

**Achievement of Market-Friendly Initiatives and Results Program
(AMIR 2.0 Program)**

Funded By U.S. Agency for International Development

Jordan e-Government Information Security Plan

Final Report

**Deliverable for ICTI Component, Task No. 431.4.4
Contract No. 278-C-00-02-00201-00**

April 2002

This report was prepared by Paul De Luca, in collaboration with Chemonics International Inc., prime contractor to the U.S. Agency for International Development for the AMIR Program in Jordan

0 Document Control

Table of Contents

0	DOCUMENT CONTROL	3
0.1	Document History	5
0.2	Changes From Last Issue	5
0.3	Acknowledgements	5
0.4	Distribution List	5
0.5	Referenced Documents	5
0.6	Abbreviations	5
0.7	Glossary	6
1	FOREWORD	7
1.1	What is Information Security	7
1.2	Why information security is needed	7
2	INTRODUCTION	8
2.1	Documentation hierarchy	8
2.2	In scope	8
2.3	Out of scope	9
3	THE INFORMATION SECURITY POLICY	10
3.1	Statement of intent	10
3.2	Policy control	10
3.2.1	Ownership	10
3.2.2	Implementation	10
3.2.3	Review	10
3.3	Principles	10
3.3.1	Governance and responsibility	10
3.3.2	Information asset ownership	10
3.3.3	Information asset custodianship	10
3.3.4	Information asset classification	11
3.3.5	Risk assessment	11
3.3.6	Asset protection	11
3.3.7	Uniquely identifiable	11
3.3.8	Access to assets	11
3.3.9	Use of assets	11
3.3.10	Incident management	12
3.3.11	Development of information processing facilities	12
3.3.12	Contingency	12
3.3.13	Legal and regulatory requirements	12
3.3.14	Training and awareness	12
4	INFORMATION SECURITY MANAGEMENT CODE OF PRACTICE	13
4.1	Risk based approach to information security management	13
4.1.1	Risk Management	13
4.2	Organisational security	14
4.2.1	Information security infrastructure	14
4.2.2	Security of third party access	16

4.3	Asset classification and control.....	16
4.3.1	Accountability for assets	16
4.3.2	Information classification.....	16
4.4	Personnel security	17
4.4.1	Security in job definitions and resourcing.....	17
4.4.2	User training	18
4.4.3	Security incident response.....	18
4.5	Physical and environmental security.....	19
4.5.1	Secure areas	19
4.5.2	Equipment security.....	19
4.5.3	General controls.....	19
4.6	Communications and operations management.....	20
4.6.1	Operational procedures and responsibilities.....	20
4.6.2	Systems planning and acceptance.....	20
4.6.3	Protection against malicious software	21
4.6.4	Housekeeping	21
4.6.5	Network management.....	21
4.6.6	Media handling and security	21
4.6.7	Exchanges of information and software	21
4.7	Access control.....	22
4.7.1	Business requirements for access control.....	22
4.7.2	User access management.....	22
4.7.3	Monitoring system access and usage.....	23
4.8	Systems development and maintenance.....	23
4.8.1	Security requirements of systems	23
4.8.2	Security in applications	24
4.8.3	Cryptographic control.....	24
4.8.4	Security in development and support processes.....	24
4.9	Business continuity management.....	24
4.9.1	Aspects of business continuity management.....	24
4.10	Compliance	25
4.10.1	Compliance with legal requirements	25
4.10.2	Review of security policy and technical compliance	25
4.10.3	System Audit Considerations	25

Table of Figures

Figure 1: Documentation Hierarchy for Information Security Management.....	8
Figure 2: Risk management concepts.....	13
Figure 3: Information security fora	15

Document History Versions will be identified numerically with the Status either Draft, Draft for Review or Approved. Approved documents will have a whole numbering sequence, eg. 1.0, 2.0, with Draft documents using a decimal numbering sequence, eg. 0.1, 0.2.

Version	Status	Date
0.1	Draft	25 April 2002
0.2	Draft	28 April 2002
1.0	Final	30 April 2002

Changes From Last Issue This section is a brief overview of the changes made in the current version of the document.

Version	Status	Reviewer	Date
0.1	Draft	Dave Arthur	27 April 2002
0.2	Incorporate Changes from review of v0.1	Dave Arthur	29 April 2002
1.0	Addition of GOJ Specific PMO Requirements		

Acknowledgements

N/A

Distribution List

Allan Gormley	EDS
Kendall Lott	EDS
Reginald Miller	AMIR
Mahmoud Ali Khasawneh	MoICT

Referenced Documents This section is where documents referenced in the body of the document should be listed giving the full document title and the document reference number.

Number	Title	Reference	Note
	N/A		

Abbreviations

AMIR	Access to Microfinance & Improved Implementation of Policy Reform
GOJ	Jordan E-Government Programme
MoICT	Ministry of Information, Technology and Communications (previously MoPC).
PMO	Programme Management Office
PO	Project Office

Glossary This section is optional and is a list of all terms used within the document which require explanation

Availability	Ensuring authorised access to information as and when required.
Confidentiality	Ensuring that information is only disclosed to those authorised to see it.
Employee	Those providing e-Gov with direct or indirect services.
Information Asset	A set of related information for which unauthorised disclosure, modification or unavailability would adversely impact day-to-day business.
Information Processing Facility	An electronic or manual system for processing information (which may consist of a single entity or a significant number of related entities).
Information Security	Preservation of confidentiality, integrity, and availability of information.
Integrity	Ensuring the accuracy and completeness of information.
Risk Assessment	Process of determining threats and vulnerability to information, the potential business impacts, and likelihood of a security incident occurring.
Risk Management	The process of proactively managing down the risk profile to an acceptable level for an acceptable cost.

1 Foreword

What is Information Security

Information exists in many forms. It can be printed, written on paper, stored electronically, transmitted by post, using electronic means, shown on films or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information security protects information from a wide variety of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

Information security is characterised here as the preservation of:

- confidentiality: ensuring that information is only disclosed to those authorised to see it;
- integrity: ensuring the accuracy and completeness of information and processing methods;
- availability: ensuring that authorised users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which include policies, practices, procedures, organisational structures and software functions. These controls need to be established to ensure that specific security objectives of an organisation are met.

Why information security is needed

Information and the uses it is put to are important business assets which contribute towards organisations' competitive edge, cash-flow, profitability, legal compliance, commercial image, and public perception.

