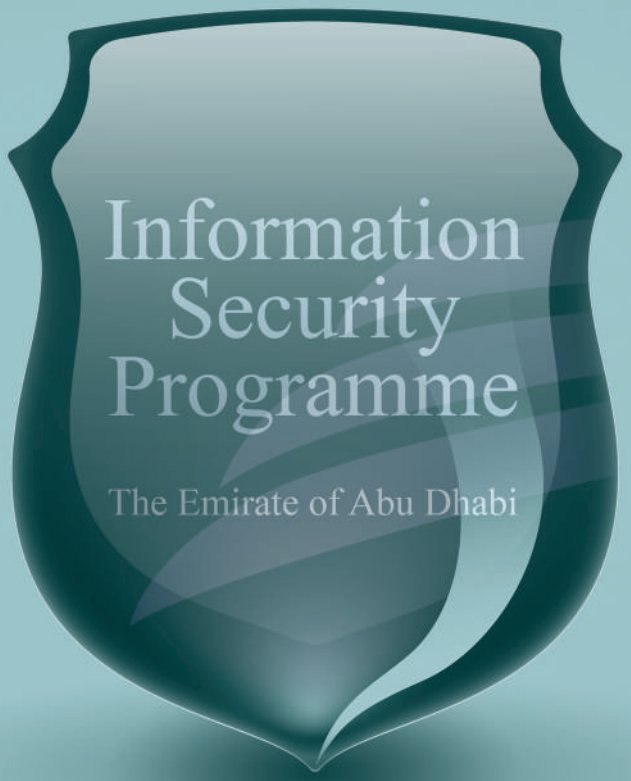
مركز أبوظبي للأنظمة الإلكترونية والمعلومات
Abu Dhabi Systems & Information Centre



GUIDE

RISK ASSESSMENT

Version 1.0

أبوظبي
abudhabi

RISK ASSESSMENT 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

1.1 OVERVIEW 1
1.2 SCOPE 2
1.3 APPLICABILITY 2
1.4 COMPLIANCE AND ENFORCEMENT 2
1.5 DOCUMENT LAYOUT 3

2. FREQUENTLY ASKED QUESTIONS 4

2.1 WHY CONDUCT A RISK ASSESSMENT? 4
2.2 WHEN SHOULD A RISK ASSESSMENT BE CONDUCTED? 4
2.3 WHO IS RESPONSIBLE FOR CONDUCTING THE RISK ASSESSMENT? 4
2.4 HOW IS THIS DIFFERENT FROM A SECURITY AUDIT OR PENETRATION TEST? 4
2.5 HOW DOES RISK ASSESSMENT RELATE TO ISO/IEC 27001:2005 CERTIFICATION? 4
2.6 HOW IS A THREAT DEFINED? 5
2.7 HOW IS A VULNERABILITY DEFINED? 6
2.8 WHAT IS THE RELATIONSHIP BETWEEN A THREAT AND A VULNERABILITY? 6
2.9 WHAT IS A CONTROL? 6

3. RISK ASSESSMENT STEPS 7

3.1 STEP 1: DEFINE SCOPE OF ASSESSMENT 9
3.2 STEP 2: IDENTIFY SUPPORTING ASSETS 11
3.3 STEP 3: ASSESS IMPACT 15
3.4 STEP 4: IDENTIFY THREATS 20
3.5 STEP 5: IDENTIFY VULNERABILITIES 25
3.6 STEP 6: IDENTIFY RISK 28
3.7 NEXT STEPS 34

4. APPENDICES 36

APPENDIX A: ACRONYMS 37
APPENDIX B: REFERENCES 39
APPENDIX C: DEFINITIONS 40
APPENDIX D: RISK ASSESSMENT TEMPLATE 44
APPENDIX E: RISK ASSESSMENT REPORT FORMAT 45
APPENDIX F: WORKED EXAMPLE 49
APPENDIX G: ASSET INVENTORY TEMPLATE 50

1. INTRODUCTION

1.1 OVERVIEW

This *Risk Assessment Guide* is intended to equip a designated assessor to conduct a risk assessment for e-Government services provided by the Abu Dhabi Government. Risk assessment is the first of the four phases that constitute the overall Risk Management[1] process to be adopted by Abu Dhabi Government Entities (ADGE). E-Government services are defined as those that make use of information technology (IT) systems to provide services for citizens and/or enable shared services to increase the functionality and efficiency of current and future services provided by the Abu Dhabi Government.

