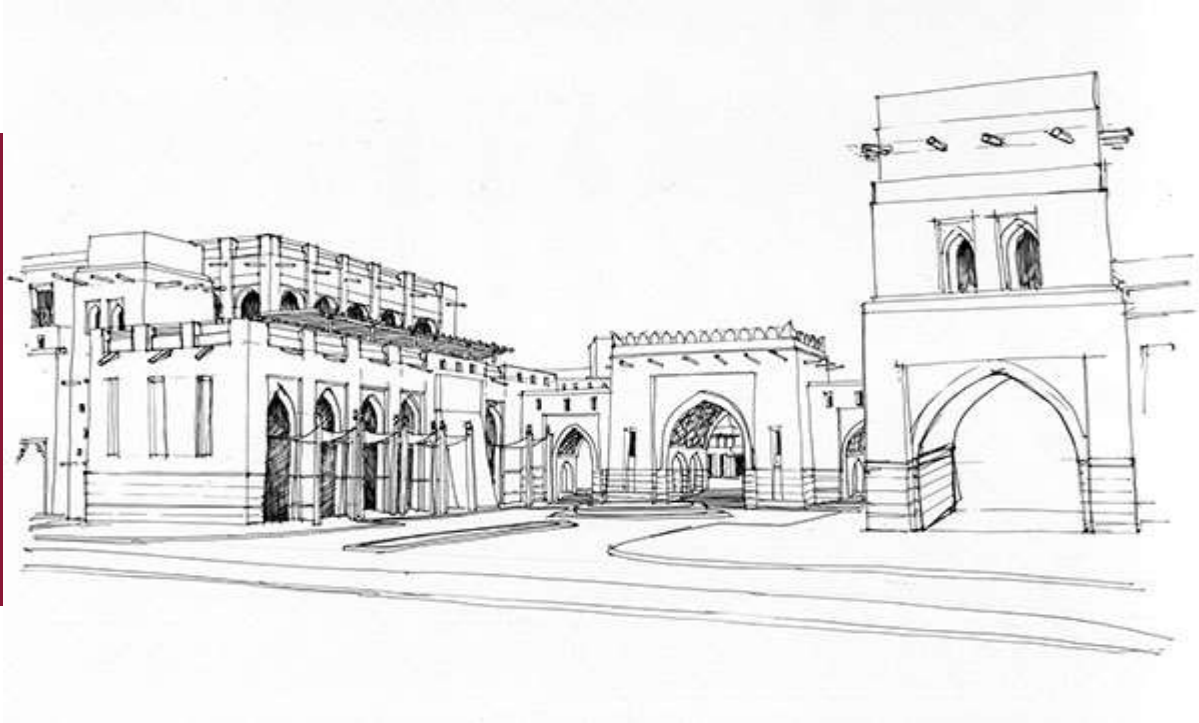




5: Security Management

Government Enterprise Architecture
(GEA)



January 2018





Table of Contents

1	Introduction	4
2	Document Structure	5
3	Security Management Overview	6
4	Security Policies	9
4.1	National Security Assurance (NIA) policy	9
4.2	Cloud Security policy	10
4.3	Bring Your Own Device (BYOD) security policy	11
5	Security frameworks and standards	12
5.1	Qatar e-authentication framework	12
5.2	Information Security Risk Management Framework and procedures	12
5.3	National Industrial Control Systems Security standards	13
5.4	Information security framework for school networks	14
5.5	Smart Qatar Information security standards	15
6	Appendix 1 Security Operations controls	17
6.1	Control Applicability	17
6.2	Security Operations Management	17
6.2.1	Information Systems Operations Management [OM]	17
6.2.2	Data Centre Security Controls (DCS)	22
6.3	Information Security Roles and Responsibilities	26
7	Glossary	27



Table of Figures

<i>Figure 1 - Security management framework</i>	<i>7</i>
---	----------

1 Introduction

Information is one of the core assets of any large organization. Within Qatari Government (like any other Government), every aspect of running the country relies on the availability of good management information (for example about all citizens and other residents). The key purpose of the Security management deliverable is to ensure that government information is securely protected. This document serves as a central registry with references to existing set of security related policies and standards prescribed for government agencies in Qatar. The diagram below illustrates all the deliverables of the GEA and highlights Security management as a cross cutting dimension.

2 Document Structure

GEA Security management document is structured as described below.

- **Security management overview** – provides an overview of security management framework in Qatar Government
- **Security Policies** – lists the current set of security related policies for Qatar government agencies
- **Security framework & standards** – lists the set of security frameworks and related standards for Qatar government agencies
- **Appendix 1: Security Operations controls** – lists the controls required for effective security operations at Qatar government agencies and also the roles and responsibilities required for effective implementation of NIA policies and controls in agencies
- **Glossary** – lists all the Acronyms used in the document and their expansions.