Increasingly, organizations and their information processing facilities are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood, terrorism, etc. Computer viruses, computer hacking and denial of service attacks have increased significantly in both their number and sophistication. Dependence on information processing facilities and services, along with the interconnection of public and private networks, leaves organizations increasingly vulnerable to such security threats. More over, many information-processing facilities have not been designed with security in mind.

In order to establish trust, it is necessary to demonstrate that information and information processing facility are adequately protected from these security threats, hence, the need for information security (and an information security management system).

2 Introduction

Documentation hierarchy

The documentation hierarchy for managing information security can be described using analogies from the building industry, i.e. firm foundations, strong supporting structures, and a watertight roof.

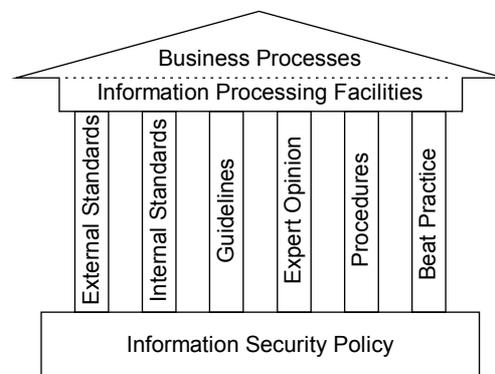


Figure 1: Documentation Hierarchy for Information Security Management

- Firm foundations

The Information Security Policy (ISP) lays the foundation that must be seen to underpin all security relevant decisions. The ISP is a concise high-level document that encompasses the fundamental principles that are essential for delivering best security practice.

- Strong supports

- External Standards reflect the legal and regulatory framework within which business processes exist, e.g. e-Payments will need to comply with certain ISO/Banking standards;
- Internal Standards define the organisational and technical framework underpinning business processes;
- Guidelines advise on implementation and operations of manual and electronic components that underpin information processing facilities, e.g. build specifications, configurations, etc.;
- Expert Opinion reflects advice from (invariably external) subject matter experts in the field;
- Procedures unambiguously and reliably describe the sequence and content of actions ensuring consistent delivery of objectives;
- Best Practice reflects sound auditable decisions, e.g. segregation of duties, dual skin firewalls, etc.

- Water tight roof

- Information Processing Facilities define the scope and roles played by each of the manual and electronic systems, and their interactions, that deliver elements of the business processes;
- Business processes define the scope and manner of interaction with each manual and electronic information processing facility necessary to fulfil business objectives.

In scope

The purpose of this document is to define the ISP for e-Gov. The scope of the ISP is to concisely reflect the fundamental security principles, roles and responsibilities that underpin the providing of adequate protection for information assets. Additionally, the ISP will include guidance on organisational security, asset classification

and control, personnel security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance.

Out of scope

The ISP provides high-level governance and, as such, is independent of technical/platform architectures and related implementation/operational details. Therefore, the areas mentioned in the ‘strong support’ and ‘water tight roof’ bullets above are beyond the scope of the ISP.

3 The Information Security Policy

Statement of intent

The ability to govern effectively is overwhelmingly dependent on the quality of information assets (assets) to hand, and the means by which they are used. Therefore, e-Gov mandates that each asset must be adequately secured and that the means by which this is achieved must reflect the principles of this ISP and the advice on information security management that follows in section 4. To this end, all those who come in touch with assets will be held personally accountable for ensuring adequate security is provided and maintained.

Policy control

3.1.1 Ownership

The ISP and subsequent security standards are owned by the e-Gov Executive, and are defined and maintained by e-Gov Information Security Forum (who reports directly to the Deputy Director General for MoICT).

3.1.2 Implementation

The responsibility for ensuring that the ISP and related security standards are implemented ultimately lies with the Deputy Director General (DDG) of each Ministry participating in e-Gov and should be reported as part of an annual self certification compliance programme. It is the DDG's responsibility to ensure that the necessary knowledge, skills, and expertise are available in order to enable their employees to meet security requirements. Furthermore, the DDGs are responsible for ensuring appropriate standards and documented procedures are provided for their operational and information processing facilities.

All employees are responsible for maintaining the required level of information security within the scope of their role.

3.2.3 Review

To ensure that it remains appropriate, the policy is reviewed every six months, or following significant security related incidents.

This policy is approved by the Information Security Forum (ISF) and endorsed by Chair of e-Gov Executive.

Principles

The fundamental principles provide a foundation for governance which will ensure that the risk to e-Gov assets is proactively managed down, in a common and consistent manner, to an acceptable level.

3.1.3 Governance and responsibility

To ensure that the risk to assets are managed in a cost effective manner

Compliance with the ISP is mandatory for all e-Gov employees and representatives.

All e-Gov employees have a personal responsibility to safeguard assets for which they will be held accountable.

Note: DDGs are further required to annually certify that their ministries comply with the ISP.

3.1.4 Information asset ownership

To ensure that each asset has an owner who is accountable for its security.

Each asset must have a single nominated owner. The Information Asset Owner (IAO) will be held accountable for ensuring the security of their assets.

Note: The IAO will be the least senior person who may legitimately take risk decisions which affect the asset.

3.1.5 Information asset custodianship

To ensure that the implementation of security requirements for each asset.

The Information Asset Custodian (IAC) will be held accountable for implementing the security controls specified by the IAO.

Note: An IAC is any individual who has the day-to-day responsibility for the storage or processing of assets on behalf of their owner. The IAO and IAC may be the same person.

3.1.6 Information asset classification

To ensure that all key assets are identified.

Each IAO must formally identify and classify each of their assets.

Note: The classification should reflect both the intrinsic criticality of the asset and the cost of recovering from a business impact resulting from a breach of confidentiality, integrity, or availability.

3.1.7 Risk assessment

To ensure that the appropriate level of protection is identified for each asset.

The risk of unauthorised disclosure, modification or unavailability of assets must be formally assessed.

Note: The risk to an asset will reflect a combination of its classification and vulnerability to a comprehensive range of threats.

3.1.8 Asset protection

To ensure that each asset receives the appropriate level of protection.

IAO must formally manage the risk to their assets by commissioning security controls to preserve appropriate levels of confidentiality, integrity, and availability.

3.1.9 Uniquely identifiable

To ensure that individuals can be held accountable for their (in)actions.

Individuals must be uniquely identifiable.

