

National Information Assurance Policy Ver 2.0 Control Types

The 'control cross check' spreadsheet characterises or classifies the controls recommended by NIAP according to types and objectives.

In this classification, controls are:

- Deterrent: the control reduces the threat, deterring hackers from attacking a given system for example.
- Avoidance: the control reduces the impact, or avoids the situation presenting a risk.
- Prevention: the control reduces the vulnerability: most security controls act in this way.
- Detection: the control helps identify an event or incident as soon as possible, generally triggering reactive measures.
- Reaction: the control helps minimise the impact of incidents by prompt reaction.
- Recovery: the control helps minimise the impact of incidents by aiding the restoration of normality, or at least a fallback service.

... while the objectives are primarily to ensure confidentiality, integrity or availability of information assets, often more than one.

Other classifications are possible. Furthermore, you may disagree with the particular classifications we have assigned to each control. However, we feel this is a valid and useful starting point for discussion.

Feel free to modify this as you wish.

One way to use the cross check spreadsheet is to identify any controls that you have chosen not to implement, documented in Statement of Exception, in other words those you have decided are not appropriate to your circumstances, in the spreadsheet.

Then look down the columns to check that you still have a reasonable mix of the types of control in the remaining control set.

You may also use this spreadsheet when deciding how to treat identified risks, choosing a balanced set of controls giving defence-in-depth.

Document Version: 1.1

Document Classification: Public

Release Date: June 2018

Author: Cyber Security Policy & Standards Section, Ministry of Transport and Communications

Document History

Version	Description	Date
1.0	Published V1.0 document	October 2016
1.1	MoTC Logo Changed	June 2018

National Information Assurance Policy V2.0 Controls Classification

Control	Type						Primary objective			
	Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability	
A	SECURITY GOVERNANCE & SECURITY PROCESSES									
1	Governance Structure [IG]									
IG 1	*Appoint a person to own and manage the Information Security programme. This person, will be referred to as the 'Security Manager' within this NIA Manual.	✓	✓	✓				✓	✓	✓
IG 2	*Allocate appropriate budget to staff and operate the Information Security Programme.	✓	✓					✓	✓	✓
IG 3	*Ensure the Security Manager has a reporting line to the Agency's risk or internal audit function.	✓	✓	✓				✓	✓	✓
IG 4	*Ensure that the Agency head provides documented and continuous support for the development, implementation and ongoing maintenance of ICT security processes and infrastructure within their Agency.	✓	✓	✓		✓		✓	✓	✓
IG 5	Where the Agency head delegates their authority to approve variations from requirements in this manual the delegate must have higher authority than the Security Manager.	✓	✓					✓	✓	
IG 6	Define information security responsibilities for the Security Manager, management, employees and/or outsourced/3rd party vendors, suppliers or contractors of the Agency.	✓	✓	✓				✓	✓	
IG 7	*Ensure the Security Manager has: a. ready access to, and full support from, executive management b. familiarity with information security and/or ICT security c. a general knowledge of, and experience in, or necessary resources in systems used by the Agency, especially operating systems, access & authorisation control systems/facilities and auditing facilities. d. a reasonable capacity and competence to support the Security Manager role.	✓	✓	✓				✓	✓	
IG 8	Include the following responsibilities within the Security Manager's role: a. identifying and recommending ICT security improvements to all business systems and business processes. b. ensuring ICT security aspects are considered as part of the change management process. c. ensuring the coordinating of development, maintenance and implementation of all ICT security documentation, in conjunction with the business managers. d. ensuring timely reporting and adequate participation in investigation for ICT security incidents, with Q-CERT.	✓	✓	✓	✓			✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
IG 9	Ensure the Security Manager is responsible for: a. ensuring the development, maintenance, updating and implementation of security risk management plans, system security plans and any security procedures used. b. providing technical security advice involved with system development, acquisition, implementation, modification, operation, support, and architecture c. assisting the system manager to develop system security standards/policies d. the certification of systems, when applicable e. ensuring the agency has an appropriate ICT security awareness and training program. f. the regular review of system security, system audit trails and logs and the integrity of system configurations.	✓	✓	✓	✓			✓	✓	✓
IG 10	Ensure the Security Manager is familiar with all security operating procedures relating to systems, including to the roles of system managers, system administrators and system users.	✓	✓	✓				✓	✓	✓
2	Risk Management [RM]									
RM 1	*Define a risk assessment process to identify threats and vulnerabilities to critical information assets (identified with an aggregate security level of Medium or High).	✓	✓	✓	✓			✓	✓	✓
RM 2	*Based on the assessment, define a risk treatment plan to address threats and vulnerabilities.					✓		✓	✓	✓
RM 3	Ensure that the risk treatment plan and residual risk selected for information assets, with an aggregate security level of High, are vetted by senior management in the Agency.		✓			✓		✓	✓	✓
RM 4	Ensure that the controls chosen in RM2 & RM3 are monitored for effectiveness on a periodic basis.		✓			✓		✓	✓	✓
RM 5	Risk assessments should be integrated within the business process and revised whenever there is a change. Changes in the business or legal/regulatory environment may also warrant the need to do risk assessment.	✓	✓	✓				✓	✓	✓
3	Third Party Security Management [TM]									
TM 1	*The areas or services being outsourced remain the governance, compliance and risk management accountability of the Agency.	✓	✓	✓				✓	✓	✓
TM 2	*They understand and acknowledge the risks associated with the outsourcing of their services.	✓	✓	✓				✓	✓	✓
TM 3	That the security controls and baseline policy specified in this NIA Manual are included in the third party service delivery agreement or contract. This SHALL also apply to sub-contractors used by the third party.	✓	✓	✓				✓	✓	✓
TM 4	The third party SHALL be contractually required to regularly report on the outsourced service'(s) security posture, including any incidents.				✓			✓	✓	✓
TM 5	The services, reports and records provided by the third party should be continuously monitored and reviewed, and audits should be conducted on defined periodic intervals.		✓	✓	✓			✓	✓	✓
4	Data Labelling [DL]									
DL 1	*Serve as a labelling authority for the data and information that it collects or maintains.	✓		✓	✓			✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
DL 2	*Rate all information assets in accordance with [IAP-NAT-DCLS]. All assets rated with a Confidentiality rating of C1, C2 or C3 SHALL be suitably marked the data label of Internal, Limited Access or Restricted respectively.		✓						✓	✓
DL 3	*By default, classify information assets as 'Internal' unless they are specifically for public release or consumption.	✓	✓	✓					✓	✓
DL 4	Establish the data labelling system to support the "Need-To-Know" requirement, so that information will be protected from unauthorized disclosure and use.	✓		✓	✓			✓	✓	✓
DL 5	Establish data labelling education and awareness for its staff, employees and contractors.	✓		✓	✓			✓	✓	✓
5	Change Management [CM]									
CM 1	*Define and adhere to a documented change management process which may include the following or similar change categories: a. Planned Major Change. Examples of planned major changes are: • 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 b. Maintenance and Minor Changes. Examples of this type of change are: • 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 c. Emergency and Unplanned Outage Changes. Examples of this type of change are: • 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	✓	✓	✓	✓			✓	✓	✓
CM 2	Establish a cross functional Change Management Committee which must include representation from security and risk divisions	✓	✓	✓				✓	✓	✓
CM 3	Document and Approve all proposed changes through the relevant Change Management Committee.	✓	✓	✓				✓	✓	✓
CM 4	*Ensure that upon implementing any proposed change that may impact the security of the ICT system assess whether the system will require re-certification. The system MUST comply with baseline requirements at minimum even after change implementation. Risk analysis may be required to ensure residual risk at acceptable level.	✓	✓	✓	✓			✓	✓	✓
CM 5	All associated system documentation is updated to reflect the change.	✓	✓	✓		✓	✓	✓	✓	✓
CM 6	Emergency changes may be carried out on the basis of a verbal/informed approval from the Change management committee Head and the Business process owner. However, post emergency, the standard procedure for documenting and risk analysis is to be applied.	✓	✓	✓				✓	✓	✓
6	Personnel Security [PS]									

