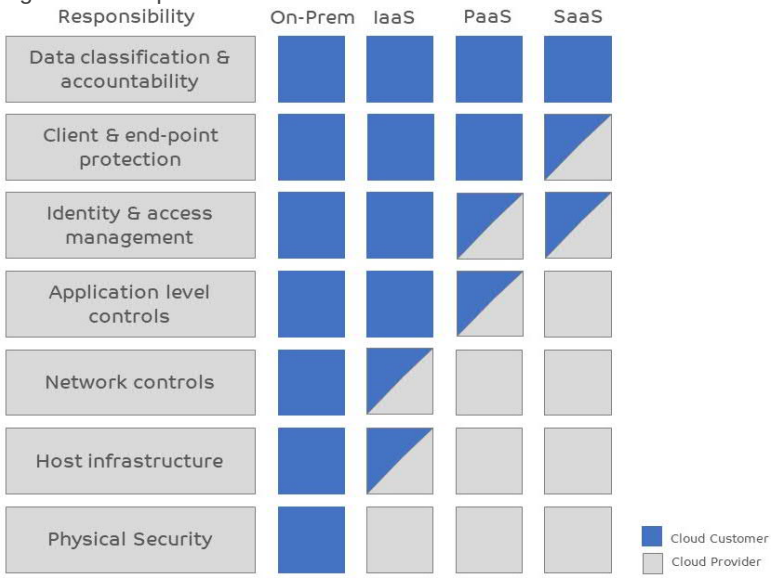

Cybersecurity Governance
Change and Patch Management
Identity and Access Management
Security Monitoring and Operations
Operations Technology Security Monitoring
Data Privacy
Recovery and Continuity
Application Security
Data Protection
Incident Handling and Response
Endpoint Security
IoT
Cloud Security
Network Security
Prevention
Detection
Response
Across Pillars

15.1 Prerequisites

Following are the prerequisites which are required to be accomplished prior to utilizing this capability:

- Based on the standard cloud models explained below, we assume that for the world cup, all entities will be required to access and use a dedicated cloud infrastructure that uses the Infrastructure as a Service (**IaaS**) Model hosted by a local Qatari Cloud Service Provider (**CSP**)
  - **Software as a Service (SaaS)**: This model offers the cloud customer the facility to use the Cloud service provider's (CSP) applications running on a commercial cloud infrastructure. The software stack and applications are accessible online. You as a cloud customer have no control over the underlying cloud fabric, networking or hardware
  - **Platform as a Service (PaaS):** This model offers the cloud customer the facility to install his own software stack (Excluding Operating system in most cases) onto the cloud infrastructure with the limitation that the software deployed uses the programming languages, libraries, services, and tools supported by the cloud service provider. The cloud customer has no control over the underlying cloud fabric, networking or hardware
  - **Infrastructure as a Service (IaaS):** This model offers the cloud customer the facility to utilize the cloud fabric and the virtual computing resources such as memory and storage allocation (as needed) and the cloud customer can install and run any software, including operating systems. The cloud customer does not manage or control the physical access to the cloud facility or the power and core-networking infrastructure

Figure 92: Responsibilities in Cloud service model



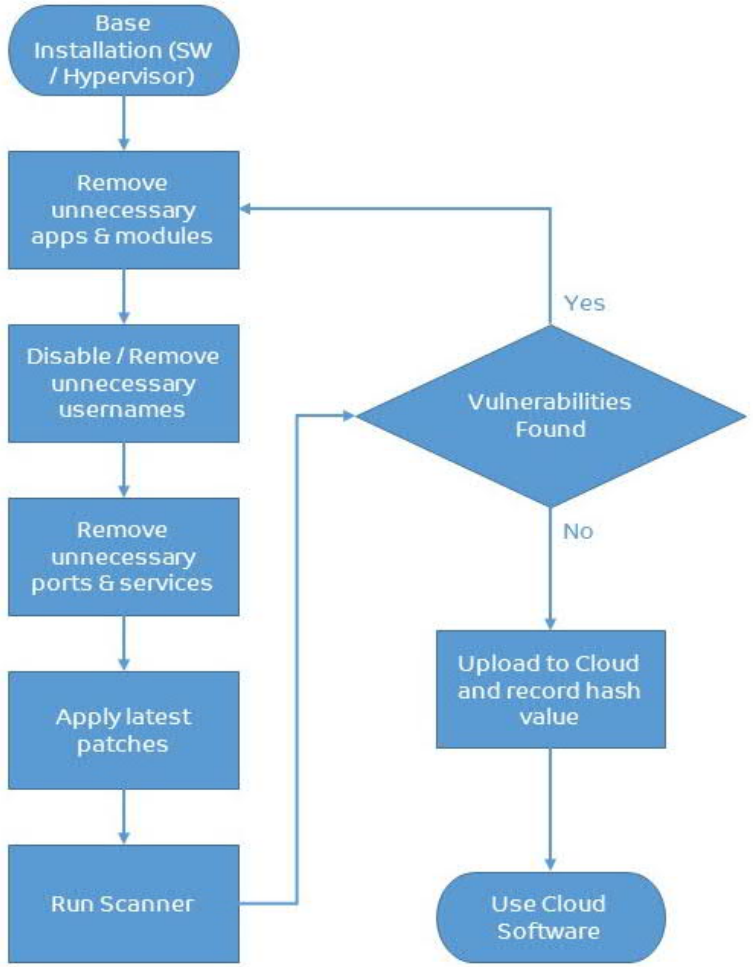
- Boundaries of the cloud-based services have been identified
- The entity has completed a data classification exercise and is aware of the types of data involved
- The entity has contracted a CSP, signed the NDA (Non-disclosure agreement), SLAs (Service level agreement)
- The entity has an agreed standardized image (Operating system), or have agreed with the CSP on a standard image (golden image) that will be used as a baseline for all vanilla installations
- The entity has agreed with the CSP on a list of pre-approved applications (White listing) that can be allowed into the environment, in case of commercial off the shelf applications
- The entity must have redundant and secure communication channels with the CSP
- The entity has agreed the roles and responsibilities, SLAs and the escalation process between them and the CSP
- The entity must have a tested DRP that accommodates the scenario of Lack of cloud-based services (refer to the recovery and continuity capability chapter)
- Security risks identified for the cloud instances during the risk assessment have been communicated and considered

Figure 93: Cloud assets security hardening service

15.2 Cloud assets security hardening service

From world cup perspective, ***Table 90: Cloud assets Security hardening*** describes cybersecurity services that has been defined under this capability and respective activities that needs to be conducted for each service. However, from preparation/planning viewpoint, following steps must be completed:

- Establish a cloud security strategy
- Establish cloud security policy, forms and procedures
- Establish governance and assign cloud specific roles and responsibilities (refer organization structure in Cybersecurity Governance chapter and compendium section of this chapter)
- Deploy and train team members
- Define cloud security monitoring parameters and incident handling procedures
- Continually improve policy, procedure & guidelines with changing risks and lessons learned



Following table describes activities established for cloud assets security hardening service:

