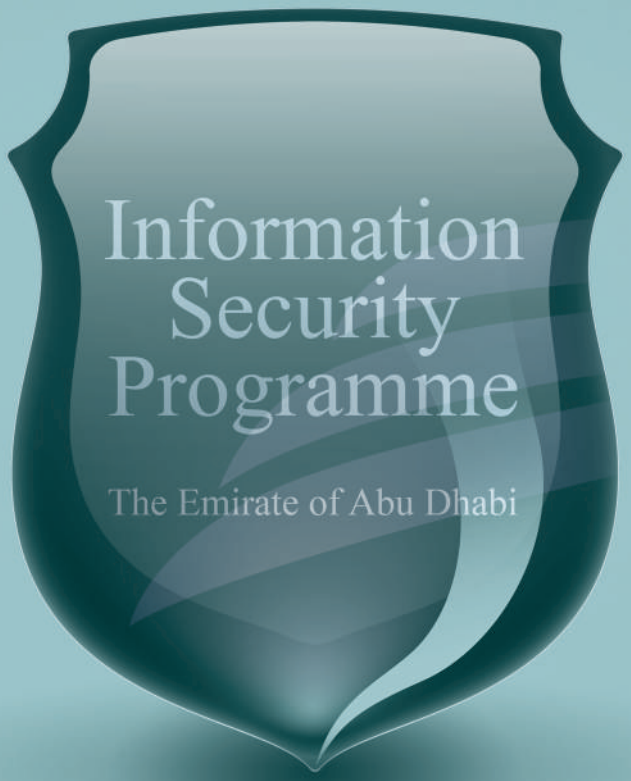
مركز أبوظبي للأنظمة الإلكترونية والمعلومات
Abu Dhabi Systems & Information Centre



GUIDE

INFORMATION SECURITY PLANNING

Version 1.0

أبوظبي
abudhabi

INFORMATION SECURITY PLANNING

GUIDE

DOCUMENT CONFIGURATION CONTROL

VERSION	RELEASE DATE	SUMMARY OF CHANGES	RELEASE APPROVAL
Version 1.0	15 March 2009	Initial Release	ADSIC, Information Security Team

Document Location

- Abu Dhabi Portal (electronic copy)
- ADSIC Portal and Office (electronic copy and hard copy)

Questions or Comments

Any questions or comments regarding this document should be directed to:
support@adsic.abudhabi.ae

Contents

1. INTRODUCTION

1.1 OVERVIEW

Information Security Planning is the second phase of the Risk Management process. This document is intended as a guide for developing an Information Security Plan (ISP) for services and their supporting systems of the Abu Dhabi Government Entity (ADGE). The intention of such a plan is to protect ADGE information within the service commensurate with the risk and magnitude of harm that could result from the loss, misuse, unauthorised access to, or modification of such information.

This document provides guidance on how to specifically select controls to address the security risks and how to develop and follow a plan that documents the implemented and planned controls for an information system and the information contained within the system. Since Information Security Planning is an ongoing process that reflects any changes made to the organisation or service, security issues should continue to be identified and addressed as the risk environment evolves.

The Risk Management process is the conduit to appropriately applying the Abu Dhabi Information Security Management and Functional processes, requiring that ADGEs protect Government information commensurate with the risk and magnitude of harm that could result from its loss, misuse, unauthorised access, or modification. The Risk Management process can be broken down into four phases, as shown in Figure 1:

Figure 1: Four Phases of the Risk Management Process and Supporting Guides

The *Abu Dhabi Information Security Planning Guide* is supported by additional accompanying Risk Management guidance *(e.g., Risk Assessment Guide, Security Testing & Evaluation (ST&E) Guide, Technical Testing Guide, Information Security Standards, and the Certification & Accreditation (C&A) Guide*[1]) and training. These documents will provide the necessary guidance to help entities appropriately determine their risk profile, select mitigating controls, verify and validate those controls as necessary, and ultimately certify and accredit that their services are adequately secure. For a complete explanation of the Abu Dhabi Systems & Information Centre (ADSIC) Risk Management process, please refer to the *Abu Dhabi Risk Management Guide.*

1.2 SCOPE

The functional scope of the *Abu Dhabi Information Security Planning Guide* centres on information security looking beyond the traditional focus of information technology. This ensures that sensitive Government information is protected throughout its lifecycle within a service, not just in the systems where data is processed. In addition, Abu Dhabi fully recognises the importance of developing such a programme in coordination and integration with the related assurance disciplines of physical

[1] *ADSIC will, over time, develop additional procedural and functional guidance across the information security domain.*

security, personnel security, business continuity, and cross-functional risk management, and the importance of directing the programme to assure Government missions rather than only information technology. Each of these related assurance disciplines are included within this programme, and contain specific activities to ensure integration under a mission assurance umbrella.

1.3 APPLICABILITY

The *Information Security Planning Guide* applies to Abu Dhabi Government personnel, contractors, and third party organisations and individuals[2]. This encompasses all information and information technology assets to include hardware, software, media, facilities, data, and electronically stored information that may be owned, leased, or otherwise in the possession, custody, or control of the Abu Dhabi Government.

1.4 COMPLIANCE AND ENFORCEMENT

Per *Abu Dhabi Information Security Policy,* compliance with the Risk Management process is mandatory[3] and Information Security Planning is a key part of the process. The successful implementation of security controls across the Government of Abu Dhabi can only be fully effective when all stakeholders operate in a consistent manner and follow this process. This means that the entire Government workforce must act responsibly.

Personnel and entities found to be non-compliant with this *Abu Dhabi Information Security Planning Guide* may have their access to information systems revoked and may be subject to disciplinary actions and legal prosecution as supported by existing laws and policies of the United Arab Emirates (UAE) and Abu Dhabi (e.g., the UAE Cyber Laws). Services that fail to comply with this document may not be allowed to process Government information.

Enforcement and monitoring of these standards is a shared responsibility of ADSIC, each Government entity's Chief Information Security Officer (CISO), and the Abu Dhabi Accountability Authority.

1.5 DOCUMENT LAYOUT

The document will provide the reader with the information and tools needed to adequately plan security controls for a Government service and its supporting systems. It is divided into three main sections:

- **Section 1** provides the overview, background, and purpose of this document, and answers the question, "Why conduct Information Security Planning?"
- **Section 2** provides answers to frequently asked questions about information security and some of its key components.
- **Section 3** provides a step-by-step guide to conducting Information Security Planning, and answers the question, "How is Information Security Planning conducted?"
- **Appendices** provide information to support the Information Security Planning process, including a template that can be used to complete the Information Security Planning steps in Section 3.

---

[2] *This document applies to civilian Government organisations only; intelligence/military services are excluded.*

[3] *Consistent with the overall concept of risk management, the implementation of controls shall be done in consideration of the System Owner's view of acceptable risk. Deviations from the Abu Dhabi security controls and processes are acceptable when residual risks are formally accepted by the System Owner through the Risk Management process.*

2. FREQUENTLY ASKED QUESTIONS

2.1 WHY CONDUCT INFORMATION SECURITY PLANNING?

Abu Dhabi's Information Security Policy requires risk assessments to be performed as part of the mandatory adoption of a Risk Management process for all services and their supporting systems. Benefits of performing risk assessments include:

- Identifying weaknesses in Government services as well as the underlying IT infrastructure
- Enabling management to make informed decisions on the implementation of security controls and remediation measures
- Promoting a consistent approach to measuring risk
- Allowing stakeholders to place values on potential losses

Information Security Planning is the second phase of the Risk Management process and follows the Risk Assessment phase. During the second phase, the Information Security Planning process intends to identify and select risk mitigation routes to reduce, avoid, transfer, or accept risks. A detailed Information Security Plan is developed to address the problems identified during the risk assessment.

2.2 WHEN SHOULD INFORMATION SECURITY PLANNING BE CONDUCTED?

Information Security Planning is a continuous process that addresses risks identified through risk assessments or any other means. Government services are continuously evolving to meet the requirements of their organisation, and as their components change and new functionalities are added, new risks are introduced. These changes may warrant a risk assessment to be conducted outside of the normal cycle. Even if a risk assessment is not triggered, the Information Security Plan should be updated to reflect the changes and their impact on currently implemented security controls.