The method of authentication to information processing facilities must reflect the classification of, and risk to, the subsequently accessible assets.

Individuals will be held personally accountable for all actions performed under their unique identity regardless of whether they actually performed the actions.

3.1.10 Access to assets

To ensure that access to assets is not excessive.

The scope of access to assets through information processing facilities must be based on the principles of least privilege and need-to-know.

3.1.11 Use of assets

To ensure that assets are used appropriately.

Assets and information processing facilities should only be used to meet the legitimate business needs of e-Gov.

Note: Assets must not be used for private business or personal gain.

3.1.12 Incident management

To minimise business impacts arising from security incidents.

Security incidents and suspicious events must be reported and managed in order to ensure timely, effective and orderly resolution.

3.1.13 Development of information processing facilities

To ensure cost effective protection of assets.

Information processing facilities should be developed with the requirement for security services addressed from the outset.

Note: Security should be designed in and not simply bolted on (as an after thought).

3.1.14 Contingency

To ensure critical information processing facilities and assets are available when needed.

The IAO must ensure that adequate contingency arrangements are in place to recover their business critical assets in a timely manner.

3.1.15 Legal and regulatory requirements

To ensure that e-Gov meets all legal and regulatory requirements

e-Gov, and its employees, must comply with all statutory, regulatory, and contractual requirements which relate directly or indirectly to information security.

3.1.16 Training and awareness

To ensure that individuals are empowered to deliver best security practice.

All employees will receive awareness and training commensurate with their roles and responsibilities.

Note: Training and awareness is the most cost effective means to best security practice.

4 Information Security Management Code of Practice

Risk based approach to information security management

The ISP states the fundamental principles that should underpin and be reflected in the way that e-Gov conducts its activities. The advice below outlines the means by which e-Gov can foster best security practice and develop organisational security standards. The advice and recommendations introduced below should be used in accordance with statutory, regulatory, and contractual requirements.

4.1.1 Risk Management

4.1.1.1 Overview

Risk Management forms the basis for adequately securing assets, and the resources that interface to them. All risk assessment methods follow a similar approach. The steps involved are to:

- evaluate the assets that are to be protected;
- analyse the impact on the enterprise of each asset being compromised;
- consider the possible threats that might result in compromise;
- identify the vulnerabilities that might expose the assets to the threats;
- propose countermeasures that mitigate the risk and are appropriate to the level of risk.

The interplay between the risk management concepts is illustrated in Figure 2.

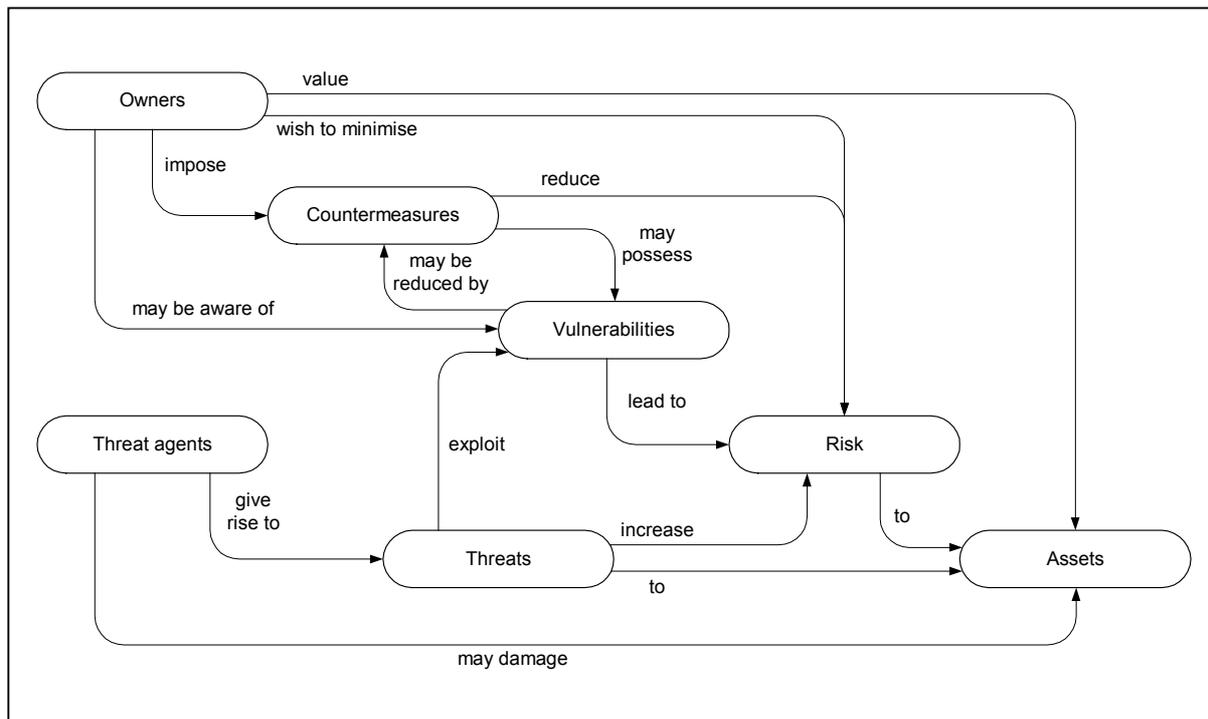


Figure 2: Risk management concepts

4.1.1.2 Description of the risk management Process

Each of the steps in the risk assessment process is summarised below.

- Identify assets. Assets can be physical or intangible. They include information, data, money, intellectual property, brand name, goodwill, legal compliance and national security.
- Analyse business impact. Each asset is assessed in terms of the impact to the business of any compromise of confidentiality, integrity or availability. Because the units of valuation are not consistent, in risk assessment we use terms like low, medium, high, minor, significant and serious to describe the impact of compromise.

- Consider threats. Threats are potential hazards. They are malicious or accidental. The likelihood of a particular threat is often related to how attractive any gain might be to an attacker as well as how damaging it would be to the enterprise.
- Identify vulnerabilities. Vulnerabilities are ways in which a threat may be executed. Identifying vulnerabilities requires a model of the information system that is processing the assets.
- Propose countermeasures. Countermeasures reduce the likelihood of a vulnerability being exposed. For instance, authentication militates against access to the systems by unauthorised people and guards against many threats. Countermeasures work together so that, for instance, physical access controls reduce the scope for access to terminals by many classes of potential attacker so that there would be less demanding requirements placed on the logical authentication mechanism.