Table 90: Cloud assets Security hardening

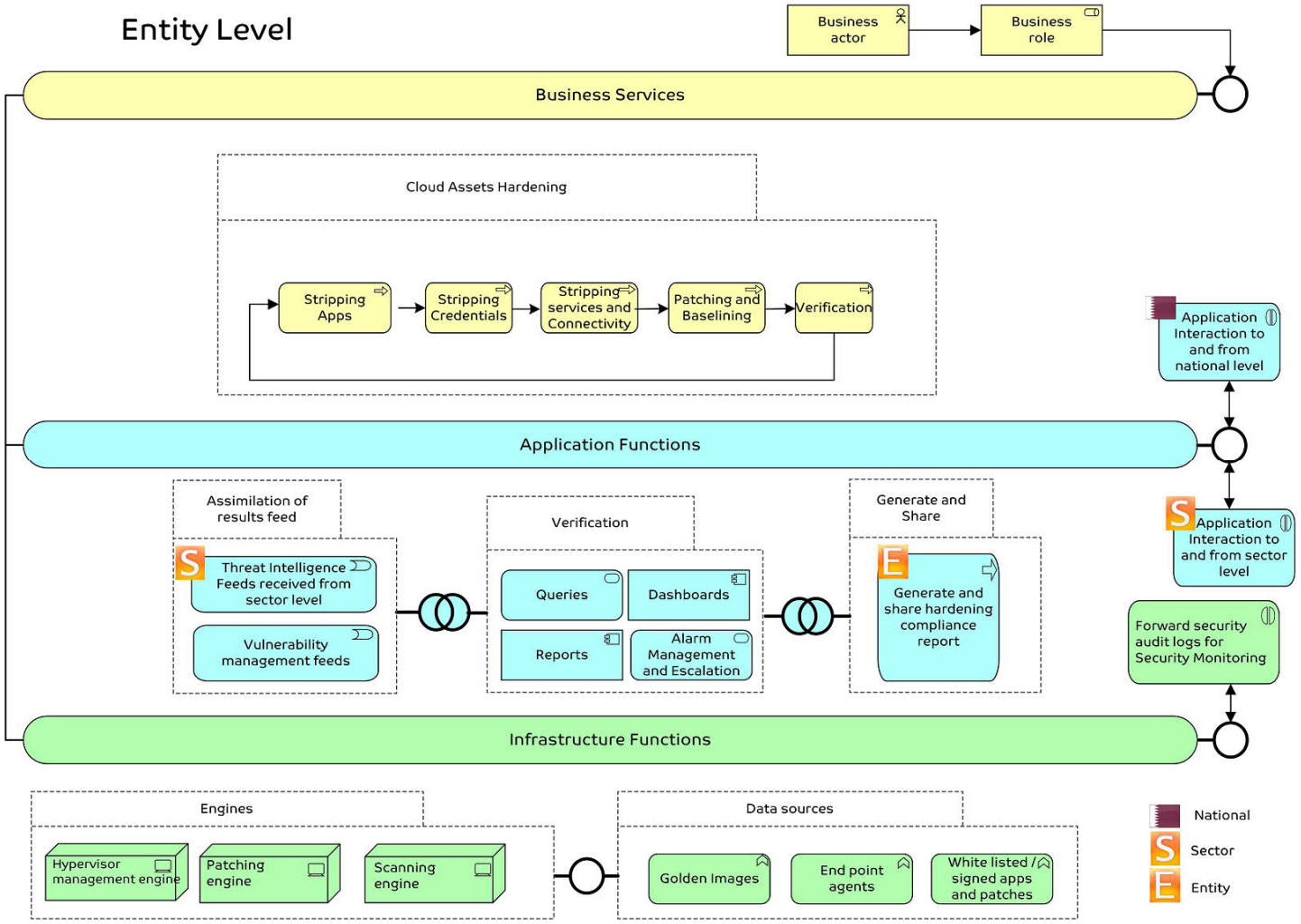
Service Name: Cloud assets security hardening	
Description	A proactive capability that ensures the secure operations of the entity cloud services offered by a local Cloud Service Provider (CSP). The capability will focus on how to ensure proper hardening for your cloud-based assets.
Process Phases	**Activities/Controls**
Stripping Apps	• Removing unnecessary software apps

Service Name: Cloud assets security hardening	
	• All systems come with a predefined set of software packages and software modules that are generic and assumed to be useful for general use. Based on your intended use of the system, you should disable/remove all unnecessary software
Stripping credentials	• Disabling or removing unnecessary usernames and credentials • (Several software has come with predefined user accounts for various uses - from remote support to service accounts for specific services.) • Removing all remote support and service accounts which are not to be used Besides changing, all default passwords
Stripping services and connectivity	• Disabling or removing unnecessary services and ports • (Remove all services, which are not used in production. You can always just disable them, but if you have the choice remove them altogether. This will prevent the possible errors of someone activating the disabled service further down the line)
Patching and baselining	• Applying security and functionality patches (Covering operating system and all approved applications)
Verification	• Performing a full scan for verification purposes preferably twice a year

15.3 Cloud assets security hardening Capability Model

Following figure illustrates an architecture model of various functions established for cloud hardening at entity level:

Figure 94: Cloud assets security hardening Capability Model



Above figure defines the cloud assets security hardening capability model in layered approach:

- The **Business service layer** is about business processes, services, functions and events of business units. This layer offers services to external stakeholders, which are realized by in the organization by business processes performed by business actors and roles.
- The **Application Functions Layer** supports the business layer with application services which are realized by (software) application components.
- The **Infrastructure Functions layer** offers infrastructural services (e.g. processing, storage and communication services) needed to run applications, realized by computer and communication hardware and system software.
- Conclusively, the infrastructure functions layer enables hardware to interact and exchange information using various protocols & medium. That information is then processed by the application function layer to present the information in human readable format. The processed information is being used in various business processes/services and shared to various stakeholders through business services layer. Various users defined in the organization structure work at this layer having respective roles & responsibilities to perform

15.4 Information Flow at various levels

Upon analysis and following confirmation that certain threats and risks are targeting the world cup specific services and associated cloud systems, this should be shared with the sector/national levels as world cup specific risks and threats via the security monitoring team and utilizing vehicles such as STIX/TAXII as mentioned in the security monitoring capability. This will help in implementing unified mitigating/compensating control across the world cup ecosystem.

15.4.1 Services expected at each level

Cloud security hardening service will be applicable to all the applications used for world cup irrespective of the level (i.e. Entity/Sector/National) it is being used.