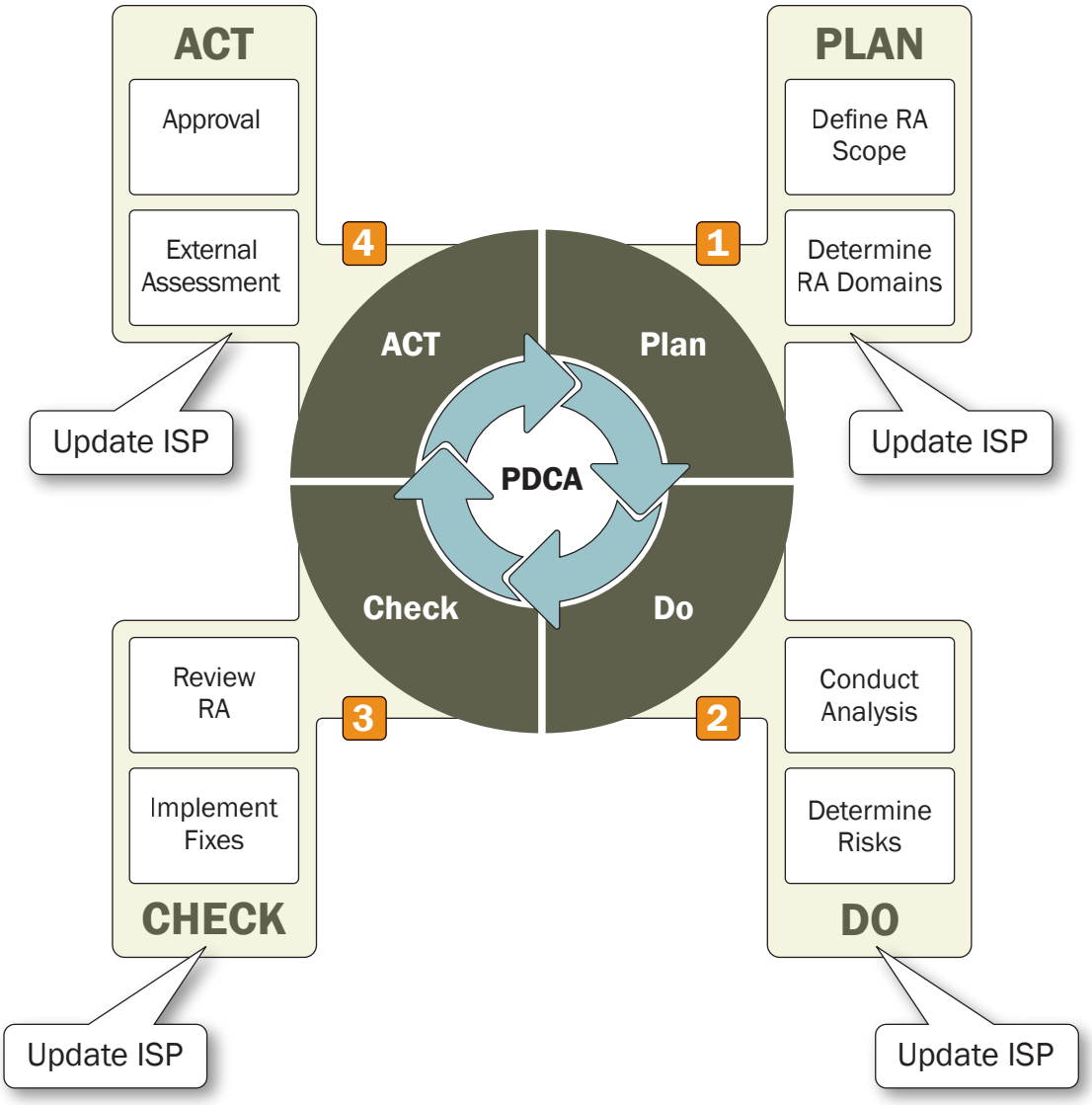


Figure 2: The Risk Management process and Information Security Plan Update

2.3 HOW MUCH TIME DOES INFORMATION SECURITY PLANNING TAKE?

The time needed for Information Security Planning depends on the service and its supporting systems in review. A complex service will take more time to evaluate than a relatively simple service. During the Risk Assessment phase, the services have been assigned a risk level designation, ranging from 'LOW' to 'HIGH'. This categorisation provides a rough guideline for the time needed for Information Security Planning, whereby a service categorised as 'HIGH' would require more time for its Information Security Planning and would need to be reviewed more frequently than a service categorised as 'LOW'.

2.4 WHAT IF RISKS DO NOT HAVE ADEQUATE CONTROLS?

In case the entity is unable to identify adequate controls during the Information Security Planning phase for risks identified during the Risk Assessment phase, it could do one of the two things: either accept the risk or avoid it by not offering the specific service for which the risk exists. Please refer to section 3.4 for further information.

2.5 WHO IS RESPONSIBLE FOR PERFORMING INFORMATION SECURITY PLANNING?

Information Security Planning is the responsibility of the System Owner. While the System Owner may delegate various tasks to individual parties, he/she is ultimately responsible and accountable for control implementation and security. Please refer to the *Risk Management Guide* for detailed overview of all applicable roles and responsibilities.

2.6 HOW DOES INFORMATION SECURITY PLANNING RELATE TO THE ISO/IEC 27001:2005 STANDARD?

ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System (ISMS) within the context of an organisation's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of an individual organisation or its parts.

A key component in establishing the Information Security Management System is to incorporate a Risk Management process. Since Information Security Planning is a step in the Risk Management process, it is required to be implemented and demonstrably operated to realise the benefits of implanting the ISO/IEC 27001:2005 standard.

2.7 WHAT ARE SECURITY CONTROLS?

Security controls are actions, devices, procedures, techniques, or other measures that intend to reduce the risks associated with an information system. The term itself is synonymous with countermeasures and safeguards.

2.8 WHAT ARE CONFIGURATION SETTINGS AND PATCHES?

Software configuration settings allow information systems to be configured in a specific manner to meet organisational needs, and often impact on the security posture. Default configuration settings are often insecure, providing services that may not all be required by the organisation and are often used for backward compatibility. These types of vulnerabilities can be detected by automated scans and may be corrected by changing software parameters.

Software programmes are complex and are littered with bugs and flaws that introduce vulnerabilities into the system where the programmes reside. These vulnerabilities are frequently detected after the software has been released—sometimes years afterward. When these vulnerabilities are detected, vendors investigate the cause and fix them. Theses fixes, issued as patches, usually require a considerable amount of time to implement. Once a patch is made available, it must be applied to eliminate the vulnerability.

3. INFORMATION SECURITY PLANNING STEPS

3.1 METHODOLOGY

This section of the document provides a logical flow that represents the order in which Information Security Planning steps should be followed. The process is divided into eight steps:

STEP 1: Determine Risk Treatment Priority

STEP 2: Identify Potential Controls

STEP 3: Determine Cost-Effective Controls (Optional)

STEP 4: Determine Mitigation Route and Select Controls (Optional)

STEP 5: Assign Responsibility and Schedule Implementation

STEP 6: Implement Controls

STEP 7: Verify Control Implementation

STEP 8: Develop Information Security Plan

All of these steps are mandatory except 3 and 4, and each is reliant upon output from the previous step and should be done in sequence. Figure 3 depicts the Information Security Planning process.

At the end of this Information Security Planning exercise, two deliverables will be produced, the Risk Treatment Plan and the Information Security Plan (ISP). The output of the first 7 steps should be captured in the template provided in Appendix D of this document, that will result in the risk Treatment Plan. Step 8 will produce the Information Security Plan (a template is provided in Appendix E), taking the information captured in the Risk Treatment Plan and conducting interviews with administrator and developers to obtain additional information. The guidance for conducting each step is provided in this document, with specific reference to the key inputs and outputs that are expected for each step. A worked example[4] is also provided to demonstrate outputs for each step and a snapshot of this example is provided at the end of each step that shows the completed information.

[4] *The worked example is based purely on fictional data, and any resemblance to real services is coincidental.*