Finally, there is an iterative process that adjusts the business process, the system model and the non-technical environment to arrive at a set of technical and procedural countermeasures that is both appropriate to the risk, affordable, and achievable.

Therefore, best security practice is contingent on a risk-based approach.

Organisational security

4.1.2 Information security infrastructure

4.1.2.1 Management information security forum

The e-Gov Executive devolves the maintenance and development of the ISP to the Government Information Security Manager (GISM). To direct, lead, challenge and co-ordinate information security within the e-Gov, the e-Gov Executive should empower the GISM to establish an Information Security Forum (ISF). The ISF membership should comprise a senior manager from each Ministry, e.g. Deputy Director General, who has responsibility for information security within their ministry. The ISF will typically undertake the following:

- reviewing and approving ISP and overall responsibilities;
- monitoring significant changes in the risk profile;
- monitoring and reviewing information security incidents;
- approving major initiatives for all security related activities.

4.1.2.2 Information security co-ordination

As the size and diversity of the e-Gov membership increases, the ISF should establish a cross-functional forum of management representatives from relevant parts of the e-Gov membership to co-ordinate the implementation of information security controls. Members of this forum will each assume the role of Ministerial Information Security Officer (MISO). This information security co-ordination forum (ISCF) will typically:

- agree specific roles and responsibilities for information security across the (growing) e-Gov membership;
- agree specific information security methodologies and processes, e.g. risk assessment, asset classification system, security incident reporting and notification, etc.;
- agree and support e-Gov wide initiatives, e.g. information security awareness programme;
- ensure security is part of the information processing facility planning process;
- assess the adequacy and co-ordinate the implementation of specific information security controls for new and existing information processing facilities and business processes;
- review information security incidents;
- promote the visibility of business support for information security throughout e-Gov.

Figure 3 illustrates the composition of the ISF and the ISCF.

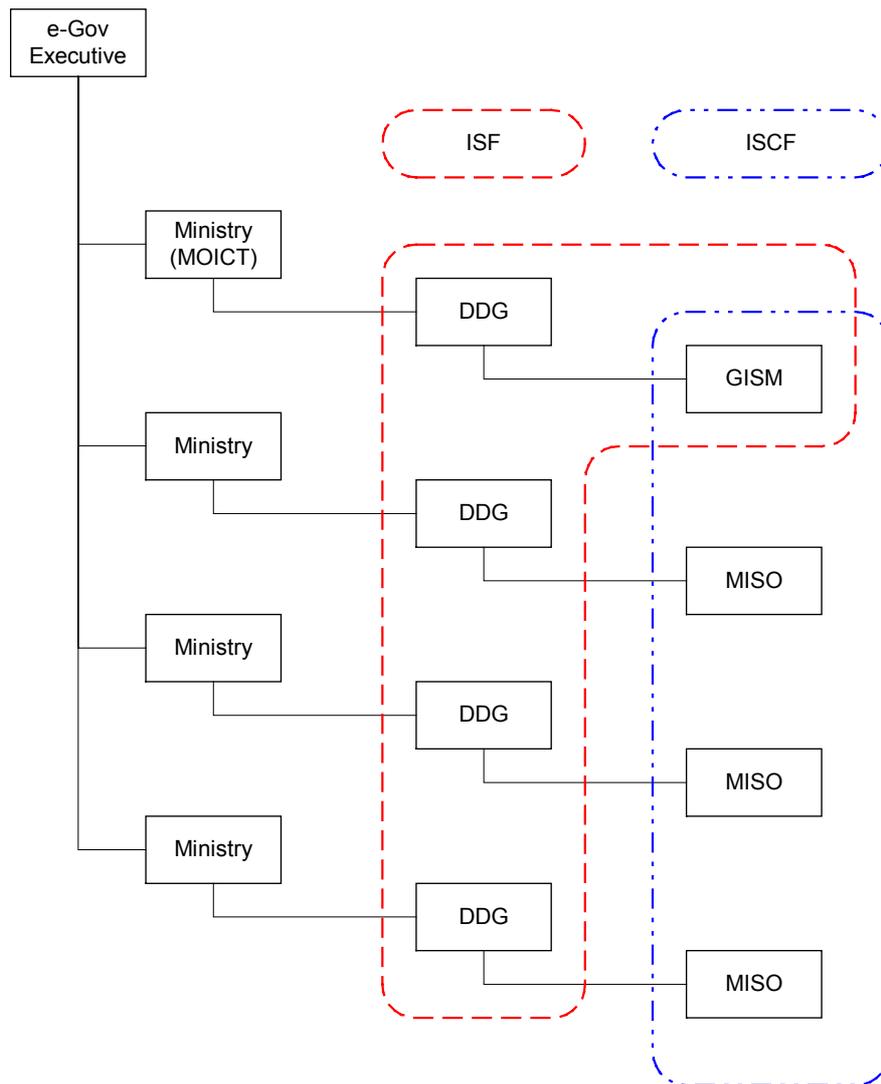


Figure 3: Information security fora

4.1.2.3 Allocation of information security responsibilities

The e-Gov must formally document the structure of its information assets (IA), e.g. the citizen's personal details IA is likely to comprise citizen identity number, first name, last name, date of birth, current address, etc. Similarly, the citizens' health IA is likely to comprise citizen identity number followed by a chronology of health related information. IAs should not be constrained to citizens but developed to encompass the whole spectrum of information required by e-Gov.

Each IA must have a single nominated owner who will be held accountable for ensuring it is appropriately secured. The IAO is the least senior individual who may legitimately take a risk decision that may affect the IA, and is likely to be operating within a business domain rather than a technology domain. It is, therefore, unreasonable to assume that IAOs will have the technical expertise to implement the required security services. IAO will be expected to delegate the day-to-day operational responsibility for ensuring on-going delivery of their specified security services to information asset custodians (IAC). IAC invariably exist within a technology domain, a growing number of which will be preferred partners and third party service providers who must explicitly agree to comply with the ISP.