Compendium – Cloud Security

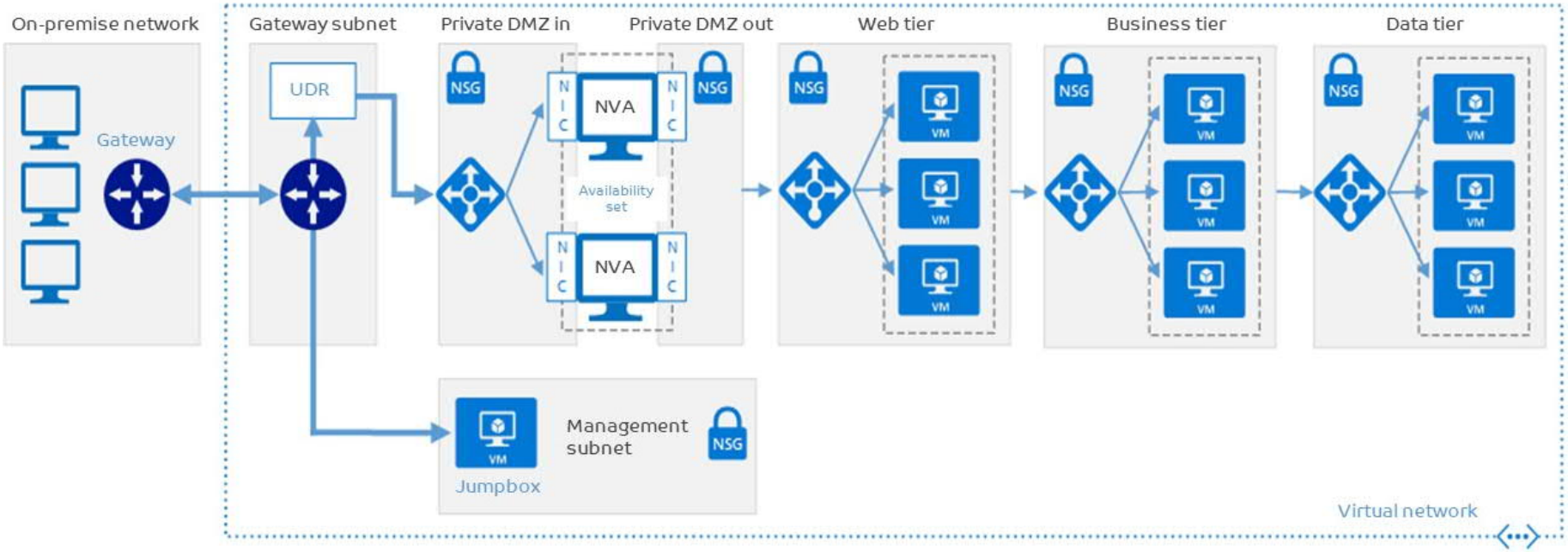
15.5 Milestones

The following milestones have been defined for cloud assets security hardening:

- Complete the data classification for the shared information/data using the cloud
- Ensure that the CSP utilizes the below model architecture
- Set and define the golden image and configuration baselines
- Establish the process to continuously harden and verify that the control exists and is effective.

15.6 Model CSP architecture

Figure 95: Model CSP architecture



As per the above model architecture, the entity shall work with the CSP to verify that those security layers and tiers exist:

- On-premises network: A the entity's local-area network
- CSP virtual network: The Virtual network hosts the application and other resources running in the cloud
- The Cloud Gateway: The "gateway" provides connectivity between the routers in the on-premises network and the virtual network
- Network virtual appliance (NVA): is a generic term that describes a VM performing tasks such as allowing or denying access as a firewall, optimizing wide area network (WAN) operations (including network compression), custom routing, or other network functionality. This can also be a dedicated hardware network appliance
- Web tier, business tier, and data tier subnets: Subnets hosting the VMs and services that implement an example 3-tier application running in the CSP environment
- User defined routes (UDR): user defined routing tables that directs the traffic either to the cloud services or to other cloud-based segments such as the management subnet
- Network Security Group Policy (NSG): a set of security policies or configurations applicable to a set of VMs or cloud assets that share the same function and subject to the same security policy

- VM: virtual Machine
- The virtual network: is the CSP environment

15.7 Sample cloud security hardening controls

1. Ensure that multi-factor authentication is enabled for all privileged users
2. Ensure that multi-factor authentication is enabled for all non-privileged users
3. Ensure that there are no guest users
4. Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled'
5. Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'
6. Ensure that 'Notify users on password resets?' is set to 'Yes'
7. Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes'
8. Ensure that 'Users can consent to apps accessing entity data on their behalf' is set to 'No'
9. Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No'
10. Ensure that 'Users can register applications' is set to 'No'
11. Ensure that 'Require Multi-Factor Authentication to join devices' is set to 'Yes'
12. Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' (Applicable on Microsoft Azure based Cloud services)
13. Ensure that 'System updates' is set to 'On'
14. Ensure that 'Disk encryption' is set to 'On'
15. Ensure that 'Web application firewall' is set to 'On' for every virtual machine
16. Ensure to activate a service/solution for continuous vulnerability assessment
17. Ensure that 'Storage Encryption' is set to 'On'
18. Ensure that 'SQL auditing & Threat detection' is set to 'On', Applicable for MS-SQL cloud-based installations
19. Ensure that 'SQL Encryption' is set to 'On'
20. Ensure that 'Secure transfer required' is set to 'Enabled'
21. Ensure that 'Storage service encryption' is set to Enabled for data at rest
22. Ensure that storage account access keys are periodically regenerated
23. Ensure that shared access signature tokens expire within an hour
24. Ensure that shared access signature tokens are allowed only over https
25. Ensure that 'Storage service encryption' is set to Enabled for File Service
26. Ensure that 'Public access level' is set to Private for online data containers
27. Ensure that 'Auditing' Retention is 'greater than 90 days'
28. Ensure that Active Directory Admin is configured properly for all SQL Services
    a. On Microsoft based cloud – Type
       Get-AzureRmSqlServer *"to get a list of all installed SQL servers"*

Get-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource group name> -ServerName <server name> *" type on each server*"
Set-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource group name> -ServerName <server name> -DisplayName "<Display name of AD account to set as DB administrator>" *"to setup on each server*"

29. Ensure that a Log Profile is created and is active
    a. On Microsoft based cloud – Type
       az monitor log-profiles list – query [*].[id,name] *"to list the log profile and ensure activation*"
       az monitor log-profiles create -- categories <space separated category values Write|Delete| Action> --days <numberofDaysForRetention> --enabled true --location <locationName> --locations <Space separated list of regions> --name <logprofileName> *"to create a log profile if not created*"
30. Ensure that Activity Log Retention is set 90 days or greater
31. Ensure that Activity Log Alert exists for policy Creation Assignments
32. Ensure that Activity Log Alert exists for Create or Update Network Security Group
33. Ensure that Activity Log Alert exists for Delete Network Security Group
34. Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule
35. Ensure that Activity Log Alert exists for Delete Network Security Group Rule
36. Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule
37. Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule
38. Ensure that Activity Log Alert exists for Update Security Policy
39. Ensure that RDP access is restricted/disabled from the internet
40. Ensure that NONE of the below rules exist in the CSP firewall
    a. "access" : "Allow"
       "destinationPortRange" : "3389" or "*" or "[port range containing 3389]"
       "direction" : "Inbound"
       "protocol" : "TCP"
       "sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or "any"
41. Ensure that SSH access is restricted/disabled from the internet
    a. Ensure that NONE of the below rules exist in the CSP firewall
       "access" : "Allow"
       "destinationPortRange" : "22" or "*" or "[port range containing 22]"
       "direction" : "Inbound"
       "protocol" : "TCP"
       "sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or "any"
42. Ensure that any SQL server access is restricted from the internet
43. Ensure that 'OS disk' are encrypted for all the Virtual machines
44. Ensure that 'Data disks' are encrypted for all the virtual machines
45. Ensure that the latest OS Patches for all Virtual Machines are applied
46. Ensure that an endpoint protection for all Virtual Machines is installed