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
PS 1	Ensure that the Human Resources (HR) processes are aligned with information security policies and initiatives of the organization.	✓	✓					✓	✓	✓
PS 2	*Ensure the HR department documents security requirements and obligations and ways of working in HR manual, which is read, understood and available to all staff to ensure they are aware and comply with their obligations to information security.	✓	✓					✓	✓	✓
PS 3	*Obtain, manage and retain information related to personnel with due care and due diligence, in line with the requirements for handling Personal Information as specified in the proposed information Privacy and Protection Law.			✓				✓	✓	✓
PS 4	Ensure information security responsibilities are included as part of the employees' job responsibilities and job descriptions and are applied throughout an individual's employment within the organization.	✓	✓					✓	✓	✓
PS 5	*Conduct adequate screening to ascertain the integrity of prospective candidates for employment and contractors (including sub-contracted workers). The Agency may further extend this exercise to existing employees as deemed necessary to satisfy conditions arising out of factors such as but not limited to "Change of employee responsibilities" or "Suspicion raised on the conduct of an employee".	✓	✓					✓	✓	✓
PS 6	*Ensure that staff sign an agreement, on joining the Agency or when there is a change in job profile or duties, which outlines their security obligations and responsibilities. This SHALL include: a. Confidentiality and non-disclosure obligations.	✓	✓					✓	✓	✓
PS 7	Ensure that adequate controls are in place to prevent personnel (employees, vendors, contractors and visitors) from making unauthorized disclosures, misusing or corrupting information as per Agency security policies.	✓	✓	✓				✓	✓	✓
PS 8	Ensure that users access rights are restrictive to the information they need to fulfill their job requirements as per least privilege and need to have principles.	✓	✓	✓				✓	✓	
PS 9	Implement a split of responsibilities over sensitive security processes and tasks, using the four eyes principles to ensure knowledge sharing and to avoid a single individual having full control over critical processes or tasks.	✓	✓	✓				✓	✓	✓
PS 10	*Define, communicate and enforce a disciplinary process and ensure that employees are made aware of the process. Disciplinary processes SHOULD be documented in the employee or HR manual.	✓	✓	✓	✓	✓	✓	✓	✓	✓
PS 11	*Ensure that vendors, contractors, delegates or guests visiting Agency premises are: a. Logged with unique identifiable information including date, time and purpose of admittance. b. Provided with a visitor badge or identification tag. c. Wearing a noticeable sign displaying their status as "visitor" at all times. d. Made aware of their obligations in complying with the security policies of the Agency. e. Escorted by Agency employees while accessing secure areas.	✓	✓	✓		✓		✓	✓	✓
PS 12	*Ensure that a change request from the HR department is generated when a change of duties or termination of contract of an employee, contractor or third party occurs. This ensures that employees, contractors and third parties return Agency assets and physical & logical access are amended/removed as appropriate.	✓	✓	✓				✓	✓	✓
7	Security Awareness [SA]									

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
SA 1	*A security awareness programme is defined and adequate budgets are allocated for its implementation.	✓	✓	✓	✓	✓		✓	✓	✓
SA 2	*As a minimum, such training includes a. Baseline requirements specified in this NIA Manual b. Agency's security requirements c. Legal and regulatory responsibilities d. Business specific processes and controls e. Acceptable use of information processing facilities, (e.g. log-on procedures, use of software packages, etc.) f. Information on the enforcement and disciplinary process g. Information on who to contact for further security advice and the proper channels for reporting information security incidents	✓	✓	✓	✓	✓		✓	✓	✓
SA 3	*All employees of the Agency and, where relevant, contractors and third party users receive appropriate security awareness training regarding the Agency's policies and procedures, as relevant for their job function, roles, responsibilities and skills.	✓	✓	✓	✓	✓		✓	✓	✓
SA 4	Employees should be trained to recognize social engineering attempts on them and not disclose any information that could violate the Agency's security policies, such as during social gatherings, public events and training events.	✓	✓	✓	✓	✓		✓	✓	✓
SA 5	Contents of the security training and awareness are reviewed and updated regularly to reflect new trends, new threats, and changes to the Agency's information technology infrastructure or applicable laws and regulations.	✓	✓	✓	✓	✓		✓	✓	✓
SA 6	New employees are provided information security awareness training as part of the employee induction process and refresher training must be conducted on periodic basis.	✓	✓	✓	✓	✓		✓	✓	✓
SA 7	Training is followed up with an assessment, to ascertain the effectiveness of the programme, including maintaining of records of attendance of security awareness programmes.	✓	✓	✓	✓	✓	✓	✓	✓	✓
SA 8	Indirect media such as posters, intranet, email, etc. may be used effectively to support the awareness programme.	✓	✓	✓				✓	✓	✓
8	Incident Management [IM]									
IM 1	*Appoint a person to own and manage the Incident Management programme, including a point of contact for all information security communications.				✓	✓	✓	✓	✓	✓
IM 2	Establish an information security incident response capability, based on the [IAP-NAT-DCLS] which is capable of making a periodic risk assessment (from threat, vulnerability and asset value) of data, processes, systems and networks in accordance with this Information Assurance Manual.					✓	✓	✓	✓	✓
IM 3	*Define procedures to detect, evaluate and respond to incidents.				✓	✓	✓	✓	✓	✓
IM 4	Define procedures to report, manage and recover from information security incidents, internally, with Q-CERT and with other Agencies.				✓	✓	✓	✓	✓	✓
IM 5	*Create awareness amongst its staff to report incidents.	✓			✓	✓	✓	✓	✓	✓
IM 6	Categorise and prioritize all incidents according to the incident criticality classification provided in Appendix C.					✓	✓	✓	✓	✓
IM 7	Co-ordinate with Q-CERT to create a repository of incidents in the Agency.					✓	✓	✓	✓	✓
IM 8	*Report all Criticality Level 1 incidents to Q-CERT within one (1) hour of identification.					✓	✓	✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
IM 9	The Incident Management coordinator is responsible for developing and executing an annual Security Assurance Plan. This may include activities such as penetration testing, audit of security procedures, and incident scenario testing.	✓	✓	✓	✓			✓	✓	✓
9	Business Continuity Management [BC]									
BC 1	*A person is appointed to own and manage the Business Continuity Programme.						✓			✓
BC 2	*A Business Continuity (BC) Plan is prepared to ensure continuance of critical processes and the delivery of essential services to an acceptable level. This plan SHALL include, and be based on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each Agency process.					✓	✓			✓
BC 3	The BC Plan covers disaster scenarios possible and adequate and includes disaster recovery provisions.						✓			✓
BC 4	*The BC Plan is maintained and updated to reflect the current status and requirements and relevant information is made available for all team members, employees and service providers.						✓			✓
BC 5	*The BC Plan is maintained and updated to reflect the current status and requirements and relevant information is made available for all team members, employees and service providers.					✓	✓			✓
BC 6	They identify alternate disaster recovery sites, whose readiness is determined by the RTO requirements. These sites may be Hot/Warm/Cold Sites depending upon the Agency's requirements.						✓			✓
BC 7	They specify strong controls in contracts that involve outsourcing a portion of their business or information technology functions or business continuity services.	✓	✓					✓		✓
BC 8	The BC Plan is periodically tested at least on an annual basis or when significant changes take place in the business or legal/regulatory requirements.					✓	✓			✓
BC 9	*Awareness about the BC plan is created amongst its employees.	✓	✓	✓						✓
10	Logging & Security Monitoring [SM]									
SM 1	*Adequate set of technical control implementations, or processes exist for logging, identification and continuous monitoring of access, changes, command execution to, any/ all information assets for protection of business sensitive information.	✓			✓	✓		✓	✓	✓
SM 2	*Monitoring practices are established in accordance with criticality of the infrastructure , data, and applications. It is RECOMMENDED to provide a 24/7 monitoring for C3, I3 and A3 classified infrastructures and ensure that monitoring responsibilities are allocated as specified in clause PS9, section B- 6, Personnel Security [PS].	✓			✓	✓		✓	✓	✓
SM 3	Monitoring activity is in line with regulatory and legal frameworks such as the proposed Information Privacy & Protection Law and SHALL cover use or access to systems.	✓	✓					✓	✓	✓
SM 4	*They enable logging on all infrastructure and data processing equipment, and applications that are associated with the access, transmission, processing, security, storage, and/or handing of information classified with a confidentiality rating of C2 and above.	✓			✓	✓		✓	✓	✓
SM 5	They classify all security logs with a confidentiality rating of C3, while application and system logs SHALL be classified in accordance with the confidentiality rating of the system.	✓	✓	✓				✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
SM 6	Logs containing Personal Information have appropriate privacy protection measures in place, in accordance with the Proposed Information Privacy & Protection Legislation.			✓				✓		
SM 7	*These logs are retained for a minimum of ninety (90) days and a maximum depending on criticality assessments and sector specific laws and regulations.	✓	✓	✓				✓	✓	✓
SM 8	Agency's MUST enable audit logging or log capture, to record date, time, authentication activity with unique user and system identifiers, including all failure or change actions, further including commands issued and output generated to provide enough information to permit reconstruction of incidents and move system to its original state.	✓			✓	✓		✓	✓	✓
SM 9	Exceptions are identified and reported in accordance with the Incident Handling policy, as defined in section B- 8, Incident Management [IM].	✓			✓	✓		✓	✓	✓
11	Data Retention & Archival [DR]									
DR 1	*They determine and document the retention periods of suitable information assets including but not limited to the critical information assets that they hold. Data retention periods SHALL, at a minimum, be governed by: a. Agency policies & needs b. Regulatory requirements c. Legal requirements			✓	✓	✓	✓	✓	✓	✓
DR 2	*Data, which needs to be retained, is stored ensuring confidentiality, integrity and availability and that it can be accessed for defined future purposes.			✓	✓	✓	✓	✓	✓	✓
DR 3	Personal and sensitive Information is not retained for longer than it is necessary as per the Proposed Information Privacy & Protection Legislation.			✓				✓		
DR 4	Processes for backup, archival and recovery of data have corresponding procedures which ensure that the integrity and confidentiality of the data is retained.		✓	✓			✓		✓	✓
DR 5	*Archived data retains its classification markings and is secured accordingly.		✓	✓			✓		✓	✓
DR 6	The archiving technology deployed is regularly reviewed to ensure that it does not suffer from obsolescence and archived data is maintained in a state that allows successful recovery.		✓	✓			✓		✓	✓
12	Documentation [DC]									
DC 1	*Produce a Agency security policy, incorporating the requirements of this NIA Manual.	✓	✓	✓		✓	✓	✓	✓	✓
DC 2	Ensure that every system that is determined to be critical to the Agency is covered by a system security plan/standard. Agencies SHOULD ensure that, where necessary, security operating procedures are created and documented.		✓	✓		✓	✓	✓	✓	✓
DC 3	Ensure system security standards and procedures are aligned and consistent with the Agency's security policies and objectives.	✓	✓	✓		✓	✓	✓	✓	✓
DC 4	*By default, classify ICT security documentation as a minimum of C3/RESTRICTED		✓						✓	✓
DC 5	*Review and update documentation periodically to ensure that they are up to date and current.		✓	✓		✓	✓	✓	✓	✓
13	Audit & Certification [AC]									