In broad terms, "risk" can be defined as the variable that results from information based upon the likelihood and impact of a security incident occurring. The diagram below shows a more specific representation of risk:

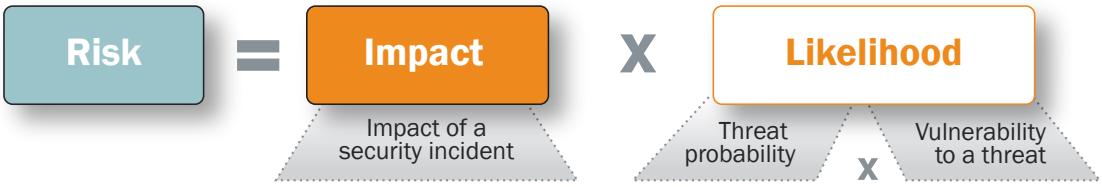


Figure 1: The Concept of Risk

The risk assessment will allow entities to obtain an accurate view of risks to information that supports e-Government services through application of the methodological approach described in this Guide. This view, which takes into account assets that need protection and the impact and likelihood of attacks, is then used as a basis to make business-led decisions on how the risks should be treated. This helps meet the overall goal of enabling e-Government services that can be used securely and with confidence.

The conduit to bringing these management and functional processes to an environment is Risk Management, which provides a foundation for the Information Security Programme by requiring that entities protect Government information commensurate with the risk and magnitude of harm that could result from its loss, misuse, unauthorised access, or modification. Risk Management can be broken down into four phases, as shown in Figure 2:

Figure 2: Four Phases of the Risk Management Process and Supporting Guides

[1] *The scope of this risk management—and risk assessment—will be applicable to the specific services identified by ADSIC during the pilot phase and beyond. "Pilot phase" refers to the period where risk management steps within the guides will be trialed and refined.*

This *Abu Dhabi Risk Assessment Guide* is supported by additional Risk Management guidance (*e.g., Information Security Planning Guide, Security Testing & Evaluation Guide,* and *Information Security Standards*[2]) and training. Together, 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 *Risk Assessment Guide* centres on information security—looking beyond the traditional focus of IT. This ensures that sensitive Government information is protected throughout its lifecycle, 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 security, personnel security, business continuity, and cross-functional risk management, and the importance of directing the programme to assure Government missions rather than solely focus on security. 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 *Risk Assessment Guide* applies to Abu Dhabi Government personnel, contractors, and third party organisations and individuals[3]. It encompasses all information and IT 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 this *Risk Assessment Guide* is mandatory. The implementation of security controls can only be fully effective when all stakeholders are aware of the harmful consequences of not securing Government information. This means that the entire Government workforce must act responsibly.

Personnel and entities found to be non-compliant with this *Risk Assessment Guide* may have their access to information systems and data revoked, and be subject to criminal disciplinary actions 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 the shared responsibility of ADSIC, each Government entity's Chief Information Security Officer (CISO), and the Abu Dhabi Accountability Authority.

Any instances of intentional non-compliance with this *Risk Assessment Guide* must be clearly documented and justified by the entity, and are subject to review and approval for acceptance by ADSIC.

---

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

[3] *This document applies to civilian Government organisations with the exception of intelligence services. This Information Security Policy does not apply to the military service.*

1.5 DOCUMENT LAYOUT

This document will provide the reader with the information and tools needed to carry out an information security risk assessment. It is divided into three main sections:

- **Section 1** provides the overview, background, and purpose of this document, and answers the question, “Why Conduct a Risk Assessment?”
- **Section 2** provides answers to frequently asked questions about risk assessment and some of its key components.
- **Section 3** provides a step-by-step guide to conducting a risk assessment, and answers the question, “How Do I Conduct a Risk Assessment?”
- **Appendices A through G** provide information to support the risk assessment process, including a template that can be used to complete the steps covered in Section 3.

2. FREQUENTLY ASKED QUESTIONS

2.1 WHY CONDUCT A RISK ASSESSMENT?

Abu Dhabi Information Security Policy requires that risk assessments 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 public e-Government services
- Enabling management to make informed decisions regarding implementation of security controls and remediation measures
- Promoting a consistent approach to measuring risk
- Allowing stakeholders to place values on potential losses

2.2 WHEN SHOULD A RISK ASSESSMENT BE CONDUCTED?

ADGE information systems need to go through the Risk Management process every three years, or if a major change is made that can affect the information security of the system. This ensures that system security is up to date with all current threats and vulnerabilities.

2.3 WHO IS RESPONSIBLE FOR CONDUCTING THE RISK ASSESSMENT?

An "assessor" will be designated to conduct the risk assessment for a given e-Government service. This assessor will be a member of the Abu Dhabi Government – Information Security Office (ADG-ISO).

2.4 HOW IS THIS DIFFERENT FROM A SECURITY AUDIT OR PENETRATION TEST?

A security audit or penetration test is a momentary, non-perpetual assessment of a system that provides a snapshot of its security posture at a given point in time. Although it is possible to react to an audit or test and correct any findings, these are not sustainable methods to ensure that services remain secure, because a vulnerability may arise days after a fix is implemented, placing the service at risk again.