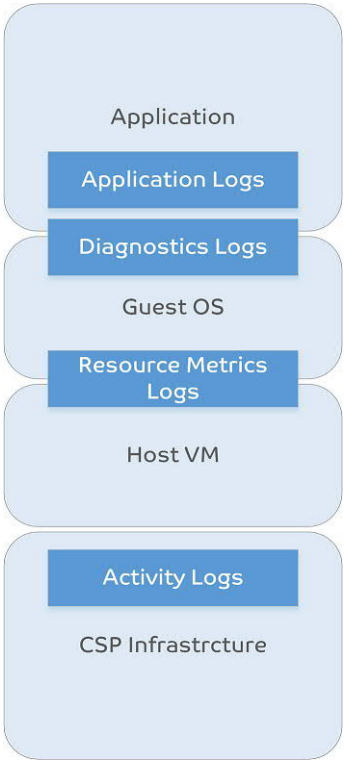
47. Ensure that the expiry date is set on all encryption Keys and secrets
48. Ensure removing all unnecessary interfaces, ports, devices and services
49. Ensure Secure configuration for all virtual network interfaces and storage areas
50. Ensure establishing limits on VM resource usage
51. Ensure all operating systems and applications running inside the virtual machine are also hardened;
52. Ensure that the entity has complete access to the Hypervisor administrative access logs
53. Ensure to adopt identity federated standards such as SAML or OpenID and use that for users CSP authentication
54. Ensure that the entity does NOT grant the CSP permissions to directly access the entity authentication environment such as the AD
55. Ensure that the CSP is certified as ISO 22301 or an equivalent standard
56. Ensure that the evidence discovery costs and forensics artefacts collection costs are included in the CSP agreement
57. Ensure that the CSP is providing adequate security controls across the various layers of cloud fabric, including network, physical, system and application layers
58. Ensure that the CSP develops an incident escalation tree and is committed to the SLAs as agreed
59. Ensure that the CSP is committed to notify the entity as soon as a breach is suspected
60. Ensure that the CSP is committed to handover the data as created by the entity in the entity-required format without any vendor lock-in restrictions or format limitations.
61. Enable encryption on all Windows and Linux VMs and managed disk VMs
62. Enable encryption on all volumes with mount paths
63. Enable encryption on Linux VMs configured with disk striping (RAID) using mdadm or using LVM for data disks
64. Ensure that the role-based access controls (RBAC) have been set
65. Ensure that X.509 certificates have been enabled on the service fabric by an approved CA (such as the CA provided by the Qatar MOI and MOTC)
66. Ensure that cluster security has been configured to support node to node authentication and communication
67. Ensure that encryption of date across nodes takes place during replication

Note: *the above hardening guidelines are derived mainly from (Cloud Security Alliance (CSA), Microsoft Azure hardening guidelines and the Qatari Cloud security standard)*

15.8 Cloud Logs and log sources

The below diagram illustrates the location and type of logs expected to be collected from the various cloud fabric layers

Figure 96: Cloud logs and log sources



This table below lists the type of events expected to be enabled and collected in the cloud infrastructure.

Table 91: Types of events to be enabled and collected in cloud infrastructure

Security Logs	Activity logs	CSP Audit reports
Sign-ins from unknown sources	Application usage: summary	Directory audit report
Sign-ins after multiple failures	Application usage: detailed	
Sign-ins from outside Qatar/Restricted geographies	Application dashboard	
Sign-ins from IP addresses with suspicious activity	Account provisioning errors	
Irregular sign-in activity	Individual user devices	
Sign-ins from possibly infected devices	Individual user Activity	
	Password Reset Registration Activity Report	

15.9 Cloud security tools

Type of security devices or tools that should be used for hardening and securing the cloud infrastructure.

Table 92: Cloud Security Tools

Device	Features
Network Firewall	• Enforcing firewall rules or access control policies for the incoming network access requests • Provision to export log data to the central logging server • Provision to export specific duration of logs
Web Application Firewall	• Enforcing firewall rules or access control policies for the incoming web-based requests • Provision to export log data to the central logging server • Provision to export specific duration of logs
IDS/IPS	• Detecting and mitigating malicious attacks from the Internet

Device	Features
	• Security network detection tools that can support in identifying malware and malicious traffic based on known signatures • Provision to export log data to the central logging server • Provision to export specific duration of logs
SIEM	• Maintaining and correlating logs for monitoring, auditing and analysis • Optional: Analytics Solutions capable of identifying network anomalies based on machine learning and network and behaviour baselining • Provision to export log data to the central logging server • Provision to export specific duration of logs
Reverse proxy	• Redirecting the incoming requests to the corresponding back-end servers. This redirection involves mapping and translating the destination addresses on the front-end devices, typically firewalls, to the back-end server addresses
Forward proxy	• Performing auditing for communication initiated from within the virtual network to the Internet.
VPN Concentrator	• Acting as the cross-premises VPN gateways for cross-premises VPN connectivity between customer on-premises networks and the CSP • Provision to export log data to the central logging server • Provision to export specific duration of logs
OTA multi factor authentication system	• Providing the cloud services users with an additional one-time security for accessing the services in the beginning of every session • Provision to export log data to the central logging server • Provision to export specific duration of logs
Cloud based logs	• Provision to access the following logs: NetFlow logs, DNS logs and Virtualization fabric security logs.

15.10 Skills required for cloud security assets hardening

Following are the skills expected from personnel executing cloud hardening and security activities:

- Solid Knowledge of cloud security concepts and fundamentals
- Capable of Evaluating the cyber risks to cloud security and virtualized environments
- Solid knowledge of hardening cloud platforms and the underlying cloud fabric
- Knowledge of the unique cyber security risks pertaining cloud environments such as multi-tenancy, the rapid and agile deployment risks
- Capable of working with and supporting the Security monitoring team and the entity's SOC function in monitoring the Cloud infrastructure
- Solid understanding of applicable best practices and security standards such as ISO 27017, NIST SP 800-145, NIST SP 500-291 and Qatar National cloud security standard version 2.0 and above

- Good understanding of the legal, regulatory and privacy implications of cloud computing
- Suggested professional certifications which can help personnel to attain skills for the services defined under cloud security

Table 93: Cloud security certifications

Category	Recommended Certifications
Cloud Fundamentals	• SANS GIAC Cloud Security Fundamentals (SEC 524) • Cloud Security Alliance (CCSK) certificate of cloud security knowledge
Security hardening (General)	• EC-Council Certified Ethical Hacker (CEH), • SANS GIAC Certified Enterprise Defender (GCED) • SANS GIAC Security Essentials (GSEC)

15.11 Mapping with Industry Standards

Following table provides mapping of activities defined in the capability with other local Qatari and prevalent industry information security standards.