3 Security Management Overview

Information security is not only a technical issue, but also a business and governance challenge that involves risk management, reporting, and accountability. It is a top-down process requiring a comprehensive information security strategy that is explicitly linked to the organization's business processes and objectives.

Effective security requires the active engagement of executive management to address emerging threats and provide strong cyber security leadership. The term used to describe executive management's engagement is Information Security Governance. Information Security Governance consists of the set of policies and internal controls by which information security activities within an organization, irrespective of size or form, are directed and managed. Risk management, reporting, and accountability are core focus area of all information security policies and internal controls.

Information security governance is a subset of an organization's overall corporate governance programme. For security to be effective, it must be included in all organizational and business processes from end to end - physical, operational and technical. A formal information security strategy must be implemented by developing comprehensive information security policies consistent with the goals and mission of the organization. To provide effective governance, a set of enterprise standards for each policy must be developed to provide defined boundaries for acceptable processes and procedures. Education, training and awareness must also be considered to convey information to all personnel as part of an ongoing process to change behaviours not conducive to secure, reliable operations.

The strategy must then be implemented through a comprehensive information security programme that includes well-conceived and complete policies and standard.

The diagram below captures the security management framework for Qatar.

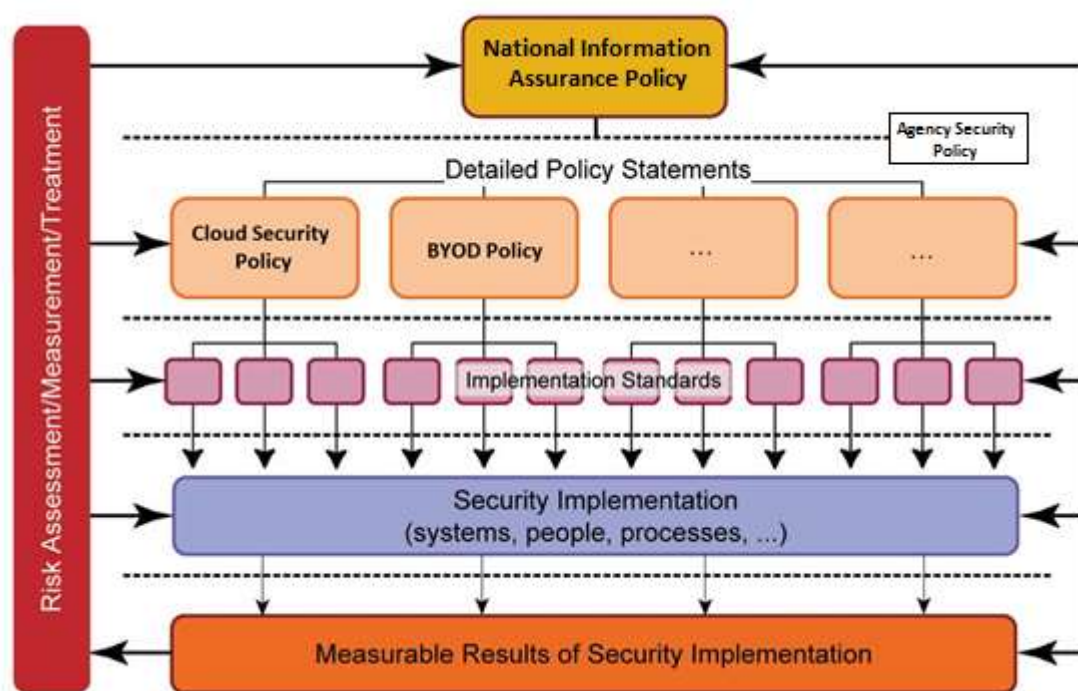


Figure 1 - Security management framework

On the top level, Qatar National Information Assurance policy documents the information security policies setting out the organization's commitment to, and high-level objectives and expectations for, the delivery of information confidentiality, integrity and availability. It provides the mandate for all more detailed security policies and controls that need to be implemented at individual government agencies.

National Information Assurance policy is a high-level (tactical) statement, endorsed by senior management, from which can be derived more detailed definitions covering specific business or operational areas.

Agency security policy will be established in individual government agencies to present and provide the senior management support for the required information assurance.

The information security policy is mapped onto a series of lower-level policies, each with a specific scope e.g. – Cloud security policies, BYOD policies. These lower-level policies together deliver the overall security policy requirement.



The standards documentation covering multiple functional areas will guide government agencies in planning and implementing security controls required by policies. Agencies are expected to implement security policies and standards through a combination of system, people and processes. Effective risk assessment, measurement and treatment processes should also be in place to effectively implement, monitor and enhance security controls in agencies.

4 Security Policies

This section captures the current list of security policies mandated to government agencies in Qatar.

4.1 National Security Assurance (NIA) policy

Published by Q-CERT, MoTC, NIA policy provides Qatar government agencies with the necessary foundation and the relevant tools to enable the implementation of a full-fledged Information Security Management System within the agency. It applies to all agencies and their corresponding information assets. Where the agency has outsourced or subcontracted any processes or activities they should ensure they comply with NIA policies and associated controls. It covers the following security domains.

- Access Control Security [AM]
- Audit & Certification [AC]
- Business Continuity Management [BC]
- Change Management [CM]
- Communications Security [CS]
- Cryptographic Security [CY]
- Data Labeling [DL]
- Data Retention & Archival [DR]
- Documentation [DC]
- Gateway Security [GS]
- Governance Structure [IG]
- Incident Management [IM]
- Information Exchange [IE]
- Logging, Auditing & Security Monitoring [SM]
- Media Security [MS]
- Network Security [NS]
- Personnel Security [PS]
- Physical Security [PH]
- Portable Device & Working Off-Site Security [OS]
- Product Security [PR]
- Risk Management [RM]
- Security Awareness [SA]
- Software Security [SS]
- System Usage Security [SU]
- Third Party Security Management [TM]

- Virtualization [VL]

For detailed set of NIA policies and controls, please refer to the current version of the document in Q-CERT website -

http://www.qcert.org/sites/default/files/public/documents/nia_policy_english_v2.0.pdf

Arabic version can be found at

http://www.qcert.org/sites/default/files/public/documents/nia_policy_arabic_2.0.pdf

4.2 Cloud Security policy

Over the years the ICT organizations and ICT professionals in Qatar became well aware of the risks, governance practices and legal requirements that came with traditional IT desktop based environments. But due to the unique architecture and cross border locality nature of cloud services the privacy and security requirements for personal information (Qatar's information privacy and protection draft Law) and security requirements for government data (National Information Assurance Policies), transactions and communication must be addressed with a different perspective.

This policy document captures all cloud related security policies and controls. It applies to all government agencies in the Qatari government that use or are planning to use cloud-computing services.

For detailed set of cloud security policies and controls, please refer to the current version of the document in Q-CERT website –

http://www.qcert.org/sites/default/files/public/documents/cs_cloud_security_policy-2017_english_v1.2.pdf

Arabic version can be found at

http://www.qcert.org/sites/default/files/public/documents/sys_tmyn_lhwsb_lshby_2017_v1.2.pdf

4.3 Bring Your Own Device (BYOD) security policy

With the rapid development in the growth, innovation and consumerization of technology, computers have become powerful and affordable. This has posed an interesting dilemma to organizations globally. Whilst the use of technology empowers users and increases productivity (the user being able to work from anywhere and being online all the time), it has stretched the organizations in terms of not only providing infrastructure support to such technology but also being able to innovatively secure their information which is now being spilled over their physical boundaries. Add to this scenarios where employees would like to choose or use their own device.

This policy expects to set the tone and expectations within an agency to deal with the current scenario wherein users would like to use their own devices for official work (Bring Your Own Device (BYOD)) or have a say in the choice of devices being made available to them.

This policy is applicable to the following type of devices:

- Any Computing device that can store and / or process and / or transmit / receive information when connected to the controlled network

The policy applies to

- All government and semi government entities - MANDATORY
- All Critical sector organizations - RECOMMENDED
- Other corporate organizations operating in Qatar - OPTIONAL

For detailed set of BYOD security policies and controls, please refer to the current version of the document in Q-CERT website –

http://www.qcert.org/sites/default/files/public/documents/cs-csps_byod_policy_v1.0.pdf

5 Security frameworks and standards

This section captures the current list of published security standards and frameworks for Qatar government agencies.

5.1 Qatar e-authentication framework

Electronic authentication (or “e-Authentication”) is the process of determining the degree of confidence that can be placed on assertions that a user is who he claims to be or an identity is what it declares to be. Assertions include identity, role, delegation and value. The Qatar e-Authentication Framework (QeAF) is primarily concerned with the electronic authentication of assertions. Electronic transactions occur across a number of channels, including:

- Internet or web-based
- Telephone (IVR)
- Facsimile transmissions

The Qatar e-Authentication Framework (QeAF) intends to ensure that a strategic approach is adopted by entities involved to assure online identification. The framework advocates a risk based approach, balancing between the business objectives and the risks.

The scope of the Qatar e-Authentication Framework (QeAF) applies to:

- All government and semi government entities
- All Critical sector organizations
- Private businesses incorporated and / or operating in Qatar

Each entity should use this framework to assess and evaluate their existing e-authentication means.

For detailed set of e-authentication framework and standards, please refer to the current version of the document in Q-CERT website –

http://www.qcert.org/sites/default/files/public/documents/cs-qima-qatar_e-authentication_framework_v1.0_0.pdf

Arabic version can be found at

http://www.qcert.org/sites/default/files/public/documents/cs-qima-qatar_e-authentication_framework_v1_0-arabic_0.pdf

5.2 Information Security Risk Management Framework and procedures

The objective of Qatar Information Security Risk Management Framework (ISRMF) is to

- provide assurance to management and stakeholders that critical information security risks are being managed appropriately
- encourage understanding by management and their staff of the implications of risk exposures
- enable better business resilience and compliance
- provide a rigorous decision-making and planning process.

Further, to achieve the objectives of Qatar National Cyber Security Strategy, QCERT has developed this ISRMF. It provides a systematic approach to agencies / organizations to identify, prioritize and manage information security risks and comply with the requirements of National Information Assurance (NIA) policy.

ISRMF provides a structured, yet flexible approach for managing information security risks resulting from the incorporation of information systems into the mission and business processes of agency / organization. This framework is suitable for the agency or organization's environment, and in particular it aligns with overall enterprise risk management framework (if applicable). Information security risk management framework addresses risks in an effective and timely manner where and when they are needed.

The following documents capture the framework and procedures.

ISRMF Framework documentation:

www.qcert.org/sites/default/files/public/documents/information_security_risk_management_framework_isrmf_ver_1.1-1.docx

ISRMF procedures documentation:

www.qcert.org/sites/default/files/public/documents/information_security_risk_management_procedure_isrmp_ver_1.1.docx

5.3 National Industrial Control Systems Security standards

Critical Infrastructure organizations that depend on Industrial Control Systems (ICS) have begun using commercial-off-the-shelf (COTS) technology developed for business systems in their everyday processes. This has provided an increased opportunity for cyber attacks against the critical systems they operate. These COTS systems are not usually as robust (at dealing with cyber attacks) as are systems designed specifically for Critical Infrastructure at dealing with cyber attack for many reasons. These weaknesses may lead to health, safety and environmental (HSE), or operational consequences that could severely affect the State of Qatar's economy, people or Government.

This ICS security baseline standard document provides the minimum controls that needs to be incorporated or addressed for any ICS system that has been determined to be critical. This document is to be used together with a suitable risk based security management program.

When assessing assets of a critical ICS system the following should be included:

- Control centres and backup control centres including systems at master and remote sites
- Transmission substations that support the reliable operation of the bulk systems
- Systems and facilities critical to system restoration, including black start generators and substations in the electrical path of transmission lines used for initial system restoration
- Systems that provide monitoring control, automatic generation control, real time systems modelling, and real time inter-utility data exchange.

For detailed set of National ICS security standards, please refer to the current version of the document in Q-CERT website –

[http://www.qcert.org/sites/default/files/public/documents/national_ics_security_standard_v.3 -
_final.pdf](http://www.qcert.org/sites/default/files/public/documents/national_ics_security_standard_v.3_-_final.pdf)

Arabic version can be found at

[http://www.qcert.org/sites/default/files/public/documents/national_ics_security_standard_v.3-
arabic.pdf](http://www.qcert.org/sites/default/files/public/documents/national_ics_security_standard_v.3-arabic.pdf)

5.4 Information security framework for school networks

Qatar Schools are vulnerable to cyber attacks, putting data of students, employees and administration at risk. This fact is based on reported security incidents from National and International Schools in Qatar. This is very alarming, considering that it is currently a common practice for Schools to have personal and confidential information about students, parents and staff on School computers, personal laptops, home computers, USB memory sticks and other media. Schools have a duty to safeguard staff and student's personal data stored and transmitted electronically.

This document provides the necessary information that enables staff and others meet their general responsibility to safeguard the School's information and assets. Schools may adapt the document to reflect their own circumstances in order to publish their own Information Security document.

It applies to:

- All services in the School;

- All employees and students of the School;
- Any third person working for the School or on School premises.

For detailed information on school network information security framework, please refer to the current version of the document in Q-CERT website –

http://www.qcert.org/sites/default/files/public/documents/information_security_framework_for_school_networks-v1_0.pdf

5.5 Smart Qatar Information security standards

Smart Qatar aims to leverage innovative applications of technologies to provide targeted services for individuals, businesses and government across priority sectors. Accelerated and effective development of Smart Qatar requires all actors from government, local and international businesses, start-ups and their supporting ecosystem, academic and research institutions, as well as the public to participate in the co-creation of smart services. The foundation of this whole-of-nation effort relies on the ability to collect and manage vast amounts of data, share and open it up based on defined rules and regulations, to be processed and analysed by these different actors for the build-up of innovative services and applications. As such, governance of this Program on a national level has been designed to harmonize efforts across the different actors and drive Smart Qatar development with a key focus on efficiency and building resilience and interoperability.

The Smart Qatar Program is expected to accelerate the build-up of ICT infrastructure, platforms, and applications and will expand the ecosystem of smart service developers and users to a national scale. As such, the Program has the potential to expose the country to additional security threats and challenges that need to be well understood.

Smart Qatar would be increasingly exposed to these threats through the employment of new technological developments in mobile applications, cloud computing, Internet of Things (IoT) in public and private spaces, and others. The vulnerabilities would either be from the technology itself or from the people owning, developing, or operating the smart services and their enabling platforms and technologies. Moreover, building capabilities to host millions of users and devices implies a virtually unlimited attack surface.

Smart Qatar needs to focus on effectively mitigating security threats and managing related vulnerabilities to protect sensitive information and infrastructure. To secure the Smart Qatar environment, the Smart Qatar Information Security Standard (SQISS) focuses on securing Smart Qatar services. These must be designed and offered with minimum levels of security to protect the confidentiality, integrity, and availability of information they leverage, and safeguard their operations.

SQISS applies to any Smart Qatar Service Owner i.e. owners of identified constituent services or enabling technology and platform services under the scope of Smart Qatar. Smart Qatar Service Owners are responsible for ensuring security controls are implemented and adopted sufficiently and effectively in relation to the information assets and capabilities being used for Smart Qatar services for which they have a custodial responsibility. This includes information assets and capabilities developed or managed by third-parties.

For detailed set of SQISS standards, please refer to latest version of Smart Qatar Information security standards document.

6 Appendix 1 Security Operations controls

In addition to the NIA policies and controls, this section lists the Security Operations specific controls that should be followed at Government agencies.

6.1 Control Applicability

The two levels of applicability are:

- *Mandatory* (should have) - The specific element of control specification is expected to be addressed in full, at all times, by all Agencies
- *Recommended* (can have) - The control specification would typically be anticipated to apply to agencies based on their asset value calculated as per asset classification standard

6.2 Security Operations Management

6.2.1 Information Systems Operations Management [OM]

Control #	Control Name	Impact Priority	High
OM 1.0	Operational Procedures and Responsibilities		
Control Definition	The Agency shall document and maintain its information security-related processes		
Control Type	Directive		
Control Specifications			
Specification #	Description		Applicability
OM 1.1	Procedures should be developed to allow for the consistent and secure development, introduction, management and retirement of information assets and information systems		Mandatory
OM 1.2	Procedures should form part of an integrated management system, aligned to the best practice of quality management. Procedures should function in support of agreed policies and should conform to agreed documentation standards active within the Agency		Mandatory
OM 1.3	Procedures should be aligned with, and conformant to, relevant laws, directives, regulations, and government standards. Such external references should be treated as having priority over the procedures; and contradictions should be resolved in favour of the external reference		Mandatory



OM 1.4	Procedures should be reviewed regularly, to ensure continued relevance and accuracy to the work being undertaken. Review should occur at least annually, or more frequently in the event of major business change	Mandatory
OM 1.5	Procedures should confirm the minimum mandatory activities that must be undertaken to achieve a defined outcome	Mandatory
OM 1.6	The Agency should define the roles required to transact its procedures. Procedures should show which role has primary responsibility for undertaking a given procedural activity	Mandatory
OM 1.7	Relevant staff and supplier personnel should be made aware of procedures relevant to their information security responsibilities and should be trained in their usage	Mandatory
OM 1.8	The Agency should ensure that responsibilities defined within procedures are suitably allocated between roles, to avoid segregation of duties conflicts	Mandatory
Control Dependencies	None	

NIA Policy Reference: Section B. Security Governance & Security Processes: 12. Documentation

Reference Used:

- ISO 27002 Information technology — Security techniques — Code of practice for Information Security management:
 - 10.1.1 Documented Operating Procedure

Control #	Control Name	Impact Priority	High
OM 2.0	Operational Change and Configuration Management		
Control Definition	The Agency shall control and document changes to the configuration and status of information assets and information systems		
Control Type	Directive , Preventive, Detective, Corrective		
Control Specifications			
Specification #	Description		Applicability



OM 2.1	A multi-disciplinary change approval board should review and approve proposed changes to information systems. The board's mandate should be formally defined and sponsored by the Agency's executive management. The board's quorum for decision making should be defined by the Agency and the criteria for approval determined in advance. The Agency's Chief Information Security Officer (CISO) should be a mandatory member of the board and the quorum for approving changes with a potential information security impact should include the CISO	Recommended
OM 2.2	Changes to information systems should only be undertaken in accordance with a defined change management process and only if subjected to a change impact assessment, with the change being implemented only if approved in advance of the change being implemented. All requirements for change should be documented within a Request For Change (RFC) document. The RFC should confirm: • Which party is requesting the change • What configuration items will be affected by the change • The nature of the change that will occur • The anticipated business benefit/driver for the change • When the change is proposed to occur • The urgency of the change • Who will test and who will implement the change • Who will verify the success of the change • What impact the change will have upon existing references (e.g. the information system design, relevant policies, contracts) • Which parties are anticipated to be mandatory approvers of the change	Mandatory
Control Dependencies	None	

NIA Policy Reference: Section B. Security Governance & Security Processes: 5. Change Management

Reference Used:

- ISO 27002 Information technology - Security techniques - Code of practice for Information Security management:
 - 10.1.2 Change Management
- NIST Special Publication 800-53 Revision 3:
 - CM-1 Configuration Management Policy and Procedures
 - CM-3 Configuration Change Control
 - CM-2 Baseline Configuration

Control #	Control Name	Impact Priority	High
OM 3.0	Management of Development, Test and Production Facilities		
Control Definition	The Agency shall define and manage the boundaries between its development, test and production environments for information systems		
Control Type	Preventive		
Control Specifications			
Specification #	Description	Applicability	
OM 3.1	The Agency should define the minimum, distinct levels of information security controls necessary for its development, test and production environments for information systems. Mechanisms should exist to prevent information security vulnerabilities from one environment carrying forward to the next. Such mechanisms may include: • Robust Change Management (see OM.3.2 below) • Network Access Control Lists (ACLs) restricting information flow between the environments • Isolating environments from each other where a security incident has occurred within one of them • Account segregation (where an individual needing access to more than one environment has a different account and different credentials for each environment)	Recommended	
OM 3.2	The movement of information assets and information systems from one environment to another should be controlled by the Agency's change management process. No movement between environments should occur without an approved Request For Change (RFC)	Mandatory	

OM 3.3	Access to information systems should be confined to the specific duties for which the individual has been authorised. Developers, testers, systems administrators and end users should not have access to information system types that are not required to undertake their specific duties e.g. developers should not typically have access to production information systems	Mandatory
OM 3.4	Data from one environment should not transit from that environment to another without specific and informed approval from the information owner (e.g. test data should typically not be migrated to production information systems)	Mandatory
OM 3.5	The configuration of test information systems should be in alignment with their production information system counterparts, to ensure that test results can be quantified against a known configuration baseline	Recommended
Control Dependencies	None	

NIA Policy Reference: Section C. Security Controls: 6. Software Security - Software Development & Acquisition

Reference Used:

- ISO 27002 Information technology - Security techniques - Code of practice for Information Security management:
 - 10.1.4 Separation of development, test, and operational facilities

Control #	Control Name	Impact Priority	High
OM 4.0	Monitoring of Information System and Network Performance and Usage		
Control Definition	The Agency shall establish procedures and tools for monitoring the performance and use of information systems and processing facilities		
Control Type	Detective		
Control Specifications			
Specification #	Description	Applicability	
OM 4.1	The Agency should ensure that information systems and networks are subject to on-going monitoring. Monitoring attributes may include (but not confined to) confirming: • Deviation from an information system performance baseline defined within the information security design	Mandatory	



	• Loading on the information system/network (in the context of available capacity) • Status of information security controls • Usage of information services by users • User and administrator account status (e.g. times of access, locations of access, dormant vs. active accounts) • Anomalous and suspicious events (including data access outside of the normal pattern of use). • Potential and actual attacks • Potential and actual malicious code distribution • Presence of known vulnerabilities • Status of security patches within the Agency's infrastructure • Configuration deviation from agreed baselines	
OM 4.2	The Agency should ensure that its monitoring data is protected from accidental or intentional corruption or deletion	Mandatory
OM 4.3	The Agency should ensure that its monitoring data is regularly analysed by qualified personnel, with prioritised and costed recommendations for corrective action and improvement being presented to the organisation's information security governance committee	Mandatory
Control Dependencies	None	

NIA Policy Reference: Section B. Security Governance & Security Processes: 10. Logging & Security Monitoring

Reference Used

- NIST Special Publication 800-53 Revision 3:
 - CA-7 Continuous Monitoring

6.2.2 Data Centre Security Controls (DCS)

Control #	Control Name	Impact Priority	High
DCS 1.0	Data Centre Security		
Control Definition	The Agency shall ensure that data centre facilities provide an adequate level of protection for the information assets stored and processed within them		
Control Type	Preventive , Detective		

Control Specifications		
Specification #	Description	Applicability
DCS 1.1	In addition to the other controls described in the physical security section of NIA policy document, the Agency should determine what specific, unique or enhanced controls are required to secure its data centre locations Where the Agency has outsourced information system, application or file hosting to an external, third-party provider, it should ensure that: • Its contractual terms specify the security controls that will be deployed in the data centre environment and the purpose they will serve • The Agency retains the right of audit to validate the continued presence and effectiveness of the contractually agreed controls • Sensitive information systems should be sited in dedicated (isolated) physical computing environment, demarcated from other computing environments. The level of access control to this area should be restricted to only those personnel with a verified need for access	Mandatory
DCS 1.2	Data centres should ideally not be housed in the same building as other offices, especially offices used by other, non-governmental organisations	Recommended
DCS 1.3	Security requirements should be explicitly mapped to the security service type that they correspond to. Security services types include: • Authentication • Access Control and Authorisation • Availability • Data Integrity At Rest • Data Integrity In Motion • Data Confidentiality At Rest • Data Confidentiality In Motion • Non Repudiation • Recoverability • Maintainability	Recommended



	Where the provider of the requirements does not have the experience necessary to make such a correlation, the Agency's CISO should analyse the requirements and propose a workable mapping of requirements to target security services	
DCS 1.4	Technical Vulnerability and Patch Management • Timely information about the technical vulnerabilities of information systems and networks shall be obtained, the Agency's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk • Firewalls, routers and other boundary devices should be prioritized for the application of patches and other vendor software updates, due to their exposure to public networks • The Agency should define the roles and responsibilities associated with technical vulnerability management, including: vulnerability monitoring, vulnerability risk assessment, information system/network device patching, asset tracking and any coordination activities required. • The Agency should ensure that resource planning allows for vulnerability assessment and patch management to be prioritized • Security performance metrics and associated reporting should confirm the average delta between when patches are released and when they are applied	Recommended
DCS 1.5	Network Boundary Defence (Firewalls, Gateways, Border Routers, DMZ) • The Agency should consider the deployment of anomaly detection and Multi-Verification Process (MVP) technologies to detect and limit the impact of Distributed Denial of Service (DDoS) attacks • Firewalls should be monitored by the Agency's Intrusion Detection and Prevention Services (IDPS), with the view to identifying if/when a firewall has been compromised	Recommended



	• Where software-based firewalls are used for boundary protection, the computing devices' operating system should be hardened and the firewall should be the only application permitted to run on the computing device • The Agency should consider blocking all encrypted traffic at the firewall unless the source and destination have been approved for secure communication. The Agency may consider an approach where data is de-encrypted at the firewall and then re-encrypted for onward transmission to the destination • Monitor wireless network traffic and analyze it to identify suspicious activity • Where the Agency plans to use multiple types of IDPS technology, or multiple products of the same IDPS technology type, consideration should be given as to whether the IDPS instances should be integrated • Integration may possibly be achieved through the deployment of a Security Information and Event Management (SIEM) solution	
DCS 1.6	Remote Access • Remote access gateways should only accept one connection per approved user account at any one time. • While connected to the Agency's core network via VPN, remote access users should not be authorized to connect to other networks, to avoid the potential for bridging between the networks • Scheduled maintenance activities on remote access solutions should include: deploying software updates, verifying clock synchronization, reconfiguring access control features as needed, and detecting and documenting anomalies within the remote access infrastructure	Recommended
Control Dependencies	None	

NIA Policy Reference: Section C. Security Controls: 12. Physical Security**References Used**

- ISO 27002 Information technology — Security techniques — Information Security management systems — Requirements: 12.6.1 Control of technical vulnerabilities
- NIST Special Publication 800- Revision 3: RA-5 Vulnerability Scanning
- NIST Special Publication 800-41 Revision 1: ES-1 Executive Summary
- SANS :: Critical Control 5: Boundary Defence
- NIST Special Publication 800-53 Revision 3: AC-18 Wireless Access
- NIST Special Publication 800-77 'Guide to IPsec VPNs'

6.3 Information Security Roles and Responsibilities

The successful implementation and progression of the NIA Standards is a shared responsibility among key stakeholders in an agency. The Cyber Security Department, within the Ministry of Transport and Communication has provided guidelines by publishing a RASCI Table for NIA Policy V2.0. This is to assist agencies in the adoption of NIA Policy.

The 'RASCI Table' helps to identify the Roles and Responsibilities of various Functions / departments in a typical agency, against the various domains identified in the NIA Policy. Agencies are requested to use their own discretion in mapping these out to their specific organization structure whilst using this tool.

RASCI table is a Responsibility assignment matrix where R=Responsible A=Accountable S=Supportive C=Consulted I=Informed.

Complying with the NIAP is an organization wide responsibility, with each department having their own specific roles and responsibilities. The objective of this matrix is to help in this task. The latest version of this RASCI matrix is published here:

http://www.qcert.org/sites/default/files/public/documents/cs_niap_rasci_table_eng_v1.0.pdf

7 Glossary

- **AC:** Audit & Certification
- **ACL:** Access Control Lists
- **ACRL:** Attribute Certificate Revocation Lists
- **AKA:** Authentication and Key Agreement
- **AM:** Access Control Security
- **AVL:** Authorization and Validation Lists
- **BC:** Business Continuity Management
- **BYOD:** Bring Your Own Device
- **CM:** Change Management
- **COTS:** Commercial Off-The-Shelf
- **CRL:** Certificate Revocation Lists
- **CS:** Communications Security
- **CSIO:** Chief Information Security Officer
- **CY:** Cryptographic Security
- **DC:** Documentation
- **DCS:** Data Centre Security Controls
- **DDoS:** Distributed Denial-of-Service
- **DL:** Data Labeling
- **DMZ:** Demilitarized Zone
- **DNS:** Domain Name System
- **DR:** Data Retention & Archival
- **EA:** Enterprise Architecture
- **EAP-SIM:** EAP-Subscriber Identity Module
- **EAP-TTLS:** EAP-Tunneled Transport Layer Security
- **EAP:** Extensible Authentication Protocol
- **ebXML:** Electronic Business XML
- **FIPS PUB:** Federal Information Processing Standard Publication
- **FTP:** File Transfer Protocol
- **GEA:** (Qatari) Government Enterprise Architecture
- **GS:** Gateway Security
- **GS:** Governance Structure
- **HSE:** Health, Safety and Environmental
- **HTTP:** Hypertext Transfer Protocol
- **IBM:** International Business Machines

- **ICS:** Industrial Control Systems
- **ICT:** Information Communication Technology
- **IDPS:** Intrusion Detection and Prevention Systems
- **IE:** Information Exchange
- **IEC:** International Electrotechnical Commission
- **IETF:** Internet Engineering Task Force
- **IM:** Incident Management
- **IoT:** Internet of Things
- **ISO:** International Organisation for Standardization
- **ISRMF:** (Qatar) Information Security Risk Management Framework
- **IT:** Information Technology
- **IVR:** Interactive Voice Response
- **JPEG:** Joint Photographic Experts Group
- **LAN:** Local Area Network
- **LEAP:** Lightweight Extensible Authentication Protocol
- **MoTC:** (Qatari) Ministry of Transport & Communication
- **MS:** Media Security
- **MVP:** Multi-Verification Process
- **NIA:** National Information Assurance
- **NIAP:** National Information Assurance Policy
- **NIST SP:** National Institute of Standards and Technology Special Publication
- **NS:** Network Security
- **OASIS:** Organization for the Advancement of Structured Information Standards
- **OAuth:** Open Authorization
- **OCSP:** Online Certificate Status Protocol
- **OM:** Operations Management
- **OS:** Portable Device & Working Off-Site Security
- **PDCA:** Plan-Do-Check-Act
- **PEAP:** Protected Extensible Authentication Protocol
- **PH:** Physical Security
- **PKCS:** Public Key Cryptography Standards
- **PKI:** Public Key Infrastructure
- **PMI:** Privilege Management Infrastructure
- **PR:** Product Security
- **PS:** Personnel Security

- **Q-CERT:** Qatar Computer Emergency Response Team
- **QeAF:** Qatar e-Authentication Framework
- **RASCI:** Responsible, Accountable, Supportive, Consulted and Informed
- **RFC:** Request For Change
- **RM:** Risk Management
- **SA:** Security Awareness
- **SAML:** Security Assertion Markup Language
- **SHS:** Secure Hash Standard
- **SIEM:** Security Information and Event Management
- **SM:** Logging, Auditing & Security Monitoring
- **SMTP:** Simple Mail Transfer Protocol
- **SOAP:** Simple Object Access Protocol
- **SPML:** Service Provisioning Markup Language
- **SQISS:** Smart Qatar Information Security Standard
- **SS:** Software Security
- **SSL:** Secure Sockets Layer
- **SSO:** Single-Sign-On
- **SU:** System Usage Security
- **TLS:** Transport Level Security
- **TM:** Third Party Security Management
- **TTLS:** Tunneled Transport Layer Security
- **VL:** Virtualization
- **VPN:** Virtual Private Network
- **W3C:** World Wide Web Consortium
- **WPA:** Wi-Fi Protected Access
- **WSDL:** Web Services Description Language
- **X-KISS:** XML Key Information Service Specification
- **X-KRSS:** XML Key Registration Service Specification
- **XACML:** eXtensible Access Control Markup Language
- **XHTML:** Extensible Hypertext Mark-up Language
- **XKMS:** XML Key Management Specification
- **XML:** Extensible Mark-up Language
- **XMLDSig:** XML Digital Signature
- **XMLEnc:** XML Encryption