Risk Management is used to define an ongoing approach to ensure system security, and has become the de facto international standard (in the form of ISO/IEC 27001:2005) for best practice security management. The ongoing nature of Risk Management embedded across an organisation helps reduce exposure to vulnerabilities that may arise after implementing fixes, by requiring that a process for continually detecting new vulnerabilities be in place. Risk assessment is a required component of risk management.

2.5 HOW DOES RISK ASSESSMENT RELATE TO ISO/IEC 27001:2005 CERTIFICATION?

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 individual organisations or parts thereof.

A key component in establishing the ISMS is to incorporate a Risk Management process. Since risk assessment is a step in this process, it is required to be implemented and demonstrably operated to achieve ISO/IEC 27001:2005 certification.

2.6 HOW IS A THREAT DEFINED?

A threat is defined as any circumstance, event, or act that could cause harm to an entity by destroying, disclosing, modifying, or denying service to automated information resources. Three threat categories exist—natural disaster, environmental control failure, and human. Table 1 provides examples of the threats found in each.

NATURAL DISASTER			
Storm damage (e.g., flood, snow, hurricane)	Fire	Lightning strikes	Earthquakes
ENVIRONMENTAL CONTROL FAILURE			
Long term power failure	Chemicals	Liquid leakage	Pollution
HUMAN			
Assault on an employee	Arson		Blackmail
Bomb or terrorism	Browsing of private and proprietary information		Civil disorder
Computer abuse	Corrupted data input		Falsified data input
Fraud	Hacking		Impersonation
Interception	Labour dispute or strike		Malicious code
Negligence or human error	Unauthorised disclosure of sensitive information		Password guessing (e.g., dictionary attack)
Vandalism	Sabotage		Social engineering
Spoofing	System tampering		Theft

Table 1: Categorised Examples of Threats

Examples of a natural disaster include extreme weather or earthquake. Environmental control failures are man-made occurrences, such as utility failures or chemical leakages.

A threat agent (person who exploits system vulnerabilities) is behind human threats. Examples of human threat agents include:

- **Insiders** – Anyone employed by the entity (e.g., disgruntled employees, dishonest employees, privileged/unprivileged department system users, etc.)
- **Contractors and subcontractors** – Individuals who work on the entity's premises but are not entity employees (e.g., cleaning crew, external developers, third party technical support personnel, computer/telephone service repairmen, etc.)
- **Former employees** – Employees who have retired, resigned, or been terminated

- **Unauthorised users** – Users who do not have authorised access but are motivated to conduct adversarial actions in the entity's information system environment (e.g., computer criminals, terrorists, and intruders [hackers and crackers] who attempt to access the entity's internal network, etc.)
- **Authorised users** – Any approved users (e.g., ADGE employees, contractors, business partners, etc.)

2.7 HOW IS A VULNERABILITY DEFINED?

A vulnerability is a condition that has the potential to be exploited by a threat. Baseline security requirements or security standards contained in the *Abu Dhabi Information Security Standards* document define what ADSIC views as the minimum standards to be upheld by all entities. Security requirements that are ignored or insufficiently implemented could make a system vulnerable. Security controls that were identified and selected but not properly implemented should be flagged as vulnerabilities in Step 5 of the Risk Assessment process.

Vulnerabilities are identified based on information collected from each entity, its systems, and the environment via site surveys, interviews, network scanning, and documentation. Available industry sources should be used to identify vulnerabilities that may be applicable to specific systems.

2.8 WHAT IS THE RELATIONSHIP BETWEEN A THREAT AND A VULNERABILITY?

A vulnerability cannot be exploited unless there is a potential threat and an associated threat actor. The threat actor is someone who has the means, opportunity, and motivation to exploit a potential vulnerability. Based on this description, it is evident that threats and vulnerabilities are closely aligned when assessing risks. What might begin as a minor threat has the potential to become a greater or more frequent threat if a vulnerability should emerge.

2.9 WHAT IS A CONTROL?

A control is defined as a security measure that serves to reduce a security risk. For example, automated patch updates are a control to prevent malicious code/users from exploiting vulnerabilities in software.

The term "control" can also be used in a "counter-threat" sense. For example, consider is the threat of a remote hacking attack on a database. A counter-threat control could be to ensure that the database is not connected to the Internet—either directly or by association with other technical components that could facilitate remote hacking.

3. RISK ASSESSMENT STEPS

The Risk Assessment process is divided into six steps:

STEP 1: Define Scope of Assessment

STEP 2: Identify Supporting Assets

STEP 3: Assess Impact

STEP 4: Identify Threats

STEP 5: Identify Vulnerabilities

STEP 6: Identify Risk

All steps are mandatory. Since each relies upon output from the previous step, they must be done in sequence.