Table 94: Cloud security activities mapping industry cyber security standards – Part I of II

Service Name — Cloud Assets security hardening									
Process Phases	**Activities/ Controls**	**Controls Reference — NIA (Qatar National Information Assurance - Cloud Security Policy V1.2**	**Controls Reference — NIA (Qatar National Information Assurance Policy V2.0**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Stripping Apps	Removing unnecessary software apps								

Service Name — Cloud Assets security hardening									
Process Phases	**Activities/ Controls**	**Controls Reference — NIA (Qatar National Information Assurance - Cloud Security Policy V1.2**	**Controls Reference — NIA (Qatar National Information Assurance Policy V2.0**	**Controls Reference — ISO/IEC 27001:2013**	**Controls Reference — NIST SP 800-53 Rev. 4**	**Controls Reference — PCI DSS 3.2**	**Controls Reference —HIPAA**	**Controls Reference — Cloud Security Alliance (CCMv3.0.1)**	**Controls Reference — GDPR**
Stripping credentials	Disabling or removing unnecessary usernames and credentials				AC-2	2.1			
Stripping services and connectivity	Disabling or removing unnecessary services and ports	12.2.1							
Patching and baselining	Applying security and functionality patches (Covering operating system and all approved applications)	14.2.2							
Verification	Performing a full scan for verification purposes								

Annexure – I – Security Metrics

Security Metrics

From the capabilities defined in this framework perspective, security metrics are the measurable parameters to validate effectiveness of activities defined in the capability.

The goals of defining a security metrics are:

- Ensure objectives of implementation of capability have been achieved
- Generating quantifiable data to facilitate insights
- Assist in establishing deficiencies or limitations of implemented activities
- Implicitly focus on areas for improvement
- Support the SCDL reporting office

Following Tables defines security metrics for respective capabilities defined in the framework.

- Data sets are the parameters which will be used in calculation of the metrics.

Table 95: Security Metrics – Cybersecurity Governance

Cybersecurity Governance	
Security Metrics [Frequency = Monthly]	**Data Sets**
Cybersecurity Awareness Coverage • For individual security awareness training scheduled: Percentage of employees completed security awareness training = [Number of employees completed security awareness trainings/Number of employees scheduled for that security awareness training] * 100 • For Overall security awareness training: Average (Percentage of employees completed security awareness training)	• Number of security awareness trainings conducted • Number of employees completed per security awareness trainings
Cybersecurity Training Coverage • For individual specialized cybersecurity training scheduled:	• Number of specialized trainings organized • Number of employees completed specialized cybersecurity training

Cybersecurity Governance	
Percentage of employees completed specialized cybersecurity training = [Number of employees completed specialized cybersecurity trainings/Number of employees scheduled for that specialized cybersecurity training] * 100 • For Overall specialized cybersecurity training: Average (Percentage of employees completed specialized cybersecurity training)	

Table 96: Security Metrics – Endpoint Security

Endpoint Security	
Security Metrics [Frequency = Monthly]	**Data Sets**
Secure Configuration Coverage • Percentage of endpoints on which organization's secure configuration was enforced successfully = [Number of Endpoints on which organization's secure configuration was enforced successfully/Number of Endpoints owned by the organization] * 100 • Percentage of endpoints on which organization's secure configuration enforcement failed = [Number of Endpoints on which organization's secure configuration enforcement failed/Number of Endpoints owned by the organization] * 100 • Percentage of endpoints on which organization's secure configuration was enforced successfully with exceptions = [Number of Endpoints on which organization's secure configuration was enforced successfully with exceptions/Number of Endpoints owned by the organization] * 100 • Percentage of endpoints on which organization's secure configuration was not enforced = [Number of Endpoints on which organization's secure configuration was not enforced/Number of Endpoints owned by the organization] * 100	• Number of Endpoints owned by the organization • Number of Endpoints on which organization's secure configuration was enforced successfully • Number of Endpoints on which organization's secure configuration enforcement failed • Number of Endpoints on which organization's secure configuration was enforced successfully with exceptions • Number of Endpoints on which organization's secure configuration was not enforced

Table 97: Security Metrics – Application Security

Application Security	
Security Metrics [Frequency = Monthly]	**Data Sets**
Secure Application by Development Coverage • Percentage of number of applications which has not passed through secure coding application security methods during the development phase = [Total number of application which has not passed through secure coding application security methods during the development phase/Total number of applications used in the organization] * 100 • Percentage of number of applications which has not passed through threat modelling application security methods during the development phase = [Total number of application which has not passed through threat modelling application security methods during the development phase/Total number of applications used in the organization] * 100 • Percentage of number of applications which has not passed through design review application security methods during the development phase = [Total number of application which has not passed through secure coding application security methods during the development phase/Total number of applications used in the organization] * 100	• Number of applications used in organization • Number of applications which has not passed through Secure Coding application security methods during the development phase • Number of applications which has not passed through Threat Modelling application security methods during the development phase • Number of applications which has not passed through Design Review application security methods during the development phase
Secure Application by Implementation Coverage • Percentage of number of applications which has not passed through SAST application security methods during the implementation phase = [Total number of application which has not passed through SAST application security methods during the implementation phase/Total number of applications used in the organization] * 100 • Percentage of number of applications which has not passed through DAST application security methods during the implementation phase = [Total number of application which has not passed through DAST application security methods during the implementation phase/Total number of applications used in the organization] * 100 • Percentage of number of applications which are not covered by application level vulnerability shielding = [Total number of application which are not covered by application level vulnerability shielding/Total number of applications used in the organization] * 100	• Number of applications used in organization • Number of applications which has not passed through SAST application security methods during the Implementation phase • Number of applications which has not passed through DAST application security methods during the development phase • Number of applications which are not covered by application level vulnerability shielding
Application level vulnerabilities Coverage	• Number of applications used in organization

Application Security	
• Percentage of applications having HIGH vulnerabilities = [Number of applications having HIGH vulnerabilities/Number of applications] * 100 • Percentage of applications having MEDIUM vulnerabilities = [Number of applications having MEDIUM vulnerabilities/Number of applications] * 100 • Percentage of applications having no HIGH and MEDIUM vulnerabilities = [Number of applications having no HIGH and MEDIUM vulnerabilities/Number of applications] * 100 • Percentage of applications on which HIGH and MEDIUM vulnerabilities were fixed = [Number of applications on which HIGH and MEDIUM vulnerabilities were fixed/ (Number of applications having HIGH vulnerabilities + Number of applications having MEDIUM vulnerabilities)] * 100	• Number of applications having HIGH vulnerabilities • Number of applications having MEDIUM vulnerabilities • Number of applications with no HIGH and MEDIUM vulnerabilities • Number of applications on which HIGH and MEDIUM vulnerabilities were fixed