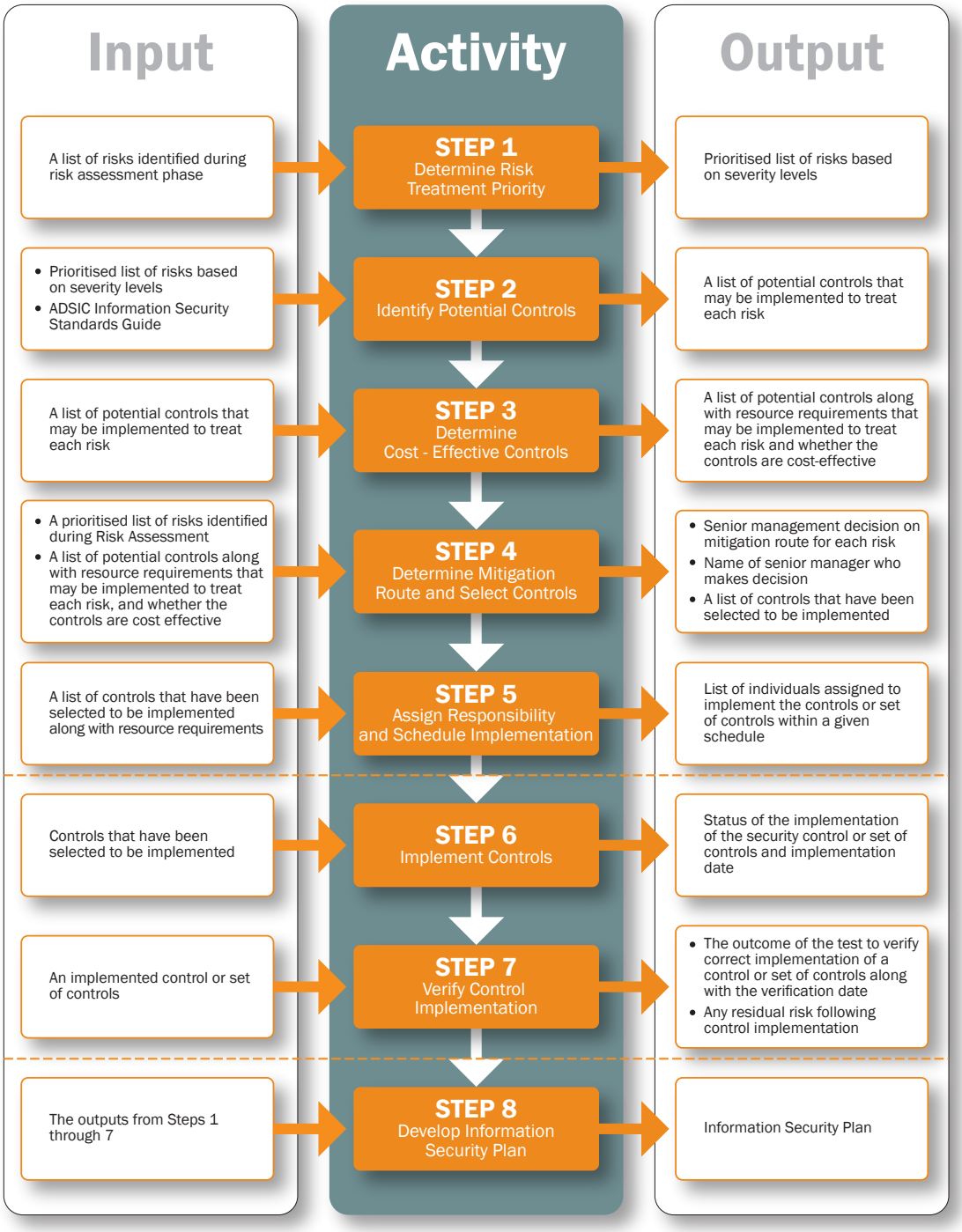


Figure 3: Information Security Planning Process Steps

3.2 PLAN RISK TREATMENT

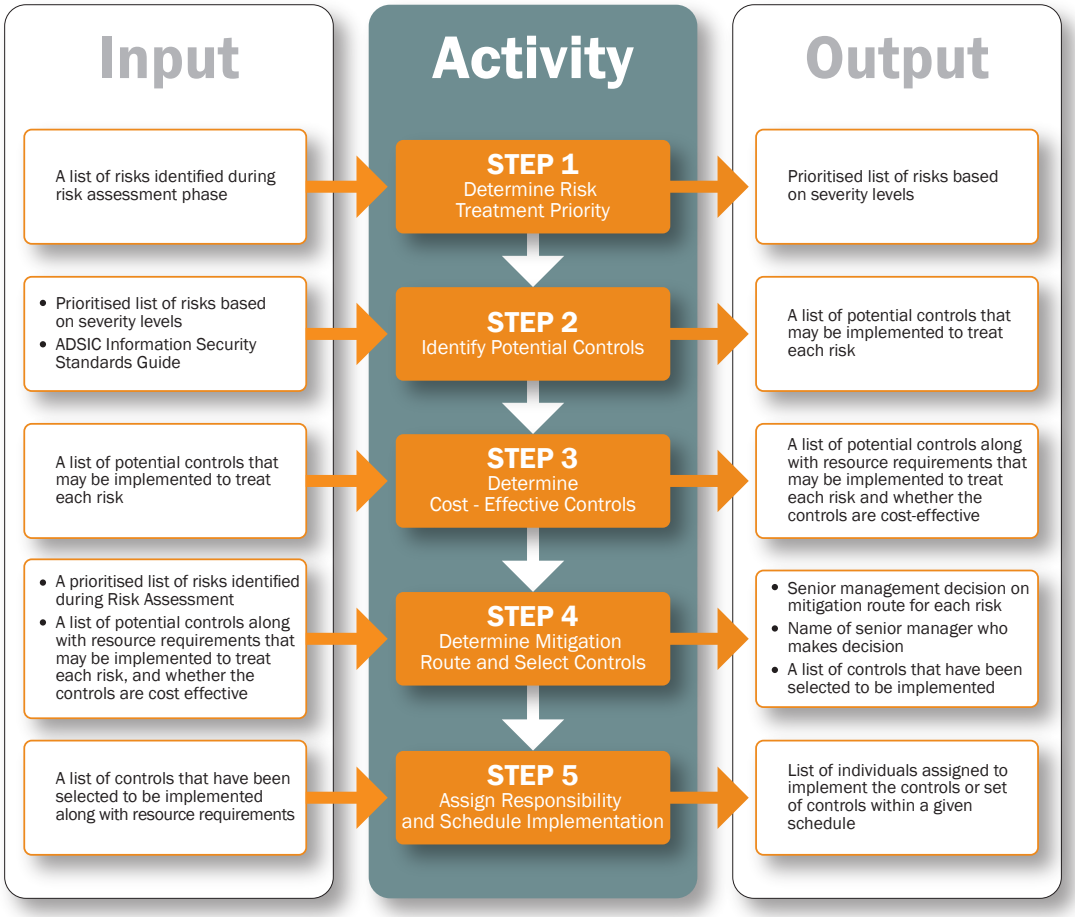


Figure 4: Plan Risk Treatment

STEP 1: Determine Risk Treatment Priority

Step 1 Input: *A list of risks identified during the Risk Assessment phase*

Severity levels defined at the end of the Risk Assessment phase for each of the identified risks will determine the prioritisation of risk treatment, which is achieved through Information Security Planning.

The use of risk severity levels ensures that risks requiring urgent treatment are given higher priority, allowing for the optimisation of resources in order to address the most urgent risks first. Later on in the Information Security Planning process, namely during Step 5, the implementation of controls is scheduled.

The following figure illustrates these risk severity levels. Risks with higher severity levels should be treated before ones with lower severity levels. For example, a risk with a severity level of 6 should be treated before a risk with a severity level of 5.

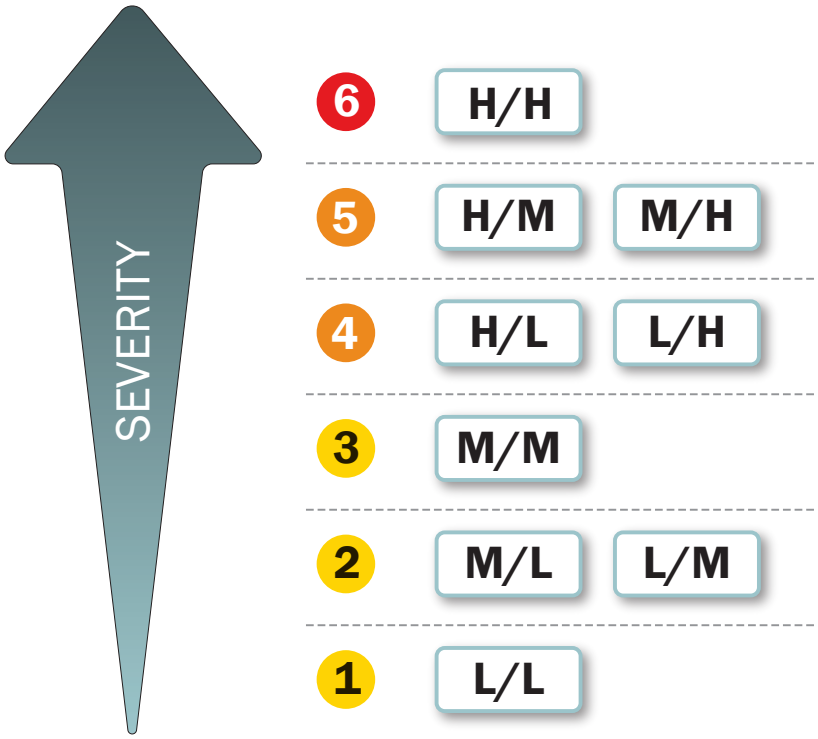


Figure 5: Risk Severity Levels

If multiple risks have the same severity level, other factors may be taken into account to prioritise treatment—such as the estimated level of skills and the cost to mitigate the risk. These adjustments will be made during Steps 6 and 7 of the Information Security Planning phase and will be reflected in the scheduled implementation dates.