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
AC 1	*Ensure the establishment of a governance and security improvement programme in compliance with the National Information Classification Policy [IAP-NAT-DCLS] and this NIA Manual.	✓	✓					✓	✓	✓
AC 2	*Comply with relevant provisions of State Laws and regulations that exist at the time and those, which may be amended and / or added at a later date in time.	✓	✓					✓	✓	✓
AC 3	*Be audited by the Certification Body or an independent body designated by MICT.		✓	✓		✓	✓	✓	✓	✓
AC 4	*Ensure that an audit of its Information System (infrastructure, people and processes) is carried out at least once every year or whenever it undergoes a change that may impact the security of the Agency.		✓	✓		✓	✓	✓	✓	✓
AC 5	*Ensure that the identified scope of the audit process includes all information assets, people and processes.	✓								✓
AC 6	*Ensure that recertification is carried out where any change or new finding invalidates or calls into question the current accreditation. Full certification is required for major changes affecting the basic security design of a system and a partial process is needed where the change is moderate or affects two or more security requirements.	✓	✓	✓				✓	✓	✓
B	SECURITY CONTROLS									
1	Communications Security [CS]									
Cabling										
CS 1	Conduits (tubes, ducts or pipes) are used to protect cables from tampering, sabotage or accidental damage, when they are carrying data classified at C4 and above. This control is RECOMMENDED for data classified at C2 and above.			✓				✓		✓
CS 2	*Separate cabling distribution is used for systems dealing with information classified at C4 and above	✓		✓				✓		✓
CS 3	Conduits installed in public or visitor areas are not labelled in a manner that attract undue attention by people who may not have the appropriate security clearances or a need-to-know of the existence of such cabling			✓				✓		✓
CS 4	*They maintain a register of cables. The register SHOULD record at least the following: a. cable identification number, b. classification, c. source, d. destination, and e. floor plan diagram.		✓	✓				✓	✓	✓
CS 5	*Inspect cables for inconsistencies with the cable register on a regular basis	✓		✓						✓
CS 6	Agency's MAY provision for redundant communication pathways to ensure continued connectivity.		✓	✓		✓	✓			✓
Telephones & Faxes										
CS 7	Advise users of the maximum permitted classification level for conversations of both internal and external telephone connections, as determined by the examination of the internal telephone system and the level of the encryption, if any, on external connections		✓	✓				✓	✓	✓
CS 8	*Ensure that the speakerphone feature is disabled during telephonic/video conversations where information classified at C3 or above is likely to be discussed and where it may be overheard.			✓				✓		

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
CS 9	*Ensure that remote initiation of conferencing equipment is not enabled where it is installed in a sensitive location.		✓	✓				✓		
CS 10	*Ensure that rooms designated for communication of sensitive material or information or meetings have appropriate controls for preventing the leakage of sound.	✓		✓				✓		
CS 11	*Ensure that fax machines on both ends are secured using encryption devices, while sending information classified as C2 and above.			✓				✓	✓	
CS 12	Ensure that all of the standards for the use of fax machines are met at both ends for the level of classification to be sent, and the sender makes arrangements for the receiver to: a. collect the information from the fax machine as soon as possible after it is received, and b. notify the sender if the fax does not arrive within an agreed amount of time, e.g. 10 minutes.			✓				✓		
2	Network Security [NS]									
Network Management										
NS 1	*Details of internal network and system configuration, employee or device related directory services and other sensitive technology are not publicly disclosed or enumerable by unauthorized personnel.	✓	✓	✓				✓	✓	
NS 2	They remove or disable all the default accounts e.g. root, administrator, etc. or change the password as specified in section C-6, Software Security [SS].	✓	✓	✓				✓	✓	
NS 3	Network configuration is kept under the control of the network manager or similar and all changes to the configurations are: a. approved through a formal change control process as defined in section B- 5, Change Management [CM] b. documented, and comply with the network security policy and security plan as defined in section B- 12, Documentation [DC]. c. regularly reviewed. Old configurations as mandated by the Agency's procedures are maintained as part of change revision. The frequency of reviewing configuration shall depend on the Agency risk and processes.	✓	✓	✓				✓	✓	✓
NS 4	*For each managed network the Agency has: a. a high level diagram showing all connections into the network, and b. a logical network diagram showing all network devices. c. processes to update NS4 (a) & (b), as network changes occur d. include a "Current at <date>" label on each page.	✓		✓					✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
NS 5	*Networks are designed and configured to limit opportunities of unauthorized access to information transiting the network infrastructure. Agencies SHOULD use the following technologies to meet this requirement: a. switches instead of hubs, b. port security on switches to limit access and disable all unused ports c. routers and firewalls segregating parts of the network on a need-to-know basis, d. IPSEC/IP Version 6 e. application-level encryption f. an automated tool that compares the running configuration of network devices against the documented configuration g. network edge authentication h. Restrict and manage end-user devices communicating to Agency network through techniques such as MAC address filtering. i. IPS/IDS to detect/prevent malicious activity within the network j. Time and day restriction.		✓	✓	✓	✓		✓	✓	✓
NS 6	*Management networks adopt the following protection measures: a. dedicated network are used for management devices, i.e. implement a separate management VLAN, or physically separate infrastructure, b. secure channels e.g. by using VPNs, SSH, etc.	✓		✓				✓	✓	
Virtual LANs (VLANs)										
NS 7	VLANs are used to separate IP telephone traffic, in business critical networks.	✓		✓				✓	✓	
NS 8	*Administrative access is only permitted from the most highly classified VLAN to one at the same level of classification or of lower classification.		✓	✓				✓	✓	
NS 9	*They implement all security measures recommended by the agency's risk assessment and the hardening guidelines by the vendor of the switch.		✓	✓	✓			✓	✓	✓
NS 10	*Trunking/port mirroring SHALL not be used on switches managing VLANs of differing classifications.	✓		✓				✓	✓	
Multifunction Devices (MFDs)										
NS 11	*Network-connected MFDs are not used to copy documents classified above the level of the connected network	✓		✓				✓	✓	
NS 12	Where network-connected MFDs have the ability to transmit information via a gateway to another network, agencies MUST ensure that: a. each MFD applies user identification, authentication and audit functions for all information transmitted by users from that MFD, b. these mechanisms are of similar strength to those required for workstations on that network, and c. *the gateway can identify and filter the information in accordance with the requirements for the export of data.	✓		✓				✓	✓	