The output of each step should be captured in the template reference provided in Appendix D. A working example is used in each of the steps to demonstrate template usage, but it is not essential that all information be captured in the template. For example, there may be hundreds of technical vulnerabilities for some systems, and it would be impractical to insert them into the template. Such types of details should be captured in a separate document and a link to the document should be provided in the template.

The sequence of steps is shown in Figure 3:

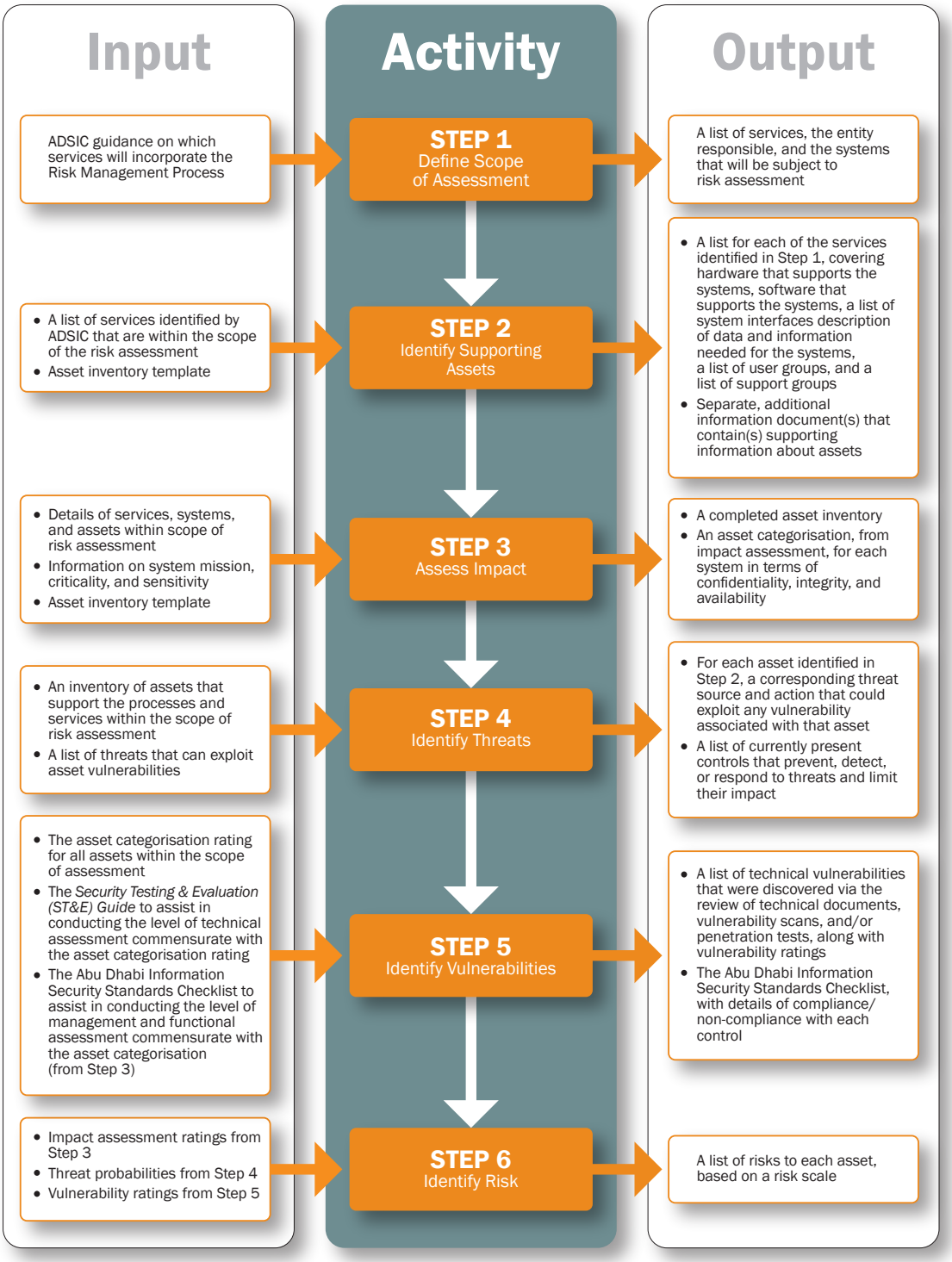


Figure 3: Steps in the Risk Assessment Process

3.1 STEP 1: DEFINE SCOPE OF ASSESSMENT

Figure 4: Define Scope Of Assessment

Step 1 Input: *ADSIC guidance on which services will incorporate the Risk Management process.*

The scope to which this assessment applies is driven by the services for which the risks will be assessed. The first step is to identify the services that exist as part of the e-Government initiative.