Step 1 Output: *Prioritised list of risks based on severity levels*

Figure 6: Prioritise Risks

STEP 2: Identify Potential Controls[5]

Step 2 Input:

- *Prioritised list of risks based on severity levels*
- *Abu Dhabi Information Security Standards Guide*

Once the risks stemming from the Risk Assessment are prioritised, security controls to treat the identified risks need to be identified. The first action is to understand the risk and determine a set of possible security controls that would mitigate the risk.

NEW OR ENHANCED CONTROLS MITIGATE RISK BY:
Eliminating vulnerabilities (weaknesses or flaws) ▪ Example: Patching servers
Reducing capacity or motivation of the threat source ▪ Example: Increasing cost of compromise vs. value of gain for the attacker
Reducing the magnitude of an adverse impact ▪ Example: Backing up data or maintaining an alternate processing site

Table 1: Determine Mitigation Steps

[5] *This step focuses on the reduction of a risk and to a lesser degree discusses risk avoidance. A risk mitigation route will be selected later in this process that includes reduction, avoidance, acceptance, or transfer based on the cost-benefit analysis of controls identified in this section.*

Additionally, the following table shows conditions and responses as they are encountered during control identification.

CONDITION	RESPONSE
When a vulnerability exists	Implement controls to reduce the likelihood of a vulnerability being exercised
When a vulnerability can be exercised	Apply layered protections, architectural designs, and administrative controls to minimise the risk of, or prevent, this occurrence
When the attacker's cost is less than the potential gain	Apply protections to increase the cost of an attack and to limit potential gain (e.g., use of system controls such as limiting what a system user can access and do)
When loss is too great	Apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, reducing the potential for loss

Table 2: Example Conditions and Resposes

In order to identify the appropriate mitigation for a risk, it is necessary to determine the object/component that needs protection, the vulnerability, and the source of the threat. All of these pieces of information are identified in the Risk Assessment. These three pieces of information will help identify the type of control[6] that will need to be implemented and whether the required solution is going to be technical or not.

Once the asset and its associated vulnerabilities are identified, the level of protection required for the asset will need to be determined. The likelihood and the impact levels will drive the protection level required. Likelihood is the probability that the vulnerability will be exercised, and impact level indicates the extent of the damage that will result. The impact of the attack is defined in terms of confidentiality, integrity, and availability and helps determine which area requires the most focus.

Some risks may require technology- or platform-specific controls for treatment (e.g., a Web application or Microsoft Windows); these could include the insecure implementation and configuration of software. Such vulnerabilities need to be addressed by applying patches and changing configurations to a more secure state.

Feasibility and effectiveness of controls should be evaluated to ensure that identified controls are compatible with the environment and do not hinder the entity's mission. The controls need to be evaluated to ensure that the degree of protection is commensurate with the security requirements of the service and its supporting systems (*see Figure 7*). Security control identification should be made with the entity's mission in mind. The impact that security controls have on productivity should be minimised, making the implemented control as transparent to users as possible.

[6] *Risks and security controls do not always have a one-to-one ratio. A single control can mitigate multiple risks, and multiple controls may be required to mitigate a single risk.*

Figure 7: Control Feasibility and Effectiveness

When identifying security controls to mitigate risks, the entity should consider management and functional processes. A security control is developed to improve the information system's security posture. These controls can be then broken down further into detective, preventative, and corrective controls:

- **Detective –** These controls aim to detect events, such as security incidents.
- **Preventative –** These controls aim to prevent events from happening, such as a security breach. Many of these controls can also be categorised as deterrent controls that discourage undesirable actions.
- **Corrective –** These controls come after the fact and are activated when an incident has taken place and are normally used in conjunction with detective controls. Many of these controls can also be categorised as recovery and are manually conducted as opposed to automated.

	DETECTIVE	PREVENTATIVE	CORRECTIVE
MANAGEMENT	Review violation reports	Background checks	Termination of employee
FUNCTIONAL	Motion detectors	Media sanitisation	Fire suppression

Table 3: Examples of Controls

The Risk Assessment process may involve the use of vulnerability and penetration testing tools, with output that entails a report containing recommended technical controls for each finding (e.g., patch upgrade recommendation, blocking access to a particular port, etc.). Each of these technical controls should be reviewed for feasibility and effectiveness. For example, a recommended operating system patch upgrade may have compatibility issues with certain applications residing on a server. This type of review can be facilitated by using information found on knowledge bases such as Mitre's Common

Vulnerabilities and Exposures (CVE[7]) and the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD[8]). The figure below depicts the patch management cycle.

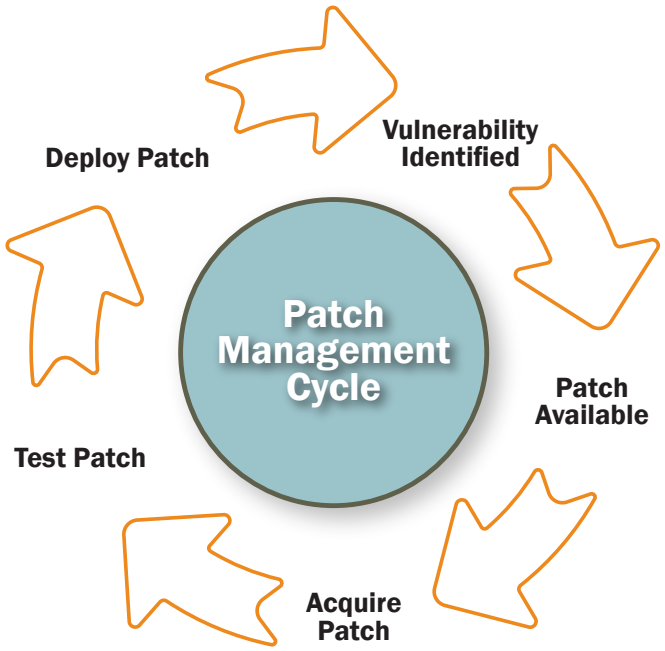


Figure 8: Patch Management

All services must be compliant with the security controls listed in the *Abu Dhabi Information Security Standards.*

Management Security Controls

Management security controls are in the form of policy, guidelines, and standards that organisations implement, and are executed through operational processes and procedures.

A full set of applicable controls is found in the *Abu Dhabi Information Security Standards.* The following is a list of examples.

Management detective controls include:

- **Background checks –** The process of conducting background investigations (usually involving official and commercial records about a person) of employees/contractors before hiring or granting access to sensitive information (Control Standard **HR-8.1.203**).
- **Risk assessments –** The process of analysing threats and vulnerabilities of an information service, and the potential impact resulting from the service's loss of information or capabilities. This analysis is used as a basis for identifying appropriate and cost-effective security controls (Control Standard **RM-3.1.103**).

[7] *Common Vulnerabilities and Exposures (CVE) is a dictionary of common names (i.e., CVE identifiers) for publicly known information security vulnerabilities. The entire dictionary is publicly available at http://cve.mitre.org/.*

[8] *NVD is the U.S. Government repository of standards-based vulnerability management data. It has a great deal of information about vulnerabilities, mitigations, and incompatibility issues. Its database is publicly available at http://nvd.nist.gov/.*

Management preventative controls include:

- **Assignment of responsibility –** The assignment of security responsibility to individuals to ensure accountability by requiring specific actions to be undertaken to maintain the security posture of the service (Control Standard **HR-8.1.103**).
- **Development of security plans –** The formulation of plans to determine and document the current security posture of a service and plan improvements (Control Objective **SP-1.3**).
- **Segregation of duties –** The principle requiring that no single user has the access to carry out a sensitive transaction without being noticed. Multiple user involvement serves as both a deterrent and multiple points of failure for an undesirable activity (Control Standard **CM-10.1.303**).
- **Least privilege –** The principle requiring that each subject be granted the most restrictive set of privileges needed for the performance of authorised tasks. Application of this principle limits the damage that can result from accident, error, or unauthorised use of an information system (Control Standard **IA-11.2.203**).
- **Rules of behaviour –** Rules established to ensure that users are aware of the expectation of responsibility and accountability with regard to information and information system usage (Control Standard **AM-7.1.303**).

Management corrective controls include:

- **Business Continuity Management –** Plan for continuing of an organisation's essential functions at an alternate site and performing those functions for the duration of an event with little or no loss of continuity before returning to normal operations (Control Standard **BC-14.1.103**).
- **Incident response plans –** Processes and procedures that ensure proper steps are taken to limit damage when an incident occurs, and which determine the cause and prevent similar future events (Control Standard **IM-13.2.103**).
- **Security planning –** The process of planning, implementing, testing, and documenting security controls of an information service and ensuring adequate security (control objective **RM-3.1**, **RM-3.2**, **RM-3.3**).

Functional Security Controls

Functional security controls are primarily implemented 'around the system' to ensure a secure functioning of that system. They are implemented to address functional deficiencies and environmental threats that could be potentially targeted. To ensure consistency and uniformity, these procedures are defined, documented, and maintained.