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
NS 13	*There is no direct connection from an MFD to a telephone network of a lower classification unless the MFD has been evaluated, and the scope of the evaluation includes: a. information flow control functions to prevent unintended and unauthorized data flows, b. data export controls capable of blocking information based on information classification, c. authentication, and audit data generation and protection	✓		✓				✓	✓	
NS 14	They deploy MFDs after developing a set of policies, plans and procedures governing the use of the equipment.	✓	✓	✓				✓	✓	✓
NS 15	Information classified at C1 or above is not retained permanently in the MFD. Where the MFD has features to schedule jobs, sufficient manual/automatic controls or configurations SHALL exist to remove the information from its memory once the job is complete.	✓		✓				✓	✓	✓
NS 16	MFDs follow the procedures specified in section C, 8.3, Media Sanitization.	✓	✓	✓				✓	✓	
Domain Name Service (DNS) Servers										
NS 17	A separate internal DNS server is set up and placed in the internal network for internal domain information that is not disclosed to the Internet.	✓		✓				✓	✓	
NS 18	DNS information that should be made public either has a locally hosted and secured (bastion server) server. State Agencies may also use the Government DNS which is part of the Government Network as the Primary DNS.	✓	✓					✓	✓	
NS 19	DNS servers are deployed to ensure there is no single points of failure in their service, they are security-hardened and security is proactively maintained.		✓	✓				✓	✓	✓
NS 20	*Zones files are digitally signed, and cryptographic mutual authentication and data integrity of zone transfers and dynamic updates is provided.		✓	✓	✓	✓		✓	✓	✓
NS 21	*Cryptographic origin authentication and integrity assurance of DNS data is provided.	✓	✓					✓	✓	✓
NS 22	DNS services including zone transfers are provided to authorized users only.		✓	✓				✓		✓
NS 23	*Cryptographic functions related to NS 20 and NS 21 above, use a hardware security module for both key management and cryptographic processing as specified in section C- 10, Cryptographic Security [CY].	✓	✓					✓	✓	
Internet Security										
NS 24	All software and files downloaded from the Internet are screened and verified against malicious software, including mechanisms to scan HTTP traffic.	✓		✓	✓	✓	✓	✓	✓	✓
NS 25	*The Internet gateway denies all Internet services unless specifically enabled.	✓	✓					✓		✓
NS 26	Web browsers running on user's workstation are properly configured and updated. Agencies SHOULD reference the following guidelines when configuring web browsers: a. Disable any active content options, e.g. Java, JavaScript and ActiveX, in the email application/ browser, except when communicating with a trusted source b. Use up-to-date browser versions and apply latest security patches c. Disable password auto-complete/password remembering features d. Enable pop-up blocking features, except when communicating with trusted sites e. Regularly remove cache files or temporary files of the browsers to protect data privacy f. Disable automatic installation of plug-ins, add-ons or software	✓	✓	✓				✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
NS 27	*They have the capability needed to monitor the traffic, deduce traffic patterns, usage etc. See section B- 10, Logging & Security Monitoring [SM] for more information.	✓	✓	✓	✓			✓	✓	✓
E-Mail Security										
NS 28	E-mail servers are hardened as per best practices and configured as a bastion server. If technically and operationally feasible, information revealing the specific details of internal systems or configurations MUST be avoided in email headers to avoid the disclosure of system information to external parties.		✓	✓				✓	✓	✓
NS 29	TLS protection is used with the SMTP Mail server in line with section C-10, Cryptographic Security [CY].	✓	✓		✓			✓	✓	
NS 30	*They implement the email Sender Policy Framework (SPF) [RFC4408]. Agencies SHOULD only send undeliverable or bounce emails to senders that can be verified via SPF.	✓	✓					✓	✓	✓
NS 31	*Internal email distribution lists are secured to prevent access from external parties to reduce the risk of unsolicited email.	✓	✓	✓				✓	✓	✓
NS 32	Email gateways are employed to scan all incoming and outgoing emails to ensure it complies with the Agency's security policy and that it is free of any malicious code.	✓		✓	✓				✓	✓
Wireless Security										
NS 33	*Where wireless LANs (WLANs) are used, they are used with sufficient authentication and transmission encryption measures in place, complemented by proper security management processes and practices.			✓	✓	✓		✓	✓	✓
NS 34	*Strong wireless security protocols such as WPA2 and EAP-TLS are used. However, such wireless security protocol should not be solely relied upon to protect data confidentiality and integrity. Agency SHALL deploy dynamic key exchange mechanisms, secure Virtual Private Network (VPN) on top of wireless network if classified data, C3 and above, is to be communicated over wireless networks. WEP SHALL NOT be implemented within any network.			✓	✓	✓		✓	✓	✓
NS 35	*A good inventory of all devices with wireless interface cards is maintained. Once a device is reported missing, consider modifying the encryption keys and SSID.		✓	✓		✓		✓	✓	✓
NS 36	*Network administrators regularly scan for "rouge" or "unauthorized" wireless access points.				✓	✓		✓	✓	✓
NS 37	Access points are located to minimize network tapping from publicly accessible area.	✓	✓	✓				✓	✓	✓
NS 38	The client side settings for 802.1x MUST be secured. Some of the techniques are: server certificate validation by selecting the CA certificate, specify the server address and disable it from prompting users to trust new certificates or servers.	✓	✓	✓				✓		
NS 39	*The network default name, encryption keys and Simple Network Management Protocol (SNMP) community strings (and any insecure configuration) is changed at installation. SSID SHALL NOT reflect the name of any Agency's departments, system name or product name.	✓	✓					✓		
NS 40	For non-public wireless access points, encryption keys are regularly changed and SSID broadcasting is disabled. Where applicable MAC address filtering SHOULD also be considered.	✓	✓		✓			✓		
NS 41	*A firewall or router is in place between the access point and the Agency's network to filter connections. Restricted firewall rules MUST be applied to allow only needed ports to pass from the wireless segment.	✓	✓	✓	✓	✓		✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
NS 42	WIPS/WIDS installation is recommended for networks with C3+ to monitor threats from wireless installations like rouge Aps, DOS attacks, etc.			✓	✓	✓		✓	✓	✓
NS 43	Use multiple SSIDs with different configurations for different VLANs, client authentication methods, etc. For example, contract staff or guest may use a different WIFI connections. Guest WIFI may have lower security and may only allow for connecting to the internet.	✓	✓	✓				✓		✓
Clock Synchronization										
NS 44	NTP servers MUST be secured as per best practices.		✓	✓	✓				✓	
NS 45	*Where a computer or communications device has the capability to operate a real-time clock, it shall be set to an agreed standard, e.g., Universal Coordinated Time (UTC) or local standard time. As some clocks are known to drift with time, there shall be a procedure that checks for and corrects any significant variation.		✓	✓	✓				✓	
NS 46	State Agency's MAY use the authorized Qatari Government time server (a part of the Government Network) as the primary NTP server.		✓	✓	✓				✓	
NS 47	All servers and network devices are synchronized with the local Agency NTP server which is synchronized as specified in NS45 and NS46.		✓	✓	✓				✓	
Virtual Private Networks (VPNs)										
NS 48	VPNs carrying classified data at C3 or above, SHALL authenticate using two-factor authentication : • first one a one-time password authentication such as a token device or a public/private key system with a strong passphrase • Second username and password using external authentication server (LDAP,Radius , TACACS .etc.)	✓	✓	✓				✓	✓	
NS 49	VPNs disconnect automatically from Agency's network after a pre-defined period of inactivity. The user SHALL be required to logon again to reconnect to the network.	✓	✓	✓				✓	✓	
NS 50	*Dual (split) tunneling is not permitted unless suitable controls are in place. Agencies SHOULD only permit one network connection at a time.	✓	✓	✓				✓	✓	
NS 51	All computers connected to a Agency's networks via VPN are equipped with personal security software, latest security patches, anti-virus software and malicious code detection and repair software. This security software SHALL be activated at all time and with the latest virus signatures and malicious code definitions.	✓	✓	✓	✓	✓	✓	✓	✓	✓
NS 52	Gateway-level firewalls are installed to control network traffic from VPN clients to authorized information systems or servers.			✓				✓	✓	✓
Voice over IP Security (VoIP)										
NS 53	Voice and data are separate networks. The separation SHOULD be physical, but use of Virtual LANS is permitted. The voice gateway, which interfaces with the PSTN segregates H.323, SIP, or other VoIP protocols from the data network.	✓		✓				✓	✓	
NS 54	VoIP capable gateways and other appropriate security mechanisms are employed.		✓	✓	✓			✓	✓	✓
NS 55	*They evaluate and use security enabled protocols such as Secure Real Time Protocol (SRTP) and disable unnecessary voice protocols.	✓	✓	✓	✓			✓	✓	
NS 56	*Proper physical counter measures are in place to protect the VoIP infrastructure.	✓	✓	✓	✓			✓	✓	✓
NS 57	*Adequate call log monitoring is implemented.		✓		✓			✓	✓	
NS 58	*Soft-phones, if permitted are through a secure connection. e.g. secure VPN.		✓	✓				✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
NS 59	Backup power is provided to POE VoIP phone devices in case of failure of power.	✓	✓	✓						✓
NS 60	Strong authentication and access controls are implemented to protect the voice gateway system.	✓	✓	✓				✓	✓	
NS 61	IPSEC or Secure Shell (SSH) is used for all remote management and auditing access.	✓	✓	✓				✓	✓	
NS 62	Contingency plans for making voice calls are developed if VoIP systems become unavailable.					✓	✓			✓
NS 63	*Port security features are enabled on the network LAN switches that connect VoIP devices.	✓	✓	✓				✓	✓	
Internet Protocol Version 6										
NS 64	*A proper risk assessment is conducted by the Agency to assess the security merits and demerits of IPv4 and IPv6 technology. Agencies SHOULD start considering IPv6 deployment.	✓	✓		✓	✓		✓	✓	✓
NS 65	A proper risk assessment is conducted if the Agency decided to implement a dual-stack environment.	✓	✓		✓	✓		✓	✓	✓
NS 66	Recertification is requested where Agencies deploy IPv6 in their network.		✓	✓				✓	✓	
3. Information Exchange [IE]										
IE1	Prior to establishing cross-domain connectivity, the Agency evaluates, understands and accepts the structure, security and risks of other domains. This risk review SHALL be documented for compliance requirements.		✓	✓				✓	✓	✓
IE2	*When intending to connect an agency network to another secured network, they: a. obtain a list of networks to which the other network is connected from the other network's Accreditation, Authority and System Manager, b. examine the information from both sources to determine if any unintended cascaded connections exist, and c. consider the risks associated with any identified cascaded connections prior to connecting the agency network to the other network, particularly where a connection to an un-trusted network such as the internet may exist.	✓	✓	✓	✓			✓	✓	✓
IE3	Ensure that necessary agreements (specifically confidentiality agreements) between the entities exchanging information have been established prior to information exchange. Agreements SHALL provide information on responsibilities, information exchange notification procedure, technical standards for transmission, identification of couriers, liabilities, ownership and controls. For vendors and 3rd parties a formal Non-Disclosure Agreement (NDA) SHALL be used. Appendix D provides a NDA template.		✓	✓				✓		
IE4	Ensure media which is used to exchange information is protected against unauthorized access, manipulation or misuse within or outside the Agency environment.	✓	✓	✓				✓	✓	
IE5	Maintain the classification and protection of information that has been obtained from another Agency.	✓	✓					✓	✓	✓
IE6	Maintain appropriate levels of physical protection for media in transit and store in packaging that protects it against any hazard that would render the content unreadable.		✓	✓				✓	✓	✓
IE7	*Ensure only reliable and trusted courier service or transport organization SHALL be used based on a list of known and authorized couriers.		✓	✓				✓	✓	✓
IE8	*Protect information exchanged via electronic messaging from unauthorized access, change or interruption of service.	✓		✓				✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
IE9	Ensure secure messaging (information is digitally signed and/or encrypted) is used for all information classified at C3 or above. Agencies SHALL use Secure Multipurpose Internet Mail Extension (S/MIME), equivalent or better protocol for secure messaging as specified in clause CY5, section C- 10, Cryptographic Security [CY].	✓	✓	✓				✓	✓	
IE10	*Attach the following email disclaimer, or similar, to all outgoing email: "The information in this email, including attachments, may contain information that is confidential, protected by intellectual property rights, or may be legally privileged. It is intended solely for the addressee(s). Access to this email by anyone else is unauthorized. Any use, disclosure, copying, or distribution of this email by persons other than the designated addressee is prohibited. If you are not the intended recipient, you should delete this message immediately from your system. If you believe that you have received this email in error, please contact the sender or < Agency's name & contact information>. Any views expressed in this email or its attachments are those of the individual sender except where the sender, expressly and with authority, states them to be the views of < Agency>."		✓	✓				✓		
IE11	Exercise due diligence to ensure that any information sent/received is free of viruses, trojans and other malicious code	✓		✓	✓			✓	✓	✓
IE12	Ensure information exchanged between systems is secured against misuse, unauthorized access or data corruption. For transmitting information classified at C2, I2 or above, authenticated and encrypted channels SHALL be used as specified in CY5, section C- 10, Cryptographic Security [CY].	✓		✓				✓	✓	✓
IE13	*Limit the information provided to the general public (via media outlets), to sanitized and approved information, through a designated and trained media relation spokesperson.	✓	✓	✓				✓		
Gateway Security [GS]										
GS 1	Networks are protected from other networks by gateways and data flows are properly controlled	✓		✓				✓	✓	✓
GS 2	Gateways connecting Agency networks to other Agency networks, or to uncontrolled public networks, are implemented: a. with an appropriate network device to control data flow b. with all data flows appropriately controlled c. with gateway components physically located within an appropriately secured server room.	✓	✓	✓				✓	✓	
GS 3	Only authorized and trained staff manage and maintain gateways	✓	✓	✓				✓	✓	
GS 4	*Administrative or management access to gateways processing or transmitting information classified at C3 or above is only provided based on dual control and the four eyes principles.	✓	✓	✓				✓	✓	
GS 5	Information exchanged through gateways is labelled as per the National Information Classification policy [IAP-NAT-DCLS] and protected as specified in this document. Gateways SHALL be classified inline with the information they are transmitting.	✓	✓	✓				✓	✓	✓
GS 6	Demilitarized zones (DMZs) are used to separate externally accessible systems from uncontrolled public networks and internal networks via usage of firewalls and other network security capable equipment	✓		✓				✓	✓	