The assessor will identify the service or will receive from ADSIC the name of the service that requires risk assessment.

A service can be defined as a function that allows an individual or organisation to carry out a task (or sets of tasks) that enables a benefit to the citizens of Abu Dhabi.

For each service, there must be a responsible entity. While it is possible for a single entity to provide multiple services, the scope of each risk assessment will be limited to the boundary of that service. This is depicted in Figure 5.

Each service will consist of a system (or a number of systems). Each system will be comprised of assets such as hardware, software, people, and processes. A criminal tracking service, for example, would include data capture, data update, and data access systems. Assets may also include network servers, support incident management processes, the operations user group that manages the service, etc.

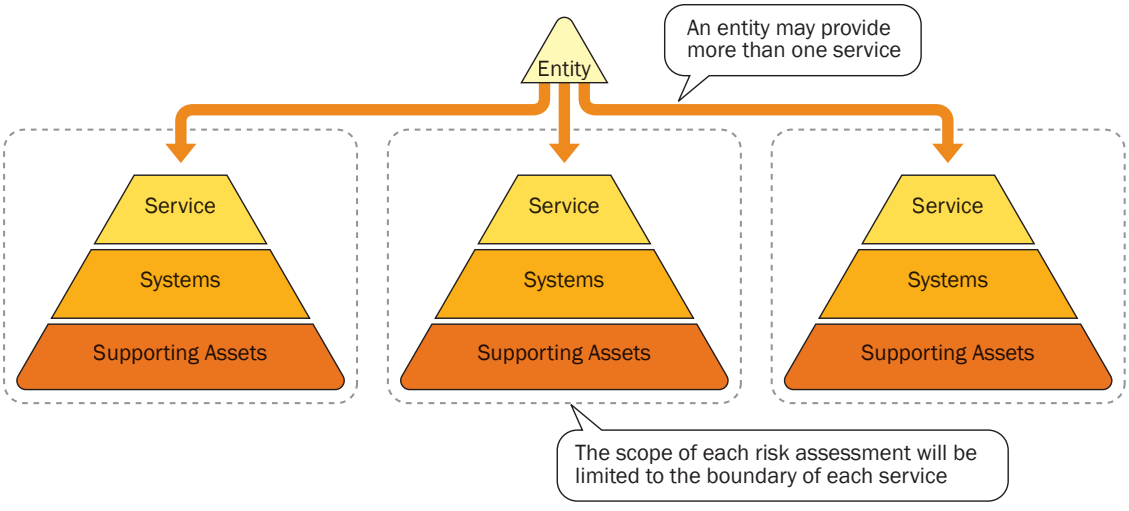


Figure 5: Relationship Between the Entity and Its Services

Step 1 Output: *A list of services, the entity responsible, and the systems that will be subject to risk assessment should populate the first three columns of the risk assessment template shown in Figure 6:*

- **Service:** ADSIC will advise which services will be within scope of risk assessment during the pilot phase.
- **Entity Responsible:** The entity hosting the service.
- **Supporting Systems:** Names of systems that support the service and are within scope of assessment.

DEFINE SCOPE OF ASSESSMENT			IDENTIFY SUPPORTING ASSETS	
STEP 1			STEP 2	
SERVICE	**ENTITY RESPONSIBLE**	**SYSTEMS**	**SUPPORTING ASSETS**	**ADDITIONAL ASSET INFORMATION**
Criminal Location Tracking	Police Force	Criminal ID system		<doc>
			Application servers	<doc>
			Front end clients (desktops)	<doc>
			Criminal tracking user group	<doc>
			HostingCo Data Centre	<doc>
			HostingCo network for hosting clients' services	<doc>