4.1.2.4 Authorisation process for information processing facilities

Under no circumstances may an IAO release IAs into information processing facilities, be they live/production or test/development, unless all associated IACs have explicitly agreed to implement the security services mandated by the IAO. The IAO will be held accountable for seeking evidential assurance that the information

processing facilities comply with the ISP. Similarly, no IAC may accept an IA into their information processing facilities without explicit details of the specific security services required, and the explicit acceptance from the IAO that (s)he is satisfied with the means by which the required security services are (to be) implemented by the IAC. To ensure that both the IAO and corresponding IAC are crystal clear as to their respective responsibility profile, the only acceptable means of agreement is through a formal e-Gov Service Level Agreement (SLA). To reinforce the importance place on this authorisation process, the e-Gov Executive deems that exchange of IA outside the protection of an e-Gov SLA constitutes serious misconduct, and will result in disciplinary action.

4.1.2.5 Specialist security advice

It is recognised that fulfilment of the ISP will require accessibility to specialist information security advice and skills which are also recognised to be in short supply. It is the intention of the e-Gov Executive to cultivate this expertise within the individual ministries by supporting the individual training needs of the GISM and each MISO. The e-Gov Executive are planning for a continued shortfall in the security arena by empowering the GISM to develop on-going working relationships with those external providers best placed to fulfil the information security requirements of e-Gov.

4.1.3 Security of third party access

4.1.3.1 Identification of risks from third party access

It follows that in some cases, specialist security advice and the fulfilment of e-Gov business, will lead to requirements for third party access to IA and information processing facilities. To ensure the principle of accountability is not undermined, it is essential that third party access is monitored and controlled. Where a third party ultimately fulfills the role of IAC, the IAO and internal IAC must formally document the assumptions, factors, risks, and justifications underpinning the decision to employ a third party. Third party access is conditional on a formally contracted SLA between; the third party itself, the internal IAC, and the IAO. The third party must be contractually bound to comply with the ISP.

Those fulfilling ancillary roles within close proximity to IA and information processing facilities must also be subject to monitoring and control at all times, this is particularly important during out of office hours where there is minimal e-Gov representation.

Asset classification and control

4.1.4 Accountability for assets

4.1.4.1 Inventory of assets

An IA register (IAR) must be maintained to ensure that each IA receives consistently appropriate protection across e-Gov information processing facilities. The IAR holds details on each IA, e.g. identity #, classification profile, IAO, a list of its IACs, a list of the business processes that it is used in, etc. To complement the IAR, a business process register (BPR) should be maintained to cross reference each process with their respective IA and information processing facilities, the BPR should include pointers to business process documentation, e.g. workflows, procedures, etc. Similarly, an information processing facility register should be maintained to cross reference each facility with its constituent components, e.g. hardware, software, computing and communications services, environmental requirements, documentation, user manuals, etc. (Together, these three registers provide a high level interdependency overview, which will be invaluable for business continuity management and disaster recovery.

The IAO must formally approve their IAR entries and ensure timely on-going maintenance. Similarly, business sponsors/owners and IAC must ensure the correctness and completeness of the business process and information processing facility registers respectively.

4.1.5 Information classification

4.1.5.1 Classification guidelines

The classification profile given to an IA effectively determines how it should be protected and handled as it interfaces with business processes and information processing facilities. It is the IAO who is responsible for determining IA classifications, which should reflect both the:

- cost of recovering from those business impacts associated with unauthorised disclosure, modification or unavailability (invariably through service denial);

• Intrinsic criticality of the business processes and information processing facilities.

It follows, from the first bullet, that the classification profile for an IA comprises three components, i.e. the level of confidentiality, integrity, and availability required for the IA. The options for the level required are: *low*, *medium*, *high*, and *extreme*. Table 1 reflects their corresponding business impact recovery costs

Cost of recovering from business impact		Classification
Descriptive	JD	
Unlimited	10 000 000	Extreme
Substantial	1 000 000	High
Significant	100 000	Medium
Minor	10 000	Low

Table 1: Impact based classification

Given that the classification profile is a significant factor in determining security controls, it is important that the classification profile accurately reflect realistic impacts. Over classification will result in a specification for expensive technical and procedural controls. Such controls are likely to impede the smooth completion of business processes and give rise to motivation for circumventing best security practice.

Once defined, classification profiles are likely to change. For example, the confidentiality classification for some economic IA may legitimately be extreme right up to the moment that the Finance Minister releases it for publication, thereafter, the IA confidentiality classification is non-existent. Therefore, the classification profile for each IA should be reviewed, at least annually, to take into account the potential shift in intrinsic criticality and adverse business impact.

4.1.5.2 Information labelling and handling

Concise procedures should be defined to ensure IAs are correctly labelled. For each of the four classification levels (low, medium, high, and extreme) and for each of classification profile components (confidentiality, integrity, and availability), handling procedures should be defined for the following information processing activities:

- copying;
- storage;
- transmission, e.g. post, fax, e-mail, ftp, etc.;
- verbal communication, e.g. face-to-face, telephone, voicemail, answering machine, etc.;
- destruction.

Information processing facilities producing information with a high or extreme classification component should be labelled accordingly. Directing output to nominated terminals and printers should be considered as an effective means of achieving this.

Personnel security

4.1.6 Security in job definitions and resourcing

4.1.6.1 Responsibility in job descriptions

A job definition statement should be defined for each employment role. These statements must reinforce the ISP by formally documenting the general responsibility for discharging best security practice appropriate to the role.

4.1.6.2 Proactive screening

Each potential employee must have their claimed identity, qualifications, and experienced verified at the time of their application. To this end, this should include checking the:

- availability of character references, e.g. at least one business and one personal;
- completeness and correctness of the applicant's curriculum vitae;
- applicant's original academic and vocational certificates;
- applicant's passport (or similar document).

Employees fulfilling job roles which involve access to a financial IAs, or ones having a classification profile component of high or extreme, should undergo periodic additional credit and lifestyle checks. This would help reduce the risk of compromising those who may be subverted.

Similar screening should be conducted for all contractors, third parties, and ancillary staff. Where these staff are provided by an agency, a contract must be in place which clearly specifies the agency's responsibility with respect to screening.

4.1.6.3 Employment terms and conditions

The terms and conditions of employment must clearly state the nature of the employee's responsibility for security and their exposure to disciplinary action. The duration of this responsibility should extend for an appropriate period beyond the term of employment with e-Gov, this extended period must be at least six months.

4.1.7 User training

4.1.7.1 Information security training

To ensure that the security relevant terms and conditions of employment can be met, and hence that there is no excuse for evading accountability, all employees should receive appropriate information security education and training. This should be periodically supplemented with updates on the implication of policy and procedure revisions.