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
GS 7	Gateways: a. are the only communications paths into and out of internal networks b. by default, deny all connections into and out of the network c. allow only explicitly authorised connections d. are managed via a secure path isolated from all connected networks e. provide sufficient audit capability to detect gateway security breaches and attempted network intrusions f. provide real-time alarms.	✓	✓	✓	✓			✓	✓	✓
GS 8	*Gateways are hardened prior to any implementation on production site and are protected against: a. Malicious code and vulnerabilities b. Wrong or poor configurations c. Account compromise and privilege escalation d. Rogue network monitoring e. Denial of service (DoS) attacks f. Information/data leakage	✓	✓	✓	✓			✓	✓	✓
GS 9	*Monitoring and supervision of gateways is in place and include threat prevention mechanisms, logging, alerts and surveillance of equipments. Section B- 10, Logging & Security Monitoring [SM].	✓		✓	✓	✓		✓	✓	✓
GS 10	Gateways block or drop any data identified by a content filter as suspicious, including at least the following: a. *Offensive language or attachments b. Malware infected content c. DoS attacks d. *Categories of website/content defined as inappropriate in the proposed Cyber Crime Law including sites hosting obscene material, gambling sites, etc.				✓	✓		✓		✓
Data Export										
GS 11	System users: a. are held accountable for the data they export b. are instructed to perform a protective marking check, a visual inspection and a metadata check if relevant whether the information can be exported		✓	✓	✓	✓		✓	✓	
GS 12	Data exports are either: a. performed in accordance with processes and/or procedures approved by the Agency; or b. individually approved by the information security manager.	✓	✓	✓				✓	✓	✓
GS 13	*Export of data to a less classified system is restricted by filtering data using at least checks on classification labels.			✓	✓			✓	✓	
GS 14	*Data exports are checked, ensuring: a. keyword searches are performed on all textual data b. any unidentified data is quarantined until reviewed and approved for release by a trusted source other than the originator.			✓	✓	✓		✓	✓	
GS 15	System users: a. are held accountable for the data they import b. are instructed to perform a protective marking check, a visual inspection and a metadata check if relevant.	✓			✓			✓	✓	
GS 16	*Data imports are either: a. performed in accordance with processes and/or procedures approved by the Agency; or b. individually approved by the information security manager.	✓	✓					✓	✓	✓
GS 17	*Data imported to a Agency system is scanned for malicious and active content.			✓	✓	✓		✓	✓	