Figure 6: Defining the Scope for Risk Assessment

3.2 STEP 2: IDENTIFY SUPPORTING ASSETS

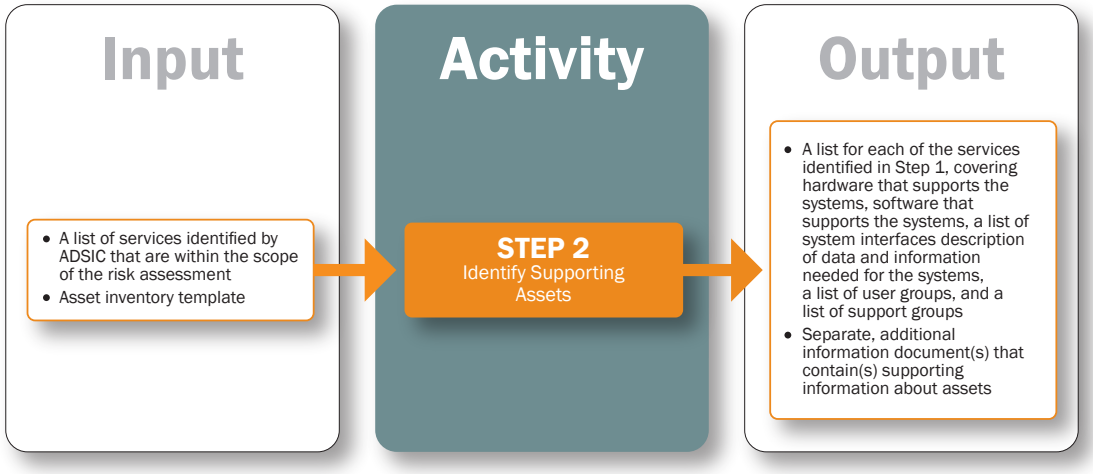


Figure 7: Identify Supporting Assets

Step 2 Input:

- *A list of services identified by ADSIC that are within the scope of the risk assessment*
- *Asset inventory template (see Appendix G)*

All assets supporting the service within scope will be subject to the subsequent steps of the risk assessment. This relationship is illustrated in Figure 8, which shows the methods used to identify assets and the typical information outputs that help to group these assets.

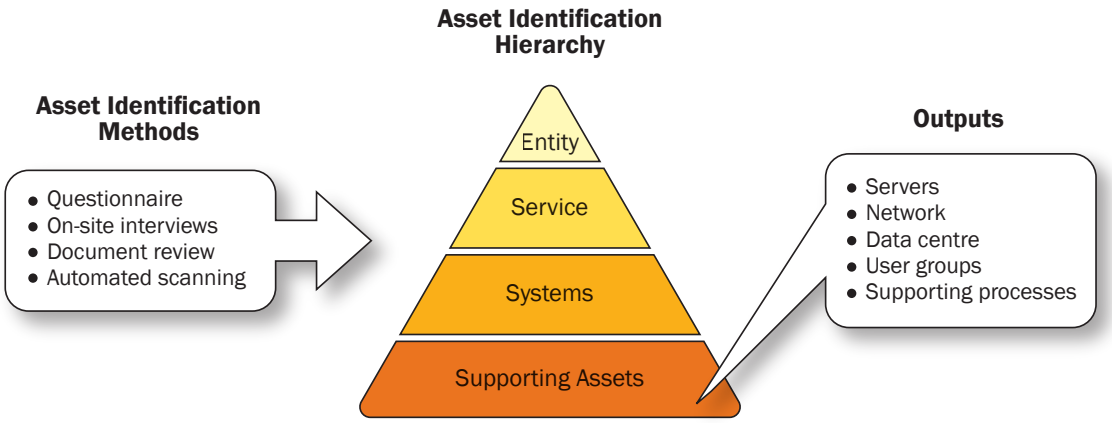


Figure 8: Relationship Between Entity, Service, Systems, and Assets

As shown in Figure 8, an entity may be responsible for multiple services. The scope of each risk assessment will cover a single service.

Every identified service is supported by an entity. This entity hosts and has access to the service's systems—each of which consists of assets that the assessor should list.

Assets can be categorised as either an inventory of general support systems (GSS) or major applications (MA). These are defined as:

- **GSS** – An interconnected set of information resources, under the same direct management control, that share common functionality
- **MA** – An application that requires special attention to security due to the risk and magnitude of harm that would result from the loss, misuse, or unauthorised access to (or modification of) information it contains

All automated entity information resources fall into one of these two categories. To begin the asset identification stage, identify the entity's business functions—work performed in support of its mission, vision, and goals. These can include grants management, provision of public information, or human resources management. Identified functions should then be separated according to the specific activities that support the entity's overall business function.

Each identified function has its own associated automated processes. Once these processes have been determined, their supporting information resources must be identified and included as candidates for the GSS and MA inventory.

For each business function, identify and describe all automated supporting processes and related information resources such as databases, stand-alone systems, communications systems, networks, and any other type of IT-related support. Automated information resources that utilise general purpose software such as spreadsheets and word processing programmes should not be included because their security is provided by the GSS on which they reside.

Keep in mind that it is possible for several automated information resources to support a single business function. It is also possible to have one automated information resource support several business functions.

To identify these GSS and MA assets and their details, the assessor can gather information by means of:

- **Questionnaires** – A list of questions designed to help form a detailed picture of assets supporting the service
- **On-site interviews** – Discussions with staff in various roles to ascertain which assets support a particular service
- **Document reviews** – Scrutinising documents (e.g., network diagrams denoting network components) to help determine which assets provide the service with support
- **Automated scanning** – The use of scanning software to discover devices on a network providing support to the service

Once identified, these assets can provide additional information—such as policies and network diagrams—as well as data relating to system mission, criticality, sensitivity, etc. This information should be captured in a separate document, and a link or reference should be provided in the risk assessment template. Examples of additional information for supporting assets are shown in Figure 9.