4.1.8 Security incident response

4.1.8.1 Reporting security incidents

The ISF, through the ISCF, should agree a formal security incident reporting and notification (SIRAN) procedure. All employees must be formally made aware of the procedure and required to report (potential/suspicious) incidents without delay. A suitable management process should be developed to ensure incidents are appropriately dealt with and closed; the process should include providing feedback to those raising incidents.

4.1.8.2 Security weaknesses

Users of information processing facilities should be required to note and report any observed or suspected security weakness or threats. It is essential that users must not attempt to prove a suspected weakness as it could easily be interpreted as a potential misuse of information processing facility.

4.1.8.3 Software malfunctions

The ISF, through the ISCF, should agree a formal procedure for reporting software malfunctions, which ensure that the:

- symptoms of the problem are fully recorded;
- affected device is isolated from information processing facilities;
- incident is immediately reported to the MISO;
- only appropriately trained, experienced, and authorised staff carry out recovery.

4.1.8.4 Learning from incidents

Mechanisms should be put in place to enable the types, volumes, and costs of incidents and malfunctions to be monitored and quantified. This information should be used to identify reoccurring and high impact incidents which may flag the requirement for improved or additional security controls.

4.1.8.5 Disciplinary process

There must be a formal disciplinary process for employees who violate the ISP, security best practice, or security related business and operational procedures. It is essential that this process is firm but fair, and communicated to all employees. The stages of the disciplinary process for ISP violation are likely to be:

- formal record of violation to be taken;
- verbal warnings (to a maximum of 3 over the course of a year);
- written warning;
- suspension;
- dismissal.

Deputy Director Generals will be held accountable for the immediate termination of access rights to information processing facilities of employees who have reached the suspension stage of the disciplinary procedure.

Physical and environmental security

4.1.9 Secure areas

4.1.9.1 Physical security perimeter

Physical security barriers should be deployed to define a protective perimeter for IA and associated information processing facilities; in many cases there will be a requirement to provide a layering of such barriers. In each case, the physical security perimeter:

- must be clearly defined;
- must be of appropriately solid construction with no gaps, i.e. the construction must extend into false ceilings and raised floors;
- should incorporate a single point of entry/exit which is manned during operational hours, continuously monitored by CCTV, and alarmed;
- entry/exit doors must slam shut by default.

4.1.9.2 Physical entry controls

Entry to secure areas must be controlled in an auditable manner. All employees should be required to wear their identity pass and be able to produce it on demand for closer inspection. Arrangement for receiving visitors and maintenance staff must be made in advance. Unscheduled visitors to secure areas containing IA with a classification profile component of high should be refused entry. Visitors should have their details formally recorded in a visitors log book, be escorted for the duration of the time on site, and finally escorted off site. Visitors to secure areas containing IA with a classification profile component of high should wear bright red lab coats, which have no pockets, so that they may be easily identified and monitored. Access rights to secure areas should be regularly reviewed.

4.1.10 Equipment security

4.1.10.1 Equipment siting and protection

The components forming information processing facilities should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access. To this end:

- equipment should be sited to minimise unnecessary access into work areas;
- information processing facilities handling IA with a classification profile component of high should be positioned to reduce the risk unauthorised observation during their use;
- equipment requiring special protection should be isolated from that requiring more general protection;
- controls should be adopted to mitigate exposure to theft, fire, flood, smoke, dust, vibration, electrical interference, electromagnetic radiation, etc.;
- food and drink must be kept away from information processing facilities;
- environmental conditions should be continuously monitored.

4.1.10.2 Secure reuse and disposal

Components of information processing facilities, which have come into contact with IA having a classification profile component of high, must be securely purged before reuse. Such components must be securely destroyed at the end of their lifecycle, they must not be recycled for reuse by an external party.

4.1.11 General controls

4.1.11.1 Clear desk and screen

IA having a classification profile component of medium must be locked away when unattended. The strength of the housing must reflect the overall classification profile of the IA together with its intrinsic criticality. Computers must be configured to time out after an initial period of 4 minutes inactivity, reactivation must be dependent on successful user re-authentication. Should the timed out computer experience a subsequent inactivity period of 9 minutes, it should close all current sessions and log off the 'absent' user.

4.1.11.2 Removal of property

IA, hardware, and software must not be taken off site without authorisation from the IAO or IAC. Authorisation will be contingent on demonstrating that the exposed IA will subsequently receive appropriate protection while off site. Given that the IA will be entering a location beyond the control of e-Gov, the off site security requirements are likely to be more stringent than those within the e-Gov environment.

Communications and operations management

4.1.12 Operational procedures and responsibilities

4.1.12.1 Documented operating procedures

Each DDG will be held accountable for ensuring that comprehensive operating procedures are formally documented for the business processes and information processing facilities within their Ministry. These procedures must specify the instructions for the detailed execution of each task and will include:

- processing and handling information;
- scheduling requirements and interdependencies;
- error and exception handling;
- support contact details and escalation triggers;
- system troubleshooting including recovery procedures.

4.1.12.2 Incident management procedures

To ensure a timely, orderly, and effective response, procedures should be established to cover the all potential types of security related incidents, including:

- failures of information processing facilities;
- denial of service attacks;
- errors resulting from incomplete or inaccurate business data;
- confidentiality breach.

4.1.12.3 Segregation of duties

Care should be taken to ensure that no single person could perpetuate a fraud in areas of single responsibility without being detected in a timely manner. The initiation of an event should be segregated from its subsequent authorisation. Should there be a danger of collusion, it is important that the authorisation procedure requires approval from two (or more) individuals.

4.1.12.4 Separation of development and operational information processing facilities

Development and operational information processing facilities should be separated to prevent errors, failures, and incidents affecting one from contaminating the other. To this end:

- development and operational software should run on independent platforms;
- development and testing should be further separated;
- compilers, editors, and other specialist utilities must not be accessible from operational information processing facilities;
- development and operational information processing facilities must clearly identify themselves accordingly, possibly by incorporating a common display format for each;
- development employees must not have access to operational information processing facilities (and vice versa).

4.1.13 Systems planning and acceptance

4.1.13.1 Planning

The build specifications, configuration details, and functional processes for each component of an information processing facility must be formally documented. Once operational, the capacity demands on these components must be monitored and projections for future capacity requirements made to ensure effective and timely fulfilment of business processes.