Table 98: Security Metrics – Change and Patch Management

Change and Patch Management	
Security Metrics [Frequency = Monthly]	**Data Sets**
Patch Management Coverage • Percentage of systems covered under patch management = [Number of systems covered under patch management/Total number of systems] * 100 • Percentage of systems not covered under patch management = [Number of non-patched systems/Total number of systems] * 100 • Percentage of systems where patch was not implemented successfully = [Number of systems where patch was not implemented successfully/Number of systems where patch was pushed] * 100 • Average time to apply applicable patches = Sum of all [Time to apply applicable patches]/Total Count of successful implemented patches	• Number of systems (endpoints, network devices and security devices) covered under patch management • Number of Non-patched systems = [Total number of systems - Number of systems covered under patch management] • Number of systems where patch was not implemented successfully • Time to apply applicable patches = [Number of hours (Date of availability of patch – TO – Date of successful implementation of patch)]/Number of patches implemented successfully on the all systems during specified period

Change and Patch Management	
Change Management Coverage • Percentage of change requests approved with cybersecurity review = [Number of changes approved with cybersecurity review/Number of change requests approved] * 100 • Percentage of change requests approved without cybersecurity review = [Number of changes approved without cybersecurity review/Number of change requests approved] * 100 • Average time to complete change = Sum of all [Time to complete change]/Total count of successfully completed changes	• Number change request received • Number of change requests approved • Number of changes approved with cybersecurity review • Number of changes approved without cybersecurity review = Number of change requests approved – Number of changes approved with cybersecurity review • Time to complete change = Number of hours (Date of change request submitted – TO – Date of change request completed)

Table 99: Security Metrics – Security Monitoring and Operations

Security Monitoring and Operations	
Security Metrics [Frequency = Monthly]	**Data Sets**
Threat Intelligence Coverage • Percentage of successfully implemented threat intelligence feeds = [Number of threat intelligence feeds implemented successfully/Number of threat intelligence feeds received from sector/national level] * 100	• Number of threat intelligence feeds received from sector/national level • Number of threat intelligence feeds implemented successfully • Number of threat intelligence feeds generated (internal threat intelligence) and shared with sector/national level
Security Audit Logs Coverage • Percentage of systems from where security audit logs are being collected = [Number of systems from where security audit logs are being collected/Total number of systems in the organization] * 100 • Percentage of systems from where security audit logs are not being collected = [Number of systems from where security audit logs are not being collected/Total number of systems in the organization] * 100	• Total number of systems in the organization • Number of systems from where security audit logs are being collected • Number of systems from where security audit logs are not being collected = [Total number of systems in the organization - Number of systems from where security audit logs are being collected]

Security Monitoring and Operations	
• Percentage of application from where security audit logs are being collected = [Number of applications from where security audit logs are being collected/Total number of applications in the organization] * 100 • Percentage of applications from where security audit logs are not being collected = [Number of applications from where security audit logs are not being collected/Total number of applications in the organization] * 100	• Total number of applications used • Number of applications from where security audit logs are being collected • Number of applications from where security audit logs are not being collected = [Number of applications from where security audit logs are being collected - Total number of applications used]
Vulnerability Scan Coverage • Percentage of systems having HIGH vulnerability = [Number of systems having HIGH vulnerabilities/Number of systems included for vulnerability scan] * 100 • Percentage of systems having MEDIUM vulnerabilities = [Number of systems having MEDIUM vulnerabilities/Number of systems included for vulnerability scan] * 100 • Average time to mitigate HIGH and MEDIUM vulnerabilities = Sum of all [Time to mitigate HIGH and MEDIUM vulnerabilities]/Total count of vulnerabilities mitigated	• Number of systems included for vulnerability scan • Number of systems having HIGH vulnerabilities • Number of systems having MEDIUM vulnerabilities • Time to mitigate HIGH and MEDIUM vulnerabilities = Number of hours [Date of detection – TO – Date of mitigation]
Events Categorization Coverage • Percentage of ALERTS observed = [(Number of EVENTS categorized as ALERTS – Number of ALERTS considered as false positives)/Number of EVENTS received] * 100 • Percentage of INCIDENTS observed = [(Number of EVENTS/ALERTS categorized as INCIDENTS – Number of INCIDENTS considered as false positives)/Number of EVENTS received] * 100 • Percentage of BREACH observed = [Number of EVENTS/ALERTS/INCIDENTS categorized as BREACH/Number of EVENTS received] * 100	• Number of EVENTS categorized as ALERTS • Number of ALERTS considered as false positives • Number of EVENTS/ALERTS categorized as INCIDENTS • Number of INCIDENTS considered as false positives • Number of EVENTS/ALERTS/INCIDENTS categorized as BREACH

Table 100: Security Metrics – Incident Handling and Response

Incident Handling and Response	
Security Metrics [Frequency = Monthly]	**Data Sets**
Incident Handling and Response Coverage • Average Dwell Time = Sum of Dwell time of each incident/Number of incidents • Average Containment Time = Sum of containment time of each incident/Number of incidents • Average Recovery Time = Sum of recovery time of each incident/Number of incidents • Average time between incidents = Sum of all [Time between two incidents]/Total count of incidents • Average time between same category of incidents = Sum of all [Time between two same category of incidents]/Total count of incidents	• Number of INCIDENTS/BREACH handled • Dwell time = Number of hours (Time of attack – Time of detection) • Containment time = Number of hours (Time of detection – Time of containment successfully completed) • Recovery Time = Number of hours (Time of containment successfully completed – Time of recovery successfully completed) • Time between two incidents = Number of hours [Date of last incident detection – TO – Date of current incident occurrence] • Number of each type of incidents observed (refer incident categories) • Time between two same categories of incidents = Number of hours [Date of last incident detection – TO – Date of current incident occurrence]

Table 101: Security Metrics – Identity and Access Management

Identity and Access Management	
Security Metrics [Frequency = Monthly]	**Data Sets**
User Accounts Coverage • Percentage of dormant accounts = [Number of dormant accounts/Total number of user accounts] * 100	• Total number of user accounts • Number of privileged user accounts • Number of dormant user accounts • Number of user accounts created

Identity and Access Management	
• Percentage of privileged user accounts = [Number of privileged accounts/Total number of user accounts] * 100 • Percentage of new privileged user accounts created = [Number of privileged accounts created/Number of privileged user accounts] * 100 • Percentage of deleted user accounts = [Number of user accounts deleted/Total number of user accounts] * 100	• Number of user accounts created with privileged access • Number of user accounts deleted