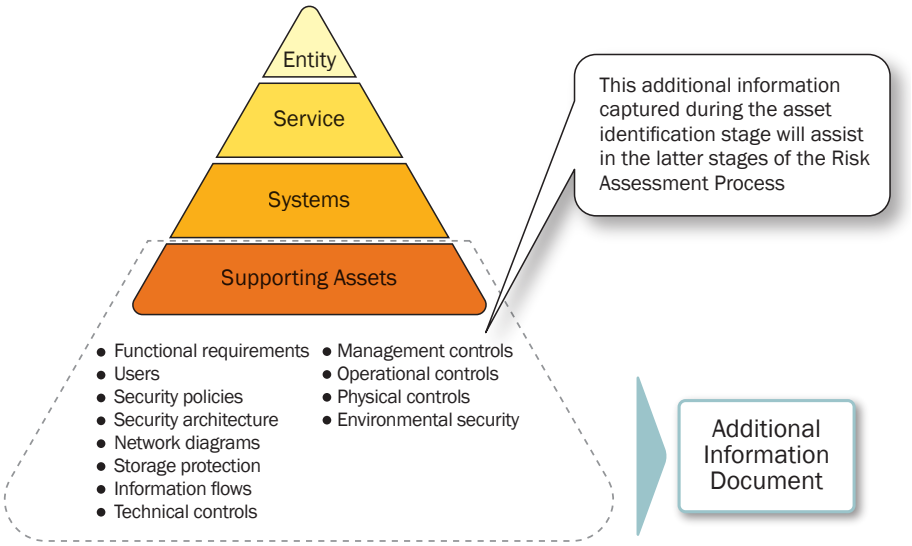


Figure 9: Examples of Additional Information for Assets Under Assessment

Details for each specific asset should be captured in the asset inventory template provided in Appendix G. This asset inventory can then serve a purpose beyond the risk assessment, by providing a reference point for assets within the entity. This particular asset inventory will also capture the assets' classification, which will be discussed in Step 3.

Step 2 Output:

- *A list for each of the services identified in Step 1, that includes hardware and software, system interfaces, a description of data and information needed to populate the systems, user groups, and support groups*
- *Separate, supplemental information documentation that contains supporting information about assets*
- *A partially completed copy of the Asset Inventory Template (Appendix G) containing details of automated information resources*

- **Supporting Assests:** The assets which are components of the service will then be listed.
- **Additional Asset Information:** Information (e.g., types, versions etc.) can be captured in a separate document(s). The document(s) should be linked to cells in this column.

DEFINE SCOPE OF ASSESSMENT			IDENTIFY SUPPORTING ASSETS		IMPACT ASSESSMENT
STEP 1			STEP 2		STEP 3
SERVICE	ENTITY RESPONSIBLE	SYSTEMS	SUPPORTING ASSETS	ADDITIONAL ASSETS INFORMATION	IMPACT ASSESSMENT
Criminal Location Tracking	Police Force	Criminal ID system	Database server	<doc>	Moderate
			Application servers	<doc>	Moderate
			Front-end clients (desktops)	<doc>	Low
			Criminal tracking user group	<doc>	High
			HostingCo Data Centre	<doc>	High
			HostingCo network for hosting clients' services	<doc>	Low

- Information captured in Step 2 will help populate the first section of the Asset Inventory Template in Appendix G

- In this column add any references to documents that contain supporting information

Figure 10: Details of Assets Supporting the Service Under Assessment

3.3 STEP 3: ASSESS IMPACT

Figure 11: Assess Impact

Step 3 Input:

- *Details of services, systems, and assets within the scope of the risk assessment*
- *Information on system mission, criticality, and sensitivity*
- *Partially completed asset inventory template from Step 2*

This step is used to categorise assets in terms of High, Moderate, and Low based upon how the entity would be impacted by loss of confidentiality, integrity, and availability.

These impact levels allow the assessor to define the scope of vulnerability assessment in the next steps of the risk assessment, which varies according to the risk rating. For example, while a system categorised as Low may require a vulnerability scan, a system categorised as High may require a penetration test as well.

Service-level categorisations are inherited from the highest categorisation of assets that constitute the service[4].

The *Abu Dhabi Information Security Policy* defines Information security as protection of information from a wide range of threats, and is achieved through the preservation of confidentiality, integrity, and availability.