4.1.13.2 Acceptance

The ISCF must formally agree clearly defined criteria for the acceptance of new, and upgrades to existing, information processing facilities. These criteria must be associated with objectively measurable key performance indicators.

4.1.14 Protection against malicious software

4.1.14.1 Software integrity

Perhaps the threat with greatest potential for impact is that of the covert introduction of malicious code, e.g. viruses, Trojan Horses, network worms and logic bombs. (There will continue to be cases where irreparable damage is done long before any evidence to the fact emerges.) Employees must be educated about the consequences of unauthorised or malicious software, i.e. not only could IA be compromised but individual employees will be held personally accountable for the action of the malicious software operating through their unique UID. To manage down exposure to malicious software, software usage must be constrained to that licensed from those authorised by the ISF to supply e-Gov. Furthermore, a comprehensive technical solution to malicious code must be deployed and complemented by a mandatory end-user procedures for managing file exchange.

4.1.15 Housekeeping

4.1.15.1 Back-ups and logs

Routine procedures should be developed to ensure the regular back-up of essential IA and software from each information processing facility. Back-up and recovery facilities should be provided to test the integrity of back-ups and ensure that recovery procedures fulfil the requirements of business continuity plans.

Comprehensive operational accounting logs must be maintained for each information processing facility. The contents of these logs must reflect the business and operational audit requirements of the IAO, BPO and IAC, and must be agreed as part of the information processing facility acceptance criteria.

Faults should be reported and logged in a timely manner to ensure that corrective action may be taken without undue delay. A procedure should be defined for handling and escalating faults while corrective action must be formally reviewed to ensure that it does not compromise existing controls or adversely affect the risk profile.

4.1.16 Network management

4.1.16.1 Network security

The network servicing e-Gov must have clearly defined operational boundaries and managerial responsibilities. Each network segment should have no more than a single access point which should be regulated to prevent unauthorised traffic flow. The management of the network infrastructure, and the information processing facilities which rely on it, must be clearly separated but co-ordinated to ensure both optimised service to the business and consist deployment of security controls. Network traffic should be proactively scrutinised to ensure swift detection of unauthorised traffic and possible network intrusion. The MISO should ensure that network discovery and scanning tools are implemented to uncover anomalies, configuration errors, and network vulnerabilities that may ultimately undermine the security of IA within their Ministry and e-Gov.

4.1.17 Media handling and security

4.1.17.1 Media management

Procedures should be developed to secure media, input/output data, and documentation for information processing facilities from damage, theft and unauthorised access. Media must be securely decommissioned at the end of its lifecycle; note decommissioning does not necessarily mean destruction and disposal, this is particularly true for media containing cryptographic material.

4.6.7 Exchanges of information and software

4.1.17.2 Exchange

IAOs and IACs must ensure that the security afforded their IAs and software will not be diluted during the process, and as a consequence, of exchange with others within e-Gov and beyond. To this end, a SLA detailing

the means by which security services will be implemented must be in place prior to the exchange of assets. The SLA must clearly define boundaries of responsibility and address the issue of securely transferring assets across these boundaries. Furthermore, the SLA must define the process for resolving disputes.

The GISM will be accountable for defining a formal process an authorisation process for managing the release of IA into the public domain. The IAO will be accountable for ensuring adequate integrity protection for their asset as it crosses into the public domain.

Access control

4.1.18 Business requirements for access control

4.1.18.1 Fundamentals business requirement

Without the means to correctly attribute (in)actions to individuals it would be impossible to foster a culture of responsibility and accountability. Therefore, the ability to uniquely identify each and every individual user of an information processing facility is a fundamental e-Gov business requirement. The precise access control rules and rights for each individual user or group of users must be clearly defined by the IAOs.

Owners of business processes must identify all the IAs that are required in the fulfilment of their respective business processes and ensure that subsequent access rules and rights are aligned with those specified by the respective IAOs.

4.1.19 User access management

4.1.19.1 Registration

The GISM will be accountable for defining formal user registration, postponement, and deregistration procedures for granting access to information processing facilities. Subsequently, each individual must be assigned a unique user identity (UID) for use across e-Gov. Given that these UIDs effectively emerge into the public domain, it is trivial for one individual to claim to be someone else. To manage down the risk of masquerade, the means of authentication must reflect the classification profile of the IA for which access is sought; this is reflected in Table 2.

Classification	Authenticator
Extreme	Biometrics
High	Token and password
Medium	10 character password
Low	8 character password

Table 2: Which authenticator to use

The GISM will be accountable for defining secure authenticator life cycle procedures, this necessarily includes their generation, use, suspension, and decommissioning.

4.1.19.2 Access requirements

The granularity of control afforded by some information processing facilities is somewhat coarse. In order to understand and quantify the risk associated with excessive coarse access, it is important that the business process owner (BPO) documents the minimum access required to fulfil each process, and the roles permitted to perform these processes. The types of access are defined in Table 3.

Access type	Definition
Execute only	Invoke a process
Read	View an IA or file
Write	Alter an IA or file
Append	Add to the end of an IA or file
Create	Generate an IA or files
Delete	Remove an IA or file

Table 3: Access types

4.1.19.3 Authorisation to access

Employees should be informed of the type of access to information processing facilities for which they are authorised. The employee has a responsibility to communicate whether their rights are inadequate or excessive for the roles they fulfil.

Following successfully authentication, an individual's access rights must be bound to their unique UID. Access to information processing facilities must be conditional on an authorisation process. The authorisation process must verify whether the current access rights associated with the UID are sufficient to grant the requested access. Access rights must be regularly reviewed.

4.1.19.4 Privilege management

The allocation and use of privileges must be restricted and rigorously controlled. To this end:

- the minimum privileges required to perform each function of a information processing facility, or a component thereof, must be identified;
- privileges must be allocated on both a need-to-know and event-by-event basis, i.e. the minimum privileges required to fulfil a specific task are only made available for the time during which they are needed;
- an authorisation process and record of all privileges should be maintained and kept appropriately confidential;
- privileges should be assigned to a different UID from those used to conduct normal business processes.

4.1.20 Monitoring system access and usage

4.1.20.1 Event logging

Details of security relevant events and exceptions should be logged and maintained to assist in investigations and access control monitoring. As a minimum the following should be logged:

- UID
- dates and times of log-on and log-off
- terminal identity or location;
- details of successful and unsuccessful attempts to access information processing facilities and components;
- details of successful and unsuccessful attempts to access IA and other resources.