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
5. Product Security [PR]										
PR 1	The process for product selection is carried out with due diligence and ensures product and vendor independence.	✓	✓	✓				✓	✓	✓
PR 2	Products are classified and labeled as per National Information Classification policy [IAP-NATDCLS].		✓					✓	✓	✓
PR 3	*The selection process includes proper identification of vendor, screening of vendors and evaluation criteria definition which should include as a minimum: a. Vendor status and identification, including location and ownership b. Financial situation c. References from previous successful engagements d. The ability of the vendor to build and/or maintain appropriate controls as determined by a risk assessment	✓	✓		✓			✓	✓	✓
PR 4	Proper testing and effective matching between vendor's claim and functionality is carried out, to avoid loss of confidentiality, integrity and/or availability.		✓	✓	✓			✓	✓	✓
PR 5	*Security evaluation of the product is done on a dedicated evaluation configuration including functionality tests, security tests and patching to protect against potential threats and vulnerabilities.		✓	✓					✓	
PR 6	Delivery of products is consistent with the Agency's security practice for secure delivery.	✓	✓					✓	✓	✓
PR 7	Secure delivery procedures SHALL include measures to detect tampering or masquerading.			✓	✓			✓	✓	✓
PR 8	*Products have been purchased from developers that have made a commitment to the ongoing maintenance of the assurance of their product.	✓	✓	✓				✓	✓	✓
PR 9	Product patching and updating processes are in place. Updates to of products SHALL follow the change management policies specified in section B- 5, Change Management [CM].	✓	✓					✓	✓	✓
6. Software Security [SS]										
Software Development & Acquisition										
SS 1	Security is considered in all phases of the SDLC and that it is an integral part of all system development or implementation project.	✓	✓	✓				✓	✓	✓
SS 2	*All applications (including new and developed) are classified using the National Information Classification Policy [IAP-NAT-DCLS] and accorded security protection appropriate to its Confidentiality, Integrity and Availability ratings.		✓					✓	✓	✓
SS 3	Security requirements (functional, technical and assurance requirements) are developed and implemented as part of system requirements.		✓	✓				✓	✓	
SS 4	*Dedicated test and development infrastructure (systems and data) are available and is separate from production systems. Furthermore, information flow between the environments SHALL be strictly limited according to a defined and documented policy, with access granted only to system users with a clear business requirement and write access to the authoritative source for the software SHALL be disabled.		✓	✓				✓	✓	
SS 5	All applications (acquired and/or developed) are available for production use only after appropriate quality and security assurance tests and checks to ensure that the system confirms and complies with the intended security requirements.		✓	✓	✓				✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
SS 6	*Software developers use secure programming practices when writing code, including: a. complying with best practices, for example the Mitre top 25 most dangerous programming errors [Mitre] b. designing software to use the lowest privilege level needed to achieve its task c. denying access by default d. checking return values of all system calls e. validating all inputs.		✓	✓	✓			✓	✓	✓
SS 7	Software should be reviewed and/or tested for vulnerabilities before it is used in a production environment. Software SHOULD be reviewed and/or tested by an independent party and not by the developer.		✓	✓					✓	
SS 8	System (acquired and/or developed) complies with all legal requirements including license, copyrights, IPR etc.	✓	✓					✓	✓	✓
SS 9	All systems (acquired and/or developed) are adequately documented.	✓	✓	✓		✓	✓	✓	✓	✓
SS 10	*Source code of custom developed critical applications is available and in the case of commercial applications (serving critical applications / processes) a Agency SHOULD look into options of arranging an escrow for the source code.	✓	✓	✓		✓			✓	
SS 11	Prior to commissioning of applications, they are certified as specified in section B- 13, Audit & Certification [AC].	✓	✓					✓	✓	
Software Applications										
SS 12	All server and workstation security objectives and mechanisms are documented in the relevant system security plan.	✓	✓			✓	✓	✓	✓	✓
SS 13	*Workstations use a hardened standard operating environment (SOE) covering: a. removal of unwanted software b. disabling of unused or undesired functionality in installed software and operating systems c. implementation of access controls on relevant objects to limit system users and programs to the minimum access needed to perform their duties d. installation of software-based firewalls limiting inbound and outbound network connections e. configuration of either remote logging or the transfer of local event logs to a central server.	✓	✓	✓	✓			✓	✓	✓
SS 14	*Potential vulnerabilities in their SOEs and systems are reduced by: a. removing unnecessary file shares b. ensuring patching is up to date c. disabling access to all unnecessary input/output functionality. d. removing unused accounts e. renaming default accounts f. replacing default passwords.	✓	✓	✓				✓	✓	✓
SS 15	High risk servers e.g. Web, email, file and Internet Protocol telephony servers, etc. having connectivity to uncontrolled public networks: a. maintain effective functional separation between servers allowing them to operate independently b. minimise communications between servers at both the network and file system level, as appropriate c. limit system users and programs to the minimum access needed to perform their duties.	✓	✓	✓				✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
SS 16	Check the integrity of all servers whose functions are critical to the Agency, and those identified as being at a high risk of compromise. Wherever possible these checks SHOULD be performed from a trusted environment rather than the system itself.	✓	✓						✓	
SS 17	Store the integrity information securely off the server in a manner that maintains integrity	✓	✓						✓	
SS 18	Update the integrity information after every legitimate change to a system		✓						✓	
SS 19	*As part of the Agency's ongoing audit schedule, compare the stored integrity information against current integrity information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred				✓				✓	
SS 20	Resolve any detected changes in accordance with the Agency's information and communications technology (ICT) security incident management procedures.					✓	✓		✓	
SS 21	*All software applications are reviewed to determine whether they attempt to establish any external connections. If automated outbound connection functionality is included, Agencies SHOULD make a business decision to determine whether to permit or deny these connections, including an assessment of the risks involved in doing so.			✓	✓	✓		✓	✓	
Web Applications										
SS 22	*All active content on their Web servers is reviewed for security issues. Agencies SHOULD follow the documentation provided in the Open Web Application Security Project (OWASP) guide to building secure Web applications and Web services.	✓	✓		✓			✓	✓	
SS 23	Connectivity and access between each Web application component is minimised.	✓		✓				✓	✓	
SS 24	That Personal Information and sensitive data is protected whilst in storage and in transmission using appropriate cryptographic controls	✓		✓				✓	✓	
SS 25	Critical sector websites that need to be strongly authenticated, use SSL certificates provided from a Certificate Service Provider (CSP) licensed in the State of Qatar.	✓	✓	✓				✓	✓	
SS 26	Web application firewall (WAF) MUST be used for applications with MEDIUM or higher risk rating.	✓		✓	✓	✓		✓	✓	✓
Databases										
SS 27	All information stored within a database is associated with an appropriate classification if the information: a. could be exported to a different system, or b. contains differing classifications and/or different handling requirements.	✓						✓	✓	✓
SS 28	Agencies should ensure that classifications are applied with a level of granularity sufficient to clearly define the handling requirements for any information retrieved or exported from a database.		✓					✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
SS 29	*Database files are protected from access that bypasses the database's normal access controls.			✓				✓		
SS 30	Databases provide functionality to allow for auditing of system users' actions.	✓	✓	✓				✓	✓	✓
SS 31	*System users who do not have sufficient privilege to view database contents cannot see associated metadata in a list of results from a search engine query. If results from database queries cannot be appropriately filtered, agencies MUST ensure that all query results are appropriately sanitized to meet the minimum-security privilege of system users.	✓	✓					✓	✓	
SS 32	Sensitive data in database shall be masked using data masking technology for C3 & above.	✓		✓				✓	✓	✓
7. System Usage Security [SU]										
SU 1	System users SHALL be responsible for the information assets (systems / infrastructure) provided to them to carry out their official responsibilities. They SHALL handle the information assets with due care and operate them in line with the vendor / Agency's Acceptable usage policy.		✓	✓	✓	✓	✓	✓	✓	✓
SU 2	System users will conduct due diligence when accessing the web and browsing the web SHALL strictly follow Agency principles and guidelines on accessing the internet. Agencies SHOULD consider whether usage of forums, social networks, etc is permitted or not.		✓	✓				✓	✓	✓
SU 3	ICT assets are protected against web-based threats by implementing measures that will prevent downloading software programs, active content and non- business related websites.		✓	✓				✓	✓	✓
SU 4	Web access is provided through secure proxies and filtering gateways as defined in section C 4, Gateway Security [GS].		✓	✓				✓	✓	✓
SU 5	*Staff is aware of the types of content permitted and restricted within the Agency, as specified in section B- 4, Gateway Security [GS]. Agencies SHOULD consider an effective solution for monitoring content of encrypted channels.		✓	✓	✓	✓		✓	✓	✓
SU 6	Staff use e-mail with due diligence and include necessary classification labeling depending upon the content/attachments according to National Information Classification Policy [IAP-NAT-DCLS].	✓	✓	✓				✓	✓	✓
SU 7	Appropriate measures are taken that e-mail is protected against potential threats as viruses, trojans, spam mails, forgery and social engineering			✓	✓	✓		✓	✓	✓
SU 8	*Staff is aware that web based public e-mail services are not allowed to be used to send and receive e-mails from Agency systems.		✓	✓				✓	✓	
SU 9	Staff is aware that e-mails used to exchange confidential information SHOULD only be sent to named recipients and not to a group or distribution list.		✓	✓				✓	✓	
SU 10	Staff is aware that the use of automatic forwarding of e-mails is dependent upon the sensitivity of their normal e-mails. Emails carrying information classified at C2 and above SHALL NOT be automatically forwarded outside to the Agency's systems.		✓	✓				✓	✓	

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
SU 11	*When dealing with external parties, Agencies ensure that external recipients/originators understand and agree on the usage of classified data as defined in section C- 3, Information Exchange [IE].		✓	✓				✓	✓	
8. Media Security [MS]										
Media Classification and Labelling										
MS 1	Hardware containing media is classified at or above the classification of the information contained on the media		✓					✓	✓	✓
MS 2	Non-volatile media is classified to the highest classification of information stored on it		✓					✓	✓	✓
MS 3	*Volatile media that has a continuous power supply is classified to the highest classification of information stored on it while the power is on. Volatile media may be treated as classified C1 information once the power is removed from the media.	✓	✓					✓	✓	✓
MS 4	Storage media is reclassified if: a. information copied onto that media is of a high classification, b. information contained on that media is subject to a classification upgrade	✓	✓					✓	✓	✓
MS 5	Media holding classified information may be declassified after: a. the information on the media has been declassified by the originator, or b. the media has been sanitized in accordance with section C- 8.3, Policy & Baseline Controls - Media Sanitization	✓	✓							✓
MS 6	If the storage media cannot be sanitized, then it cannot be declassified and MUST be destroyed.	✓	✓	✓				✓		
MS 7	*The classification of all media is readily visually identifiable. Agencies SHOULD achieve this by labelling media with a protective marking that states the maximum classification as specified in section B-4, Data Labelling [DL]	✓		✓	✓			✓	✓	✓
MS 8	Classification of all media is easily visually identifiable. When using non-textual representations for classification markings due to operational security, Agencies SHALL document the labelling scheme and train staff members appropriately.	✓		✓	✓			✓	✓	✓
Media Sanitization										
MS 9	They document procedures for the sanitisation of media, which are regularly tested.	✓	✓	✓				✓		
MS 10	All media types which contain information classified as C1 or above are destroyed prior to disposal: a. microfiche & microfilm b. optical discs c. printer ribbons and the impact surface facing the platen d. programmable read-only memory e. read-only memory f. faulty media that cannot be successfully sanitised.	✓	✓	✓				✓		
MS 11	Volatile media is sanitised by: a. removing power from the media for at least 10 minutes, or b. overwriting all locations of the media with an arbitrary pattern followed by a read back for verification.	✓	✓	✓				✓		