Annexure – II – Glossary

Glossary

Term	Description
AAA	Authentication, authorization, and accounting
ACE	Application Control Engine
ACL	Access Control List
ACS	Access Control Server
AES	Advanced Encryption Standard
AH	Authentication Header
ARP	Address Resolution Protocol - A low-level TCP/IP protocol that maps a node's hardware address (called a "MAC" address) to its IP address
AS	Advanced Services (Cisco)
ASA	Adaptive Security Appliance – See Cisco.com
BGP	Border Gateway Protocol
BRI	Basic rate interface
CA	Certificate Authority
CAA	Clean Access Agent/NAC Agent
CAM	Clean Access Manager/NAC Appliance Manager
CAS	Clean Access Server/NAC Appliance Server
CCA	Cisco Clean Access/Cisco NAC Appliance
CCO	Cisco Connection Online
CDP	Cisco Discovery Protocol
CE	Configuration Engine
CHAP	Challenge Handshake Authentication Protocol
CPE	Customer Premises Equipment
CRL	Certificate Revocation List
CSA	Cisco Security Agent – Host based IDS/IPS software
CSAMC	CSA Management Console
CSM	Cisco Security Manager
DES	Data Encryption Standard
DH	Diffie-Hellman

Term	Description
DNS	Domain Name Service
DSL	Digital Subscriber Line
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FAA	Functional Area Analysis
FCAPS	Fault, Configuration, Accounting, Performance & Security (FCAPS) functions of the OSI management model
Firewall(ing)	Stateful packet filtering device, which maintain state tables for IP-based protocols. Traffic is only allowed to cross the firewall if it conforms to the access-control filters defined, or if it is part of an already established session in the state table. “enclosing” a network area behind a device that offers network attack protection
FTP	File Transfer Protocol.
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation protocol
HMAC	Hash Message Authentication Code
Host IDS	Host Intrusion Detection System is a software application that monitors activity on an individual host. Monitoring techniques can include validating operating system and application calls, checking log files, file system information and network connections
Host IPS	Host Intrusion Protection System
HSRP	Hot-Standby Routing Protocol
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Number Authority - Assigns all port and protocol numbers for use on the Internet. You can view port numbers at the following site: http://www.iana.org/assignments/port-numbers You can view protocol numbers at the following site: http://www.iana.org/assignments/protocol-numbers
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
IKMP	Internet Key Management Protocol
IOS	Inter-network operating system
IOS Firewall	A stateful packet filtering firewall running natively on Cisco IOS (Internetwork Operating System).

Term	Description
IOS Router	A wide spectrum of flexible network devices, which provide many routing and security services for all performance requirements. Most devices are modular and have a range of LAN and WAN physical interfaces.
IPSec	IP Security protocol
ISAKMP	Internet Secure Association Key Mapping Protocol
ISDN	Integrated Services Digital Network
ISE	Identity Services Engine
ISO	International Organization for Standardization
LAN	Local Area Network
Layer 2 Switch	Provides bandwidth and VLAN services to network segments at the Ethernet level. Typically, these devices offer 10/100 individual switched ports, Gigabit Ethernet uplinks, VLAN trunking, and L2 filtering features.
Layer 3 Switch	Provides similar high throughput functions of a Layer 2 switch with added routing, QoS, and security features. These switches often have the capability of special function processors.
LLD	Low Level Design
MD5	Message Digest 5
MIB	Management Information Base
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
MTU	maximum transmission unit
NAC	Network Admission Control (Control of non-compliant devices - NAC)
NAS	Network Access Server
NAT	Network Address Translation
Network IDS	Network Intrusion Detection System. Typically used in a non-disruptive manner, this device captures traffic on a LAN segment and tries to match the real-time traffic against known attack signatures. Signatures range from atomic (single packet and direction) signatures to composite (multipacket) signatures requiring state tables and Layer 7 application tracking
NRIA	Network Resiliency Improvement Analysis
NCE	Network Security Engineer
NSAR	Network Security Architecture Review
SDN	Software Defined Network
NTP	Network Time Protocol
ORA	Operational Readiness Assessment
OS	Operating System
OSI	Open Systems Interconnection

Term	Description
OSPF	Open Shortest Path First protocol
OTP	One Time Password
PAP	Password Authentication Protocol
PAP	Policy Administration Point
PAT	Port Address Translation
PBR	Policy Based Routing
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PFS	Perfect Forward Secrecy
PIP	Policy Information Point
PIX	Private Internet Exchange
PKI	Public Key Infrastructure
PoP	Point of Presence
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunnelling Protocol
PRI	Primary Rate Interface
PSN	Policy Services Node
RADIUS	Remote Authentication Dial-In User Service
Riverhead	DoS and Anomaly detection/mitigation device
RRI	Reverse Route Injection – a reverse route is injected into a routing area.
RSA	Rivest-Shamir-Adelman - they are the inventors of the RSA cryptosystem, an asymmetric key encryption scheme.
SA	Security Association
SAFE	Secure Architecture for Enterprise
Script kiddies	Simply download other people's hacking tools and use them to hack
SDG	Secure Data Gateway
SDP	Secure Device Provisioning
SHA	Secure Hashing Algorithm
Signatures (definitions)	tell-tale characteristics - the fingerprints or DNA of viruses and other malware Signature files are frequently updated, as often as once a day
SLA	Service Level Agreement
SLB	Server Load Balancer
SMB	Secure Management Gateway

Term	Description
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
Social engineering	Convincing a computer user to provide information, for example passwords, that makes gaining access to a computer or online account easy
SPA	Security Posture Assessment
Spoof(ing)	Sending information or messages and making it look like it's from another source.
SSH	Secure Shell - A cryptographically strong replacement for rlogin, telnet, ftp, and other programs. Protects against ``spoofing'', man in the middle attacks, and packet sniffing.
SSO	Single Sign On – a user uses one set of credentials (username and password) once only to be authentication to multiple systems at the same time.
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TP	Technology Practices (Cisco)
Trojan Horse	Parasitic software used to infiltrate targeted computers so the Trojan-master can access them remotely. Often designed for a specific purpose, such as relaying spam, but some Trojans give the master total control of the computer. Trojans seldom do damage, as a virus would, because the master wants his control to remain hidden.
Virus	A program that reproduces its own code by attaching itself to other executable or other file types so that the virus code runs when the infected file is run. Viruses almost always seek to do damage as well as replicate.
VLAN	Virtual Local Area Network (LAN)
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
War Dialling	War dialling is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise to circumvent perimeter security.
Worm	Malicious code that breaks into other computers and starts itself running with no human intervention, and subsequently attempts to break into more computers from the newly infected one
Wire Tapping	Monitoring and recording data that is flowing between two points in a communication system
WWTP	World Wide Technology Practices
Zombie	A computer with a Trojan horse installed. The Trojan lets the Trojan owner access the computer remotely. Now it can be used as a staging ground for anonymous attacks on other computers.