4.1.20.2 System usage

Procedures for monitoring information processing facilities should be established to ensure that users are constrained to those actions for which they have been explicitly authorised. The precise monitoring requirements must be agreed between the IAO and the BPO and formally recorded in a business audit requirements document. The following areas should be included:

- authorised access, including UID, type of event, associated files/resources, programs/utility used, etc.;
- privileged access, including use of supervisor account, system start/stop, device mount/unmount, etc.;
- unauthorised access attempts including alerts from intrusion detection systems, etc.;
- system alerts/failures including console messages, system log exceptions, network management alarms, etc.

Systems development and maintenance

4.1.21 Security requirements of systems

4.1.21.1 Security requirements

To ensure that the risk to IA is appropriately managed down, and that security is designed into information processing facilities from the outset, rather than bolted on at the end, IAOs and BPOs must engage their MISO at the requirements stage of their projects. To this end, the e-Gov Executive mandates that funding for each project is contingent on a formal risk assessment conducted by a MISO.

4.1.22 Security in applications

4.1.22.1 Correctness and completeness

BPOs will be accountable for demonstrating assurance in their processes by taking representative random samples of live information through the information processing facilities to detect corruption and identify possible exposure to compromise. Information processing facilities, and the combination thereof, must be independently audited prior to the release of new/revised business processes into a live operational domain.

4.1.23 Cryptographic control

4.1.23.1 Cryptographic infrastructure

Security is often compared to a chain in that it is only as strong as its weakest link. The rigorous application of security services will provide no protection if it is relatively easier to defeat the identification and authentication service. In many situations, cryptographic services provide a convenient cost effective means to secure IAs. However, too often insufficient attention is paid to the underlying key management infrastructure, which results in a grossly false sense of security. Therefore, the GISM will be held accountable for defining the cryptographic infrastructure and supporting operational procedures. These procedures must address the following:

- the process of selecting the most appropriate cryptosystem;
- cryptographic key generation;
- key storage;
- distribution of keys to identified intended recipients;
- key activation;
- recovery of lost or corrupted keys;
- key expiry;
- key replacement;
- dealing with suspected key compromise;
- emergency key revocation;
- key archiving;
- auditing of key management related activities.

The DDG will be held accountable for securely managing their Ministry's cryptographic material. The GISM will be responsible for providing fundamental cryptographic training and awareness. Delegation of responsibility and accountability for cryptographic material must be restricted to those who have completed appropriate training.

4.1.24 Security in development and support processes

4.1.24.1 Change control

In order to minimise the corruption and contamination of information processing facilities, there should be strict formal control over the implementation of change. A formal change request process must be established. Change requests are contingent on an analysis of their impact on the risk profile and must be approved by the local MISO.

Business continuity management

4.1.25 Aspects of business continuity management

4.1.25.1 Business continuity management process

The GISM will be held accountable for establishing a business continuity management process, this will require access to specialist resource which may only exist beyond e-Gov. To this end, MISOs, who lead the risk assessments for business processes, will be held accountable for informing their DDG of the continuity (availability) requirements for each of the Ministry's business process, and their subsequent dependencies on information processing facilities. The DDG will be held accountable for prioritising and formally communicating their Ministry's continuity requirements to the GISM, and back to the relevant BPO. This should help ensure that there is no confusion as to the order in which business processes are maintained/recovered.

4.1.25.2 Supplementing business risk assessments

The aim of the risk assessments conducted for business processes accessing IAs is to identify a profile of security controls that proactively manages down the current risk profile to an acceptable risk profile. It is unlikely that those conducting these risk assessments will have in depth knowledge of the specific vulnerabilities to environmental threats, and hazards. Therefore, the business continuity process should identify the events that could result in interruptions to business processes, e.g. equipment failure, fire, flood, social unrest, utility failures, etc. The vulnerability to these events along with the potential impact on all business processes and related information processing facilities must be determined. The results of this overarching risk assessment must drive the strategic business continuity plan, from which the GISM's business continuity management process is formed. (The development of the strategic business continuity plan is likely to require specialist resource from beyond e-Gov.)

4.9.1.3 Business continuity plans

Individual plans should be established to maintain or restore specific (families of) business operations in a timely manner following interruption to business processes. These plans should:

- define roles and responsibilities;
- identify and cater for external and internal dependencies;
- document emergency procedures;
- identify training and awareness requirements;
- be regularly tested, reviewed, and revised.

Compliance

4.1.26 Compliance with legal requirements

4.1.26.1 Applicable legislation

The e-Gov executive will be held accountable for ensuring that all relevant statutory, regulatory, and contractual requirements are identified in a timely manner. The e-Gov Executive is further responsible for documenting their interpretations of these requirements. Thereafter, the roles and responsibilities for ensuring appropriate compliance will be identified and empowered accordingly.

4.1.27 Review of security policy and technical compliance

4.1.27.1 Compliance with information security policy

BPOs, IAOs, and IACs should ensure that all security relevant procedures within the scope of their responsibility are documented and kept appropriately accessible. Their level of compliance with the ISP and subsequent standards, guidelines, procedures, best practice, etc. will be subject to regular review.

4.1.27.2 Technical compliance

In order to determine the acceptability of the operational risk profile, information processing facilities should be regularly checked for compliance with the ISP and subsequent standards, guidelines, procedures, best practice, etc. To this end, checks on information processing facilities build specification, configurations, and access rights will determine whether they are excessive. These checks should include penetration tests, and an appropriate element of social engineering.

4.1.28 System Audit Considerations

4.1.28.1 System audit controls

To minimise the risk of disruption of to business processes and information processing facilities, audit reviews must be carefully planned. To this end:

- audit requirements should be agreed with the appropriate management;
- the scope of the agreed audit checks controlled;
- reviews of information processing facilities should be restricted to read-only access;
- all audit accesses should be logged and monitored to ensure they do not exceed agreed scope;
- all procedures, requirements, and responsibilities should be documented.

4.1.28.2 Audit tools protection

Audit tools can be compromised and misused which may undermine the security, therefore, access to these tools must be rigorously controlled. To this end, they must be kept isolated from development and operational information processing facilities. They may only be held in shared software repositories, or user areas, if they have been adequately secured to prevent unauthorised access.