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
MS 12	Non-volatile magnetic media is sanitised by: a. overwriting the media, if pre-2001 or under 15GB, in its entirety, with an arbitrary pattern followed by a read back for verification three times b. overwriting the media, if post-2001 or over 15GB, in its entirety, with an arbitrary pattern followed by a read back for verification one time; or c. using a degausser with sufficient field strength for the coercivity of the media (NOTE: Degaussing may render some modern media unusable)	✓	✓	✓				✓		
MS 13	Non-volatile EPROM media is sanitised by erasing as per the manufacturer's specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media once in its entirety with a pseudo random pattern. Sanitization of media with rating C3 & above SHOULD be documented.	✓	✓	✓				✓		
MS 14	Flash memory media is sanitized by overwriting the media twice in its entirety with a pseudo random pattern, followed by a read back for verification.	✓	✓	✓				✓		
Media Repairing and Maintenance										
MS 15	Appropriately vetted and briefed personnel carry out repairs and maintenance for hardware containing classified information.		✓	✓	✓				✓	✓
MS 16	Repairs on systems containing classified information rated C3 or above are carried out under supervision.		✓	✓	✓	✓			✓	✓
Media Destruction and Disposal										
MS 17	Document procedures for destruction and disposal of media		✓	✓				✓	✓	
MS 18	Media is destroyed by: a. Deguassing non-volatile magnetic media b. breaking up the media c. heating the media until it has either burnt to ash or melted.		✓	✓				✓	✓	
MS 19	Staff members supervise the destruction of media: a. handling the media to the point of destruction b. ensuring that the destruction is completed successfully. c. C3 & above media destruction must be documented.		✓	✓				✓	✓	
MS 20	Media, including faulty media, containing classified information is sanitised to the extent possible prior to disposal.		✓	✓				✓	✓	
MS 21	The disposal of media and media waste does not attract undue attention.		✓	✓				✓	✓	
9 Access Control Security										
General										
AM 1	Users will be provided access based on the concept of "least privilege" and governed by a "Need to Know" or a "Need to Have" basis.	✓	✓	✓						

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
AM 2	Access will be managed and controlled through system access controls, identification and authentication, and audit trails based on the sensitivity of the information. These requests for access SHALL be authorized by a staff member's supervisor or manager.	✓	✓	✓						
AM 3	Access rights of a user or entity to create, read, update, delete or transmit a Agency's information assets SHALL be based on a matrix (hierarchical) model of rights defined by business rules established by the owners of that information.	✓	✓	✓						
AM 4	A process is established which, upon any employee role or status change (including termination), ensures that information system access is updated to reflect the employee's new role.	✓	✓	✓						
AM 5	System users that need additional access to bypass security mechanisms for any reason seek formal authorisation from the Security Manager	✓	✓	✓						
AM 6	Any unauthorized effort to circumvent the Agency's access control SHALL be perceived as a security incident, and SHALL be handled in accordance with established incident handling procedure and/or appropriate human resources policies and procedures.				✓	✓				
AM 7	Audit logs SHALL be enabled and maintained in such a manner as to allow compliance monitoring with government policy and to assist in Incident Management.	✓			✓	✓				
AM 8	Logical access to Agency Networks is technically controlled. This MAY be by using Network Admission Control (NAC) services/devices.	✓	✓	✓						
AM 9	Secure records are maintained of: a. all authorised system users b. their user identification c. who provided the authorisation to access the system d. when the authorisation was granted e. maintain the record for the life of the system to which access is granted.	✓	✓	✓	✓					
AM 10	A logon banner is displayed before access to the system is granted. These banners SHOULD cover: a. access is only permitted to authorised system users b. the system user's agreement to abide by relevant security policies c. the system user's awareness of the possibility that system usage is being monitored d. the definition of acceptable use for the system e. legal ramifications of violating the relevant policies. f. Wherever possible requires a system user response, as acknowledgement	✓	✓	✓		✓				

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
AM 11	Centralised authentication repositories such as LDAP, authentication databases, etc. are protected from denial of service attacks and use secure and authenticated channels for retrieval of authentication data. Such repositories SHALL log the following events: a. Unauthorized update/access b. Start and end date and time of activity, together with system identifier c. User identification (for illegal logon) d. Sign-on and sign-off activity (for illegal logon) e. Session/terminal or remote connection	✓	✓	✓	✓					
Identification and Authentication										
AM 12	They develop and maintain a set of policies, plans and procedures, derived from the National Information Classification Policy [IAP-NAT-DCLS], covering system users': a. identification b. authentication c. authorisation	✓	✓					✓	✓	✓
AM 13	They educate their system users of the Agency's policies and procedures.	✓	✓	✓				✓	✓	✓
AM 14	All system users are: a. uniquely identifiable b. authenticated on each occasion that access is granted to a system.	✓	✓	✓				✓	✓	
AM 15	Individuals who are not employees, contractors, or consultants are not granted a user account or be given privileges to use the Agency's information resources or communications systems unless explicitly approved by the Security Manager who SHALL check that appropriate agreements, clearance and access forms have been completed.	✓		✓				✓	✓	
AM 16	That alternate methods of determining the identification of the system user are in place when shared/non-specific accounts are used.	✓	✓					✓	✓	
AM 17	Unprotected authentication info that grants system access or decrypts an encrypted device is located on or with the system or device to which authentication information grants access to.	✓	✓					✓	✓	
AM 18	System authentication data whilst in use is not susceptible to attacks including, but not limited to, replay, man-in-the-middle and session hijacking	✓	✓	✓				✓	✓	
AM 19	A password policy enforcing either a minimum password length of 12 characters with no complexity requirement or a minimum password length of seven characters, consisting of at least three of the following character sets: a. lowercase characters (a-z) b. uppercase characters (A-Z) c. digits (0-9) d. punctuation and special characters	✓		✓				✓	✓	
AM 20	Passwords are changed at least every 90 days	✓	✓					✓	✓	

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
AM 21	System users cannot change their password more than once a day and the system forces the user to change an expired password on initial logon or if reset.	✓	✓	✓				✓	✓	
AM 22	Chosen passwords are checked to prevent: a. predictable reset passwords b. reuse of passwords when resetting multiple accounts c. passwords to be reused within eight password changes d. users to use sequential passwords	✓	✓					✓	✓	
AM 23	Screen and/or session locks configured to: a. activate after a maximum of 15 minutes of system user inactivity b. activate manually by the system user, if desired c. lock to completely conceal all information on the screen d. ensure the screen does not appear to be turned off while in the locked state e. have the system user re-authenticate to unlock the system f. deny system users the ability to disable the locking mechanism.	✓	✓	✓				✓	✓	
AM 24	Access to a system is suspended after a specified number of failed logon attempts or as soon as possible after the staff member no longer needs access, due to changing roles or leaving the Agency.	✓		✓				✓	✓	
AM 25	Lost, stolen, compromised passwords are immediately: a. reported, to the Security Manager who SHALL ensure the corresponding account is suspended b. changed upon user identity verification	✓	✓					✓	✓	
AM 26	Accounts that are inactive for more than three (3) months are suspended.	✓						✓	✓	
AM 27	Accounts on systems processing information rated C2, I2, A2 or above are audited for currency on a six (6) monthly basis.	✓		✓	✓			✓	✓	
System Access										
AM 28	Security policies document any access requirements, security clearances and briefings necessary for system access.	✓	✓					✓	✓	✓
AM 29	System users have been vetted as specified in section B- 6, Personnel Security [PS], before being granted access to a system.	✓	✓					✓	✓	
AM 30	System users have received any necessary briefings before being granted access to a system.	✓	✓	✓				✓	✓	
Privileged Access										
AM 31	The use of privileged accounts is documented, controlled and accountable and kept to a minimum. Privileged accounts SHALL only be used for administrative work	✓	✓					✓	✓	
AM 32	System administrators are assigned an individual account for undertaking their administration tasks	✓	✓					✓	✓	

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
AM 33	Only Qatari nationals have privileged access to systems processing information classified at C4 and above unless explicit authorisation for exemption to this policy is given.	✓	✓					✓	✓	
AM 34	System management log is updated to record the following information: a. sanitisation activities b. system startup and shutdown c. component or system failures d. maintenance activities e. backup and archival activities f. system recovery activities g. special or out of hours activities.				✓			✓	✓	✓
Remote Access										
AM 35	Remote access SHALL NOT be provided unless authorized explicitly by the department head and only if it is warranted by business requirements and only after due diligence has been performed to analyze associated risks and suitable controls are implemented to mitigate the identified risks.	✓		✓				✓	✓	✓
AM 36	Two factor authentication, using a hardware token, biometric control or similar is used when accessing systems processing data classified at C3 or above.	✓	✓					✓	✓	
AM 37	Remote access sessions are secured by using suitable end-to-end encryption as specified in section C- 10, Cryptographic Security [CY].			✓				✓	✓	✓
AM 38	Remote access computers are equipped with at a minimum, a personal firewall and anti-malware software. These security controls SHALL be activated at all times.	✓		✓	✓	✓		✓	✓	✓
AM 39	Software, including security software on these computers SHALL be patched and kept up to date.		✓					✓	✓	✓
AM 40	Users do not access Agency internal systems from public computers e.g. Cyber Cafes etc. or print material to any public computer.	✓	✓	✓				✓	✓	
AM 41	Vendor remote access is limited to situations where there are no other alternatives. In this case, initiation of the connection SHALL be controlled and monitored by the Agency. Vendor remote access SHALL only be for a defined period of time, dictated by the duration of the task being undertaken.	✓	✓	✓				✓	✓	✓
10 Cryptographic Security										
CY 1	The cryptographic algorithms, encryption hardware/software, key management systems and digital signatures, meet the requirements specified in Appendix B of this manual for Approved Encryption/ Cryptographic Algorithms and Systems.		✓	✓				✓	✓	