- Confidentiality – The act of preserving authorised restrictions on information access and disclosure, including methods of protecting personal privacy and proprietary information
- Integrity – The act of guarding against improper information modification or destruction, to include non-repudiation and authenticity
- Availability – The act of ensuring timely and reliable access to, and use of, information

Protection of information in these areas facilitates the uninterrupted operation of Government services and the ability to maintain "business as usual."

Each area must be rated on the scale of High, Moderate, or Low according to the following guidelines:

- High – A service is categorised as High if loss of confidentiality, integrity, or availability would have a severe or catastrophic effect on the entity's operations, assets, or individuals. In the event of a security breach, the organisation would be unable to perform one or more of its primary functions. Major financial loss or severe damage to organisation assets would also result.

[4] *From this relationship, an assessor may find it easier to categorise the service and then propagate the same categorisation to the assets that are part of that service.*

- Moderate – A service is categorised as Moderate if the loss of confidentiality, integrity, or availability would have a serious adverse effect on the entity's operations, assets, or individuals. The organisation would experience a significant degradation in mission capability and its ability to perform primary functions, which could also result in significant financial loss and damage to organisational assets.
- Low – A service is categorised as Low if the loss of confidentiality, integrity, or availability would have limited adverse effect on the entity's operations, assets, or individuals, producing a degradation in mission capability. Although the entity would still be able to perform its primary functions, it would do so in a noticeably reduced capacity that could also result in minor loss of organisational assets and possible loss of personal privacy.

Detailed Guidance for Determining Impact

Confidentiality

To determine the appropriate level of confidentiality, an application or GSS must take into consideration the need for its information to be protected from unauthorised disclosure. This level of confidentiality depends on the nature of the information. For example, information that is widely available to the public has a low level of confidentiality because it requires little, if any, protection from disclosure. However, certain types of information must be protected from disclosure due to the expectation or assurance of privacy, or because unauthorised disclosure could result in a loss to the organisation.

Assets that contain financial, proprietary, or personal information must be protected at a high or moderate level of confidentiality. Organisations should not disclose any personal record that is contained in a system of records, by any means of communication, to any person or agency without the prior written consent of the owner except in certain narrowly prescribed, statutory circumstances.

Although an application or GSS may not meet privacy concerns, it may still contain information that must be protected at a high or moderate level of confidentiality.

Examples of confidentiality considerations:

HIGH

This category of application or GSS contains proprietary business, financial, or personal information (i.e., passport numbers or equivalent identifiers), which if disclosed to unauthorised sources could adversely impact the entity, resulting in over 1 million dirhams in damages or leading to legal action with the potential of a jail sentence. This level indicates that security requirements for assuring confidentiality are of High importance.

An example of this would be an application that keeps track of letters sent to various offices within the organisation by scanning higher-priority letters and storing them as images in the event the originals are lost or destroyed. While general information such as the sender's name and address is often captured in the image, some letters contain passport numbers or other personal reference numbers. Since unauthorised disclosure of these numbers could result in identity theft, the confidentiality requirement is High.

A second example would be an application that is required to provide sensitive structured personnel and payroll information for the entity. Entities are stakeholders in the analysis and usage of this information, and its unauthorised disclosure or modification could result in fraud or loss of public confidence. The financial impact if this information were to be disclosed could be over 1 million dirhams, so the confidentiality requirement for this application is High.

MODERATE

An application or GSS in this category contains information that could only moderately impact the entity if disclosed. If unauthorised disclosure of information could result in between 100,000 and 1 million dirhams in damages, or lead to legal action without the potential of a jail sentence, security requirements for assuring confidentiality are of Moderate importance.

An example of this would be an application that manages grant abstracts for an entity, and contains home addresses and other sensitive information that must not be disclosed to unauthorised individuals. Although a personal identifier could retrieve these addresses, information must still be protected by an application-specific password or privileges that determine access level. A breach in confidentiality could result in financial damages between 100,000 and 1 million dirhams, so the level of confidentiality for this application is Moderate.

LOW

This category of application or GSS houses general information that is widely available to the public and would not impact the entity if disclosed. This information does not require protection against disclosure, and the impact on the entity's assets and resources would be minor, resulting in less than 100,000 dirhams in damages or possible administrative penalties. This level indicates that security requirements for assuring confidentiality are of Low importance.

An example of this would be an application designed to disseminate information to the public—such as a database of regulations—which contains no proprietary data or information requiring protection due to privacy concerns. Data disclosure would not result in any unfair advantage in activities performed or decisions made based on its revelation.

Integrity

To determine the appropriate level for integrity, consider how the information needs to be protected from unauthorised, unanticipated, or unintentional modification. This should include, but not be limited to, consideration of authenticity, non-repudiation, and accountability (where requirements can be traced to the originating entity)—for example