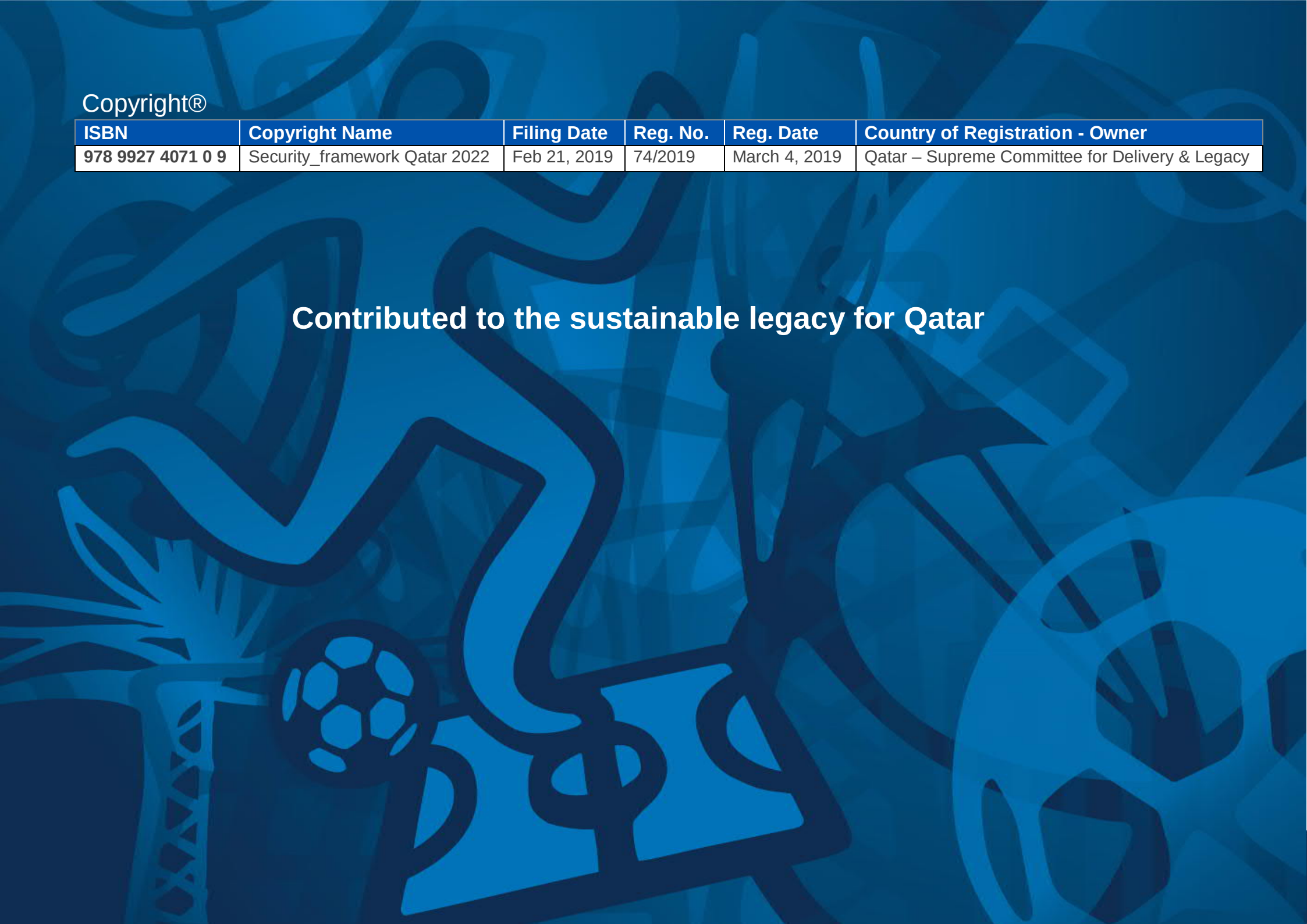
Annexure – III – References

References

- http://www.motc.gov.qa/en/documents/document/national-cyber-security-strategy
- http://www.motc.gov.qa/en/documents/document/national-information-assurance-policy
- http://www.motc.gov.qa/en/documents/document/national-standards-security-critical-industrial-automation-and-control-systems
- https://qatarlaw.com/wp-content/uploads/2017/05/Personal-Data-Privacy-Law-No.-13-of-2016.pdf
- http://www.motc.gov.qa/en/documents/document/qatars-e-commerce-law
- http://www.motc.gov.qa/en/documents/document/qatars-e-authentication-framework
- http://www.motc.gov.qa/en/documents/document/cloud-security-policy-government-agencies
- http://www.motc.gov.qa/en/documents/document/open-data-policy
- http://www.motc.gov.qa/en/documents/document/data-management-policy
- http://www.motc.gov.qa/en/documents/document/government-website-and-e-services-framework
- https://ccdcoe.org/cyber-security-strategy-documents.html
- https://www.asd.gov.au/infosec/acsc.htm
- https://www.nist.gov/cyberframework/framework-resources
- https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- https://csrc.nist.gov/publications/detail/sp/800-86/final
- https://csrc.nist.gov/publications/detail/sp/800-137/final
- https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final
- https://csrc.nist.gov/publications/detail/sp/800-145/final
- https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp
- https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final
- https://nvd.nist.gov/800-53
- http://www.crest-approved.org/industrial-control-systems-technical-security-assurance/index.html
- http://www.crest-approved.org/cyber-security-incident-response-maturity-assessment/index.html
- http://www.crest-approved.org/cyber-security-monitoring-and-logging-guide/index.html
- https://www.sans.org/reading-room/whitepapers/forensics
- https://www.sans.org/reading-room/whitepapers/incident
- https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
- https://www.sans.org/reading-room/whitepapers/assurance
- https://www.sans.org/reading-room/whitepapers/warfare
- https://www.sans.org/reading-room/whitepapers/intrusion
- https://www.sans.org/reading-room/whitepapers/detection

- https://www.sans.org/reading-room/whitepapers/malicious
- https://www.sans.org/reading-room/whitepapers/testing
- https://www.sans.org/reading-room/whitepapers/securecode
- https://www.sans.org/reading-room/whitepapers/application
- https://www.sans.org/reading-room/whitepapers/securityanalytics
- https://www.sans.org/reading-room/whitepapers/modeling
- https://www.sans.org/reading-room/whitepapers/soc
- https://www.sans.org/reading-room/whitepapers/securitytrends
- https://www.sans.org/reading-room/whitepapers/threathunting
- https://www.sans.org/reading-room/whitepapers/threatintelligence
- https://www.sans.org/reading-room/whitepapers/threats
- https://www.sans.org/reading-room/whitepapers/tools
- https://www.sans.org/reading-room/whitepapers/ActiveDefense
- https://www.cisecurity.org/controls/
- http://www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/GroupDocuments/critical-controls-poster-2016(1).pdf
- https://www.iiconsortium.org/IISF.htm
- http://qcert.org/library/36
- http://www.qcert.org/awareness/documents-presentations/guidelines-incident-management-prerequisite-measures-english-v11
- https://sqrrl.com/resource/a-framework-for-hunting-white-paper/
- https://sqrrl.com/resource/huntpedia-threat-hunting-knowledge-compendium/
- https://sqrrl.com/resource/hunt-evil-practical-guide-threat-hunting/

ISBN	Copyright Name	Filing Date	Reg. No.	Reg. Date	Country of Registration - Owner
978 9927 4071 0 9	Security_framework Qatar 2022	Feb 21, 2019	74/2019	March 4, 2019	Qatar – Supreme Committee for Delivery & Legacy



Contributed to the sustainable legacy for Qatar