A full set of applicable controls is found in the Abu Dhabi Information Security Standards. Examples include:

Functional detective controls include:

- **Audit logging –** The system-generated chronological record of system activities that enables reconstruction and examination of a sequence of events (Control Standard **CM 10.10.203**).
- **Intrusion detection systems –** Intrusion detection systems (IDS) are used to detect behaviours/attacks that can compromise the security of a computer system. These can include network attacks against vulnerable services, data-driven attacks on applications, unauthorised logins/access to sensitive files, and malware (e.g., viruses, Trojan horses, worms). IDS is a component of boundary protection (Control Standard **IA-11.4.603**).

- **Virus or malware detection software –** Also known as antivirus software. These are computer programmes that attempt to identify, neutralise, and eliminate malicious software. Today's antivirus software is designed to combat a wide range of threats, including worms, rootkits, Trojan horses, and other malware (Control Objective **CM-10.4**).
- **Intrusion alarms –** Electronic devices that detect motion in a specific area and alert of an intrusion (Control Standard **PE-9.1.303**).
- **Surveillance equipment –** A system comprised of video cameras and/or digital video recorders to conduct surveillance of a specific area such as a data centre (Control Standard **PE-9.1.303**).
- **Smoke detectors –** Electronic devices that detect fire or smoke in an area such as a data centre (Control Standard **PE-9.1.503**).
- **Change management –** Process of controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications prior to, during, and after system implementation (Control Standard **CM-10.1.203**).

Functional preventative controls include:

- **Access controls –** Access controls limit access to information system resources to authorised users, programmes, processes, or other systems. These controls are implemented through methods such as role-based access controls, mandatory access controls, attribute-based access controls, etc. (Control Objective **IA-11.4**).
- **Identification and authentication –** Identification is the process of identifying a valid user, and authentication is the process of verifying the user's claimed identity (Control Standard **IA-11.5.203**).
- **Cryptography –** A method of hiding information through crypto-algorithms by an information system to authenticate users or to ensure confidentiality and/or integrity of information (Control Standard **IS-12.3.103**).
- **Communication protection –** The process of protecting the integrity and confidentiality of information in transit, usually through use of cryptography (Control Objective **IS-12.3**).
- **Media handling and labelling –** The processes and procedures put in place to ensure that media are labelled according to sensitivity of data stored and handled to prevent unintentional disclosure (Control Standard **CM-10.7**).
- **Media sanitisation –** The processes and procedures put in place to ensure that media is disposed of or reused in a secure manner to prevent inadvertent disclosure (Control Standard **CM-10.7.203**).

Functional corrective controls include:

- **System restore –** System Restore is a component of Microsoft's Windows XP and Windows Vista operating systems that allows for the rolling back of system files, registry keys, installed programmes, etc., to a previous state in the event of a failure. Third party tools can also be used to perform similar functions for other operating systems (Control Standard **CM-10.5.103**).
- **Fire Suppression System –** This is triggered by a fire and aims to suppress that fire by means of sprinkler installation, fixed fire hoses, handheld fire extinguishers, etc. (Control Standard **PE-9.1.503**).

Step 2 Output: *A list of potential controls that may be implemented to treat each risk*

- Controls to be implemented. May contain multiple options at this point.
- Any recommendation made during the Risk Assessment process should be evaluated for feasibility and effectiveness.

PLAN RISK TREATMENT	
STEP 1	STEP 2
DETERMINE TREATMENT PRIORITY	MITIGATION OPTIONS/ POTENTIAL CONTROLS/ EXISTING CONTROLS
6	Option 1: Work with HostingCo to install a dedicated switch for our servers. Option 2: Bring operations in-house.
5	Implement access control that uses usernames and passwords to authenticate users.
5	Implement role-based access control that follows least privilege principles.
4	Configure terminal services to terminate session after 15 minutes of inactivity.

Figure 9: Identify Potential Controls

STEP 3: Determine Cost-Effective Controls (Optional)

Step 3 Input: *A list of potential controls that may be implemented to treat each risk*

Once all security controls are identified and their feasibility and effectiveness evaluated, a cost-benefit analysis is conducted to assist management in decision making and to identify cost-effective controls.

A cost-benefit analysis can involve tangible or intangible factors. Tangible cost can be further broken down into direct and indirect costs. Labour, hardware, and software are examples of direct costs. Indirect costs could include staff retraining and the development of customer awareness programmes.

Intangible factors are those that have impact on productivity, usability, or marketing efforts. For example, enabling of certain controls could result in a performance hit, reducing productivity. Intangible costs are usually difficult to gauge, but must be taken into consideration while conducting cost-benefit analysis.

The overall objective of cost-benefit analysis is to compare the cost of implementing versus not implementing a control.

During this step, sufficient information should be gathered to determine resource requirements for treatment of the risk and maintenance of the corresponding control. These resource requirements include not only the costs associated with hardware/software purchases and labour, but also those associated with maintaining the control once it is implemented—usually noted in terms of annual cost. Not all controls have associated maintenance costs, but dedicated security hardware and software implementation of controls can be costly from a maintenance standpoint, requiring the hiring of new staff or outsourcing. Without up-to-date maintenance, not only will the initial investment not produce the desired security results, but it may also have negative impacts. For example, any unpatched device will introduce new risks to the network and its information systems.

While performing a cost-benefit analysis, the following should be taken into consideration:

- Impact, to the entity, of implementing the control
  - Tangible costs of control implementation, such as: software/hardware costs; labour to implement the control, including policy development; training costs, including staff and implementation personnel; and maintenance costs
  - Intangible costs of control implementation, such as: reduced productivity due to performance of information system; and reduced productivity due to lack of user friendliness/acceptance
- Impact, to the entity, of ***NOT*** implementing the control, which is a further refinement of the impact analysis performed during the Risk Assessment phase:
  - Tangible costs of not implementing the control, for example: replacement of the physical asset, such as hardware/software; replacement of data; and lost revenues.
  - Intangible costs of not implementing the control, such as: impact on the organisation's reputation; impact on customer/user perceptions; and reduced revenues.

The below figure presents a commonly used formula to determine the value of a particular control to a company, taking into account the level of risk mitigation provided and the annual cost of the control. This formula's one drawback is that it is purely intended for quantitative analysis.

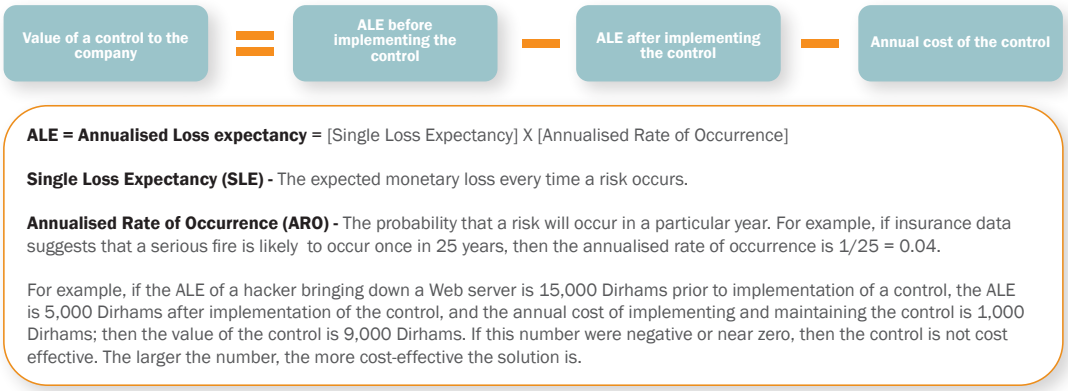


Figure 10: A Commonly Used Cost-Benefit Calculation for a Given Control

Decision makers must determine what constitutes an acceptable level of risk, which will directly feed into the selection of a particular control.

It is usually neither practical nor cost-effective to implement controls to completely eliminate all risks. The risks that remain after the implementation of controls are known as "residual risks." For example, if a username and password are used to identify and authenticate users, a user may select a weak password. If no further controls are put in place, this would be considered a residual risk. If the system is configured to enforce complex passwords, it will address the weak password issue but increase the likelihood that users may not remember their passwords and write them down.

Controls mitigate risks by reducing the number of vulnerabilities, reducing capacity or motivation of threat source, and reducing the magnitude of the adverse impact. Any gaps in the control which do not fully address the vulnerability will lead to residual risks as shown in the diagram below.

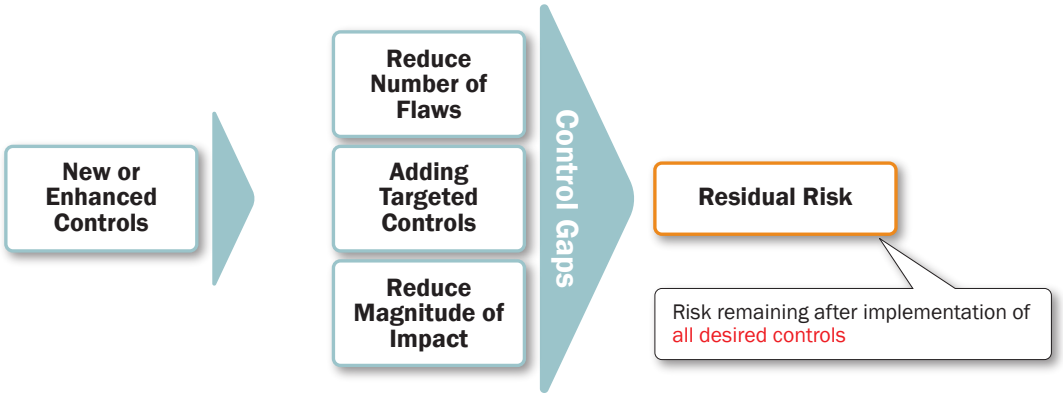


Figure 11: Residual Risk

A control is determined to be cost-effective if the cost of implementing and maintaining it, is economical in relation to the risk that is being mitigated.

Step 3 Output: *A list of potential controls with resource requirements that may be implemented to treat each risk, and a determination of whether the controls are cost-effective*

- Required resources will be determined during the cost-benefit analysis
- Determine if an available control is cost-effective

	PLAN RISK TREATMENT	
✓ STEP 2	STEP 3	
MITIGATION OPTIONS/ POTENTIAL CONTROLS/ EXISTING CONTROLS	RESOURCES REQUIRED	CONTROL COST-EFFECTIVE
Option 1: Work with HostingCo to install a dedicated switch for our servers. Option 2: Bring operations in house.	Option 1: A few days of meeting and senior management involvement may be necessary. Approximate Cost = $2000. Option 2: Extensive Operation, hire multiple employees/Hardware/ Software Purchase. Approximate Cost = Over $100,000	Option 1: Yes Option 2: No *Note: Assuming the cost of the risk is estimated at $5000.*
Implement access control that uses usernames and passwords to authenticate users.	3 Days of DBA time.	Yes
Implement role-based access control that follows least privilege principles.	3 days of admin time, System Owner, and business operational users involvement.	Yes
Configure terminal services to terminate session after 15 minutes of inactivity.	2 hours of admin time.	Yes

Figure 12: Determine Cost-Effective Controls

STEP 4: Determine Mitigation Route and Select Controls (Optional)

Step 4 Input:

- *A prioritised list of risks identified during the Risk Assessment*
- *A list of potential controls with resource requirements that may be implemented to treat each risk, and whether the controls are cost-effective*

Senior management will decide on the appropriate route to take based on the cost-benefit analysis performed in the previous step. Mitigation options include:

- **Reduce –** Apply controls to reduce the likelihood and impact of the risk.
- **Avoid –** Apply alternative methods of achieving the business objective and consider the business impact of not providing the service. For example, a risk could be avoided by designing the system so that the functionality that enables the risk to exist is removed or disabled.
- **Transfer**[9] **–** Apply methods of transferring the risk (e.g., insurance). However, even if the responsibility for limiting the risk is transferred outside an organisation, the risk will still rest wherever the business impacts are actually felt.
- **Accept –** Accept the risk. This is a viable option when the economic benefits of accepting the risk outweigh the costs involved of the risk actually materialising. It should be noted that accepting a risk does not mean that no further action is required but it means that other measures will be needed to identify when the risk is being realised.

It is necessary for the appropriate level of management to be involved in security control selection, not only for successful implementation of the control, but also to ensure that an organisation-wide perspective is provided. The cost-benefit analysis performed in Step 3 should form the basis for a management decision to determine control selection.

Controls selected should combine functional and management elements to ensure adequate security for the Government service. For example, if username- and password-based authentication is implemented, a policy can be developed to warn users of sharing passwords, reducing the residual risk.

The rules below should be followed to ensure that the most cost-effective control is selected. NOTE: The examples given consider an identification and authentication mechanism for a system that is categorised as 'LOW'.

- If a control reduces the risk more than is required, a less expensive solution may exist:
  - For example, X.509 certificate-based authentication greatly reduces the risk of unauthorised access, but is very expensive; a less costly solution may be username and password authentication.
- If a control costs more than the monetary value of the risk reduction provided, consider other controls:
  - For example, a one-time password implementation using tokens would not reduce risk significantly more than a username and password combination, which is a significantly less expensive solution.
- If a control does not reduce the risk to an acceptable level, identify other controls or consider combining controls:
  - For example, using only a personal identification (ID) to identify a user, such as a driver's license number, may not mitigate against the risk of unauthorised access to an online service. A password would also be required.

Considering all other factors the same, controls with lower residual risk should be selected. For example, if two controls cost the same and reduce a specific risk to an acceptable level, it is very likely that one control may reduce the risk more than the other, having lower residual risk and making it a more favourable choice of treatment.

---

[9] *If the decision in the previous step is to transfer the risk, individuals will be identified to carry out necessary steps, and the necessary activities may be scheduled at this time. It may not be necessary to carry the rest of the steps in this guide for that particular risk.*

Step 4 Output:

A list of Senior Management decisions

- Senior Management will make the decision on which mitigation route to take for each risk
- Senior Manager/Decision Maker's name will also be captured

- Of those controls that are cost-effective, a control or set of controls have been selected to mitigate risks
- Some risks may require installing a patch while others may require a complete strategy to address

PLAN RISK TREATMENT				
STEP 3		STEP 4		
RESOURCES REQUIRED	CONTROL COST-EFFECTIVE	MITIGATION ROUTE	SENIOR MANAGER/ DECISION MAKER	MITIGATION STRATEGY/ SELECTED CONTROLS
Option 1: A few days of meeting and senior management involvement may be necessary. Approximate Cost = $2000. Option 2: Extensive Operation, hire multiple employees/ Hardware/Software Purchase. Approximate Cost = Over $100,000	Option 1: Yes Option 2: No	Reduce	John Doe	Work with HostingCo to install a dedicated switch for our servers. Additionally, update the agreement to delineate security responsibilities.
3 Days of DBA time.	Yes	Reduce	John Doe	Implement access control that uses usernames and password to authenticate users.
3 days of admin time, System Owner and business operational users involvement.	Yes	Reduce	John Doe	Implement role-based access control that follows least privilege principles.
2 hours of admin time.	Yes	Reduce	John Doe	Configure terminal services to terminate session after 15 minutes of inactivity.

- If the mitigation route is to reduce or avoid then all the steps 5 through 9 will need to be completed
- If the mitigation route is to transfer then Steps 5 and 6 would need to be completed
- If the mitigation route is to accept, it will not be necessary to complete the rest of the steps

Additional step may be taken to reduce residual risk

Figure 13: Selection of Mitigation Route and Security Control

STEP 5: Assign Responsibility and Schedule Implementation

Step 5 Input: *A list of controls that have been selected to be implemented, along with resource requirements*

If management decides to reduce, avoid, or transfer the risk, appropriate resources with the correct skill sets must be assigned to implement selected controls within a given timeframe. Some controls may require multiple individuals to carry out their implementation and document as necessary.

The implementation schedule should be based on a detailed plan of the activities that are needed to implement the control. The severity of a risk being addressed should be a driver for implementation prioritisation[10]. For example, tasks and resources to address a Level 6 risk would take precedence over a Level 3 risk.

If there are multiple risks with the same severity level, other factors may be taken into account such as:

- Level of effort to implement the control
- Availability of resources
  - Hardware/software availability
  - Availability of employees/contractors
- Compatibility with the current environment/infrastructure
- Compatibility with the organisation's strategic initiatives

For example, if there are two risks with severity level of 6, and one requires an intrusion prevention system (IPS) to be installed and the other requires a minor change to configuration settings of the operating system, the latter one should have higher priority and be implemented first.

[10] *Additionally, controls can be implemented concurrently if their required resources are not the same.*

Step 6 Output: *List of individuals assigned to implement the control (or a set of controls) within a given schedule.*

Appropriate personnel/contractors with the right skill set are assigned responsibility to implement the fix within given time frame.

PLAN RISK TREATMENT					
✓ STEP 4			STEP 5		
MITIGATION ROUTE	SENIOR MANAGER/ DECISION MAKER	MITIGATION STRATEGY/ SELECTED CONTROLS	IMPLEMEN-TATION ASSIGNMENT	IMPLEMEN-TATION START DATE	TARGETED COMPLETION DATE
Reduce	John Doe	Work with HostingCo to install a dedicated switch for our servers. Additionally, update the agreement to delineate security responsibilities.	John Doe (System Owner)	April 10, 2008	June 30, 2008
Reduce	John Doe	Implement access control that uses usernames and passwords to authenticate users.	John Doe (DBA)	May 1, 2008	May 4, 2008
Reduce	John Doe	Implement role-based access control that follows least privilege principles.	John Doe (System Owner)	May 1, 2008	May 4, 2008
Reduce	John Doe	Configure terminal services to terminate session after 15 minutes of inactivity.	Jane Smith (Administrator)	May 10, 2008	May 10, 2008

Figure 14: Schedule Implementation and Assign Responsibility

3.3 TREAT RISK AND VERIFY TREATMENT

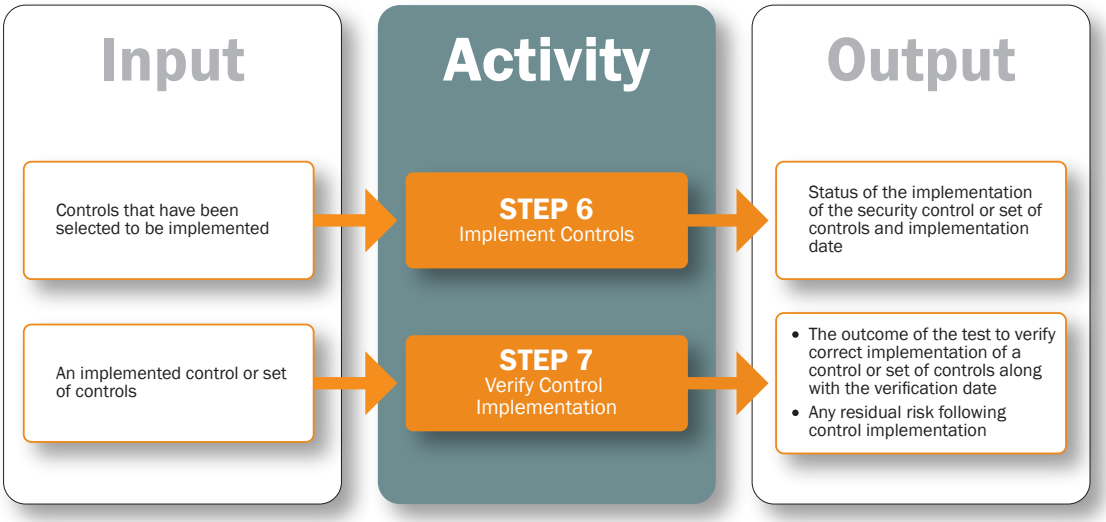


Figure 15: Treat Risk and Verify Treatment

STEP 6: Implement Controls

Step 6 Input: *A list of controls that have been selected to be implemented*

During this step, the plan that has been developed from Steps 1 through 7 of this guide is executed i.e., the actual implementation of the control takes place. The System Owner will be responsible for monitoring implementation of the controls and ensuring that the Information Security Plan is updated to reflect changes in scheduling that result from both internal delays and delays outside the control of the entity, such as delivery of hardware or software. To stay aware of the progress, it is recommended that System Owners inquire about the implementation status of controls at least once a week, and update progress in terms of percent completed. Preferably, all implementation should first occur on systems that are in the development stage.

Step 7 Output: *Implementation status of the security control (or set of controls) and implementation date*

- The implementation status of the control is tracked with the percent of completion
- It should be marked completed when implemented and ready for verification of proper implementation
- The actual date of the implementation of the control should be noted

PLAN RISK TREATMENT			TREAT RISK AND VERIFY	
STEP 5			STEP 6	
IMPLEMENTATION ASSIGNMENT	IMPLEMENTATION START DATE	TARGETED COMPLETION DATE	IMPLEMENTATION STATUS	ACTUAL IMPLEMENTATION DATE
John Doe (System Owner)	April 10, 2008	June 30, 2008	In Progress 20% Completed	
John Doe (DBA)	May 1, 2008	May 4, 2008	Not Stated	
John Doe (System Owner)	May 1, 2008	May 4, 2008	Not Stated	
Jane Smith (Administrator)	May 10, 2008	May 10, 2008	Not Stated	

Figure 16: Control Implementation Status and Date

STEP 7: Verify Control Implementation[11]

Step 7 Input: *An implemented control (or set of controls)*

When implementation of each control is complete, it should be tested to verify that its intended purpose is served and the associated risk has been reduced to an acceptable level.

The same steps that were executed to identify the risk during the Risk Assessment phase should be repeated to verify the fix. This verification should take place as soon as controls are implemented. It is not necessary to wait for all of the controls in a Information Security Plan to be implemented.

The *Abu Dhabi Information Security Technical Testing Guide* should be referred to in order to perform testing of the implemented controls. Upon completion of testing, the verification status should be marked as PASS or FAIL. In the event of failure, Step 6 will need to be repeated and retested to ensure that the control is implemented properly.

[11] *The intention of this step is not to assess the security posture of the entire system, but rather to verify the correct implementation of a control or a set of dependent controls. There could be a long period between the implementation of a control and the next Risk Assessment or Security Testing and Evaluation (ST&E). Thus it is important to verify the control implementation to avoid a false sense of security. Comprehensive testing will be conducted during the Security Testing and Evaluation phase.*

Any residual risk should also be captured in the Information Security Plan.

Step 8 Output:

- *Outcome of the test to verify correct implementation of a control or set of controls, with the verification date*
- *Any residual risk following control implementation*

- Once the control implementation is verified, the verification status and verification dates are captured
- If a control fails, step 7 may need to be repeated
- Any residual risk should also be identified during control selection and verification steps

TREAT RISK AND VERIFY TREATMENT				
STEP 6		STEP 7		
IMPLEMEN-TATION STATUS	ACTUAL IMPLEMENTATION DATE	VERIFICATION STATUS	VERIFICATION DATE	RESIDUAL RISK
In Progress 20% Completed				Potential for other risks at HostingCo arising.
Not Stated				▪ User password could be weak. ▪ Password may be written down
Not Stated				Admin users have broad access to systems
Not Stated				15 minutes may still provide sufficient time to hijack session with a super computer.

Figure 17: Verify Control Implementation

3.4 FORMULATE INFORMATION SECURITY PLAN

Figure 18: Formulate Information Security Plan

STEP 8: Develop Information Security Plan

Step 8 Input: *The outputs of Steps 1 through 7*

During Steps 1 through 7, details were gathered that can now be used to develop an Information Security Plan. The purpose of this document is to describe how each of the Abu Dhabi Information Security Standards is or will be addressed. Along with the description of the control implementation, the Information Security Plan will indicate the implementation status of each control as follows:

- **Compliant –** The control is fully in place and no further actions are required.
- **Non-Compliant –** The control is not in place. The status should be marked non-compliant even if there is a planned activity to implement the control.
- **Risk Accepted –** The control is not in place and a decision was made not to put the control in place based on risk factors.
- **Not Applicable –** The control does not apply to this information system. If this status is selected for a control, a justification must be provided.

The Information Security Plan template can be found in Appendix E of this guide. It can be completed by using information in the Risk Treatment Plan template in Appendix D, which collated inputs and outputs from Step 1 to Step 7 of this guide. Information system categorisation[12] captured during the Risk Assessment phase should also be documented in this report along with roles and responsibilities associated with the information or service. Additional information should also be gathered from the information system developers and administrators in order to develop a robust Information Security Plan.

The information System Owner should assign an individual to "own" the Information Security Plan and ensure that it is updated to reflect the current security state of the information system. Once Information Security Planning is completed, the Information Security Plan must be approved by the information System Owner. The approval date will also serve as the completion date of the Information Security Plan.

Step 9 Output: *An Information Security Plan*

[12] *Information system categorisation is completed in Steps 2 and 3 of the Risk Assessment phase.*

3.5 NEXT STEPS

Now that the Information Security Planning activities have been captured in the Risk Treatment Plan, and an Information Security Plan has been formulated, Security Testing and Evaluation would need to be conducted to assess the overall security posture of the Government service. This step also allows secondary verification that controls have been implemented as documented in the Information Security Plan.

The step-by-step process to test and evaluate security controls can be found in the *Abu Dhabi Security Testing and Evaluation Guide.*

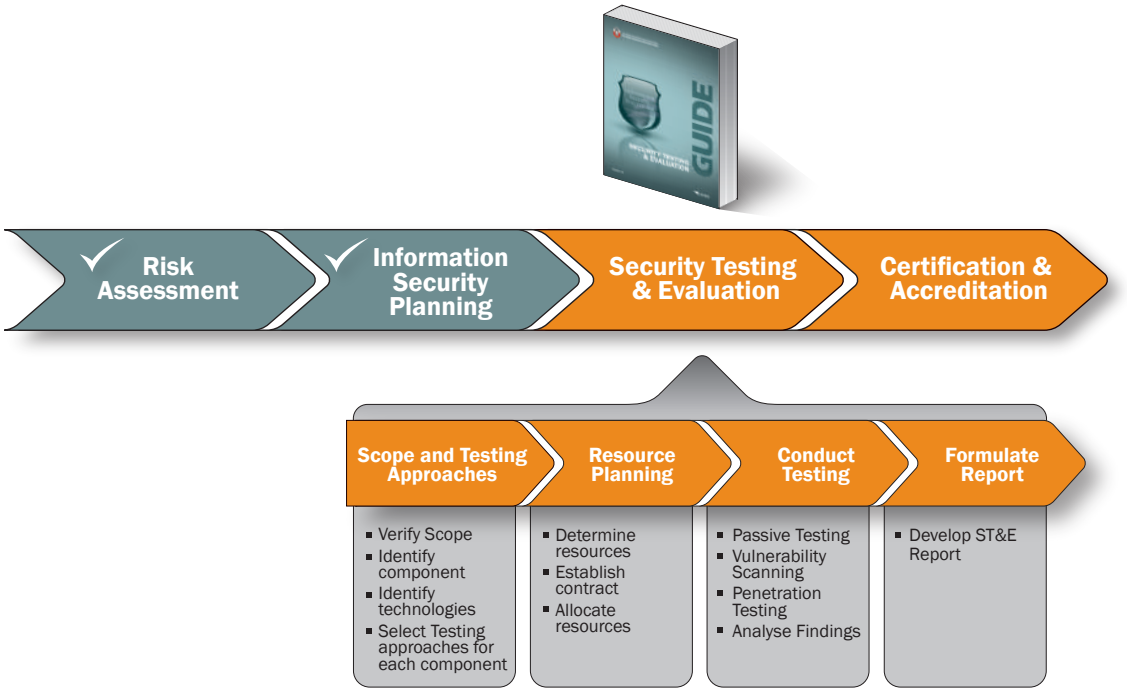


Figure 19: Overview of Next Phase: Security Testing and Evaluation

APPENDICES

APPENDIX A: ACRONYMS

ADAA	Abu Dhabi Accountability Authority
ADG-ISO	Abu Dhabi Government – Information Security Office
ADGE	Abu Dhabi Government Entities
ADP	The General Directorate of Abu Dhabi Police
ADSIC	Abu Dhabi Systems & Information Centre
ATO	Authority to Operate
BCM	Business Continuity Management
BCP	Business Continuity Plan
C&A	Certification and Accreditation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Certifying Official
CVE	Common Vulnerability Exposure
DAA	Designated Approval Authority
DTO	Denial To Operate
HR	Human Resources
IATO	Interim Authority to Operate
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Protection System
IS	Information Security
ISMS	Information Security Management System
ISO/IEC	International Organisation for Standardisation/International Electrotechnical Commission
ISP	Information Security Plan
ISWG	Information Security Working Group
IT	Information Technology
IV&V	Independent Verification and Validation

NIST	National Institute of Standards and Technology
PDCA	Plan-Do-Check-Act
POC	Point Of Contact
ROE	Rules Of Engagement
SQL	Structured Query Language
ST&E	Security Testing and Evaluation
UAE	United Arab Emirates

APPENDIX B: REFERENCES

Abu Dhabi Information Security Standards, December 2008.

Abu Dhabi Risk Management Guide, December 2008.

Abu Dhabi Risk Assessment Guide, December 2008.

Abu Dhabi Security Testing & Evaluation Guide, December 2008.

Abu Dhabi Certification & Accreditation Guide, December 2008.

Abu Dhabi Information Security Technical Testing Guide, December 2008.

Abu Dhabi Information Security Policies and Procedures Guide, March 2009

National Institute of Standards and Technology Special Publication 800-30, *Risk Assessment Guide for Information Technology Systems,* July 2002.

Risk Management Guide for Acquisition, Sixth Edition, August 2006.

National Institute of Standards and Technology Special Publication 800-17, *Guide for Developing Security Plans for Federal Information Systems,* February 2006.

International Organisation for Standardisation (ISO) 27001, *Information Technology— Security Techniques — Information Security Management Systems — Requirements,* First Edition, October 15, 2005.

APPENDIX C: DEFINITIONS

Accreditation	The official management decision given by a senior entity official (chairman) to authorise operation of a Government service and to explicitly accept the risk to entity operations, entity assets, or individuals based on the implementation of an agreed-upon set of security controls
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information
Audit	A formal (independent) review and examination of a project or project activity for assessing compliance with policy and standards
Asset	Anything that has value to the organisation, such as information or information systems
Availability	Ensuring timely and reliable access to and use of information
Certification	Comprehensive assessment of the management and functional security controls in a Government service, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security risk requirements for the services
Certifying Official	Individual, group, or organisation responsible for conducting an information security certification (see definition for Certification)
Confidentiality	Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Control	Means of managing risk, including policies, procedures, guidelines, practices, or organisational structures, which can be of administrative, technical, management, or legal nature
Control Families	Management and functional processes that are grouped into 14 specific families (e.g., Policy and Standards, Human Resources Management, etc.) in order to provide the foundation for a comprehensive Information Security Programme
Control Standards (also referred to as Standards)	Level of security that is deemed necessary (based on international standards and risk assessment) to ensure adequate security. Standards are delineated into two categories: (i) baseline, or the minimum, control standards that must be met for all risk environments; and (ii) enhancements that are recommended for moderate or high risk environments
Cost-Effective Control	A control is determined to be cost effective if the cost of implementing and maintaining the control is economical in in comparison with the risk that it is mitigating

Designated Approval Authority	Individual who has the ultimate responsibility to accredit all Government services. This individual accepts responsibility for the security of the service and accountability for any adverse impacts to the entity if a breach of security occurs
Functional Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems)
Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies
Independent Verification & Validation	The process of evaluating work products by a party who is technically, managerially, and financially independent of designing and/or executing the project under review
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form; including textual, numerical, graphic, cartographic, narrative, or audiovisual forms
Information Security	Protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability
Information Security Plan	Formal document that provides an overview of the security requirements for the Government service and describes security controls in place or planned for meeting these requirements
Information System	A discrete set of information resources organised for the collection, processing, maintenance, use, sharing, dissemination, or disposal of information, including manual processes or automated processes. This includes information systems used by an entity either directly or used by another entity, or a contractor under a contract with the entity that: (i) requires the use of such information systems; or (ii) requires the use, to significant extent, of such information systems in the performance of a service or the furnishing of a product
Information Security Event	Identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security-relevant
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information Technology	Any equipment or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information
Integrity	Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
IT Assets	Computer equipment, such as servers, workstations, routers, firewalls, etc.

Malicious Code	Software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of an information system (e.g., virus, worm, Trojan horse, other code-based entity that infects a host). Spyware and some forms of adware are also examples of malicious code
Management Controls	Security controls (i.e., safeguards or countermeasures) for an information system that focuses on the management of risk and the management of information system security.
Mitigation of Risk	Reducing risks to an acceptable level by applying controls
Personally Identifiable Information	Information in an information system: (i) that directly identifies an individual (e.g., name, address, or other identifying number or code, telephone number, email address, etc.), or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors
Policy	Overall intention and direction as formally expressed by management
Potential Impact	The loss of confidentiality, integrity, and/or availability could have (i) low adverse effect; (ii) a moderate adverse effect; or (iii) a high adverse effect on organizational operations, assets, or individuals
Privacy	Information that is linked to a specific individual or group and is controlled and managed by that individual or group – even after that information is willingly shared with a third party – such as to avoid the unwanted disclosure of private information, which could result in damaging effects for the individual. Information Security must include the implementation of controls related to private information. Best practices include the ability to provide the justification and rationalisation for why the use of private information is necessary instead of the use of an alternate identifying schema
Residual Risk	Risk remaining after implementation or enhancement of a control
Risk	The level of impact on entity services, assets, or individuals resulting form the potential consequences of a threat and the likelihood of that threat occurring
Risk Analysis	Systematic use of information to identify sources and to estimate the risk
Risk Assessment	Overall process of risk analysis and risk evaluation
Risk Evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk Treatment	Process of selecting and implementing controls to modify risk
Spyware	Software that is secretly or surreptitiously installed on an information system to gather information on individuals or organisations without their knowledge. Spyware is a type of malicious code

Standards (also referred to as Control Standards)	Level of security that is deemed necessary (based on international standards and risk assessment) to ensure adequate security. Standards are delineated into two categories: (i) baseline, or the minimum, control standards that must be met for all risk environments; and (ii) enhancements that are recommended for moderate or high risks environments
Third Party	Person or body that is recognised as being independent of the parties involved
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization
Threat Source	Intent and method targeted at the intentional exploitation of vulnerability, or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats

APPENDIX D: RISK TREATMENT PLAN TEMPLATE

A soft copy of the template can be obtained through ADSIC. ADSIC can be contacted at support@adsic.abudhabi.ae

APPENDIX E: INFORMATION SECURITY PLAN TEMPLATE

A soft copy of the template can be obtained through ADSIC. ADSIC can be contacted at support@adsic.abudhabi.ae