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
CY 2	The lifetime of the key SHALL be determined by the primarily by the application and the information infrastructure it is used in. Keys SHALL be immediately revoked and replaced if it has been or suspected of being compromised.		✓				✓		✓	✓
CY 3	Information assets classified as C3 [IAP-NAT-DCLS] are encrypted and protected against unauthorized disclosure when stored and/or in transit regardless of the storing format or media. Agencies MAY apply these cryptographic controls to assets with lower confidentiality requirements, if determined necessary by their risk assessment.		✓	✓				✓	✓	
CY 4	Information assets classified as I3 [IAP-NAT-DCLS] have assured integrity by the use of cryptographic hashing. Agencies MAY apply these cryptographic controls to assets with lower integrity requirements, if determined necessary by their risk assessment. Appendix B to this section specifies approved hashing algorithms.			✓	✓				✓	
CY 5	The following protocols or better, with approved algorithms outlined in Appendix B, are used for securing data classified as C3 when in transit: a. For securing web traffic: TLS (128+ bits) [RFC4346] b. For securing file transfers: SFTP [SFTP] c. For secure remote access: SSH v2 [RFC4253] or IPSEC [RFC 4301] d. Only S/MIME v3 [RFC3851] or better are used for securing emails. See CY11 for associated requirement.	✓	✓	✓				✓	✓	✓
CY 6	Passwords must always be encrypted/hashed and protected against unauthorized disclosure when they are stored and/or in transit regardless of the storing format or media. Privileged passwords SHALL be encrypted and stored off-site with backup files each time the password is changed to ensure complete recovery.		✓	✓				✓	✓	✓
CY 7	Where Hardware Security Modules (HSMs) are used, they are certified to at least FIPS 140-2 Level 2 [FIPS-140-2] or Common Criteria [CC3.1] EAL4.	✓	✓					✓	✓	✓
CY 8	Cryptographic keys are only physically moved in HSMs meeting CY5		✓					✓	✓	

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
CY 9	Suitable key management processes are defined, as per [ISO11770-1] and used to manage the lifecycle of cryptographic keys, covering the following functions: <ul style="list-style-type: none"> • Key Custodians Roles and Responsibilities • Key Generation • Dual Control and Split Knowledge • Secure Key Storage • Key Usage • Secure Key Distribution and in Transit • Key Backup and Recovery • Periodic Key Status Checking • Key Compromise • Key Revocation and Destruction • Audit Trails and Documentation 		✓					✓	✓	
CY 10	Agency's SHALL ensure the digital certificates are compliant to standards in use by the CSP-PMA, MICT. Agencies SHALL use online revocation systems to minimize the risk of fraudulent use of digital certificates.			✓				✓		
CY 11	Security token/smartcard provisioning systems of CSPs meet the requirements for Subject Device Provision Services as specified in [CWA14167-1].	✓		✓				✓		
CY 12	Any digital certificates used in a production system SHALL be issued by a CSP licensed in Qatar.			✓				✓		
11 Portable Devices & Working Off Site Security										
OS 1	They develop policies governing if, and how, Mobile Devices (MDs) and laptops can be used in their organisation.	✓		✓				✓	✓	✓
OS 2	They do not conduct classified conversations using MDs and laptops capable of conducting phone conversations while using Bluetooth-enabled peripherals.		✓					✓	✓	
OS 3	MDs and laptops with Bluetooth serial port connections do not have the port enabled if the device is to hold classified information.	✓						✓	✓	✓
OS 4	MDs with recording facilities are not allowed into high risk areas without prior approval from the Security Manager.		✓	✓				✓		
OS 5	All laptops and MDs SHALL encrypt the information they carry and be password protected.			✓				✓	✓	
OS 6	MDs and laptops SHALL be kept under continual direct supervision when in use or kept secured when not in use.	✓	✓	✓				✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
OS 7	MDs and laptops not directly owned or controlled by the Agency are not used with the Agency's systems. MDs and laptops not owned or controlled by the Agency SHALL be managed, accounted for and accredited in the same manner as agency owned devices. Agency MD's and laptops MAY be temporary connected to a non- Agency network provided a suitable firewall is used to protect the device from any potential threats originating from the non- Agency controlled network.		✓	✓				✓		
OS 8	Unaccredited MDs and laptops do not connect to the Agency's systems or store Agency information. However, temporary connected MDs and laptops are permitted provided they are segregated from the main networks by a firewall.	✓	✓	✓				✓	✓	
OS 9	In case of loss or theft of the MDs or laptops, the incident should be immediately reported to the Information Security Manager / Office and the concerned Law enforcement agencies. The loss / theft SHALL be handled as per the B-8 Incident Management[IM]					✓		✓		✓
OS10	Emergency destruction/locking plan /remote wipe/auto destruct is in place for any MDs and laptops.	✓	✓					✓	✓	✓
12 Physical Security										
PH 1	Appropriate protection for physical space is determined based on an assessment of risk. This assessment SHALL occur during the design phase of a new construction or, for existing workplaces, as part of an on-going risk management process.	✓	✓	✓				✓	✓	✓
PH 2	Physical spaces are zoned depending upon their security requirement. Each zone is designated a physical security level.	✓	✓					✓		✓
PH 3	Each zone has the appropriate physical security controls implemented. Appendix A provides details of these minimal and baseline protection controls, together with recommendations for additional controls. Medium protection requires one additional class of control, whereas High protection requires two additional class of control. An Agency MAY incorporate additional controls in addition to those mandated by this policy.		✓					✓		
PH 4	Implementation of a "clean desk" and "clean screen" policy.	✓	✓	✓	✓			✓	✓	✓
PH 5	Server/Data rooms meet at least the medium protection requirement		✓	✓				✓		
PH 6	Cabling carrying information at levels C1-C3 is physically separate (including for fibre optic cabling) and is in separate ducting to that carrying Nationally Classified information	✓						✓	✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
PH 7	A site security plan and where necessary standard operating procedures (SOPs) for each secure areas are developed and implemented. Information to be covered includes, but is not limited to: a. a summary of the protective security risk assessment b. roles and responsibilities of facility or ICT security officer and staff members. c. the administration, operation and maintenance of the electronic access control system and/or security alarm system d. key management, the enrolment and removal of system users and issuing of personal identification e. staff member clearances, security awareness training and regular briefings f. inspection of the generated audit trails and logs g. end of day checks and lockup h. reporting of ICT security incidents and breaches.	✓	✓	✓	✓			✓	✓	✓
13 Virtualization										
VL 1	Evaluate the risks associated with the virtual technologies. a. Evaluate the risks in context of relevant legal, regulatory policies and legislations. b. Evaluate how the introduction of virtual technology will change your existing IT infrastructure and the related risk posture.	✓	✓					✓	✓	✓
VL 2	Harden the hypervisor, administrative layer, the virtual machine and related components as per the industry accepted best practices and security guidelines and the vendor recommendations.			✓	✓			✓	✓	✓
VL 3	Enforce least privilege and separation of duties [Refer to section C-9 Access Management] for managing the virtual environment. a. Define specific roles and granular privileges for each administrator in the central virtualization management software. b. Limit direct administrative access to the hypervisor to the extent possible c. Depending on the risk and the classification of the information processed, Agencies should consider the use of multi factor authentication or dual or split control of administrative passwords between multiple administrators.	✓	✓	✓				✓	✓	✓
VL 4	Ensure adequate physical security to prevent unauthorized access to the virtual technology environment.	✓	✓	✓	✓			✓	✓	✓
VL 5	Virtualized technology environment should be augmented by third party security technology to provide layered security controls (defence in depth approach) to complement the controls provided by the vendor and technology itself.			✓	✓			✓	✓	✓
VL 6	Segregate the Virtual Machines based on the classification of data they process and / or store.		✓						✓	✓

National Information Assurance Policy V2.0 Controls Classification

	Control	Type						Primary objective		
		Deter	Avoid	Prevent	Detect	React	Recover	Confidentiality	Integrity	Availability
VL 7	A change management [Refer to Section B-6 Change Management] process encompasses the virtual technology environment. a. Ensure that virtual machine profile is updated and the integrity of the Virtual Machine image is maintained at all times. b. Care should be taken to maintain and update VM's which are not in active state (dormant or no longer used).	✓	✓					✓	✓	
VL 8	Logs from the virtual technology environment SHALL be logged and monitored along with other IT infrastructure. [Refer to Section B-10 Logging and Security Monitoring].	✓			✓	✓		✓	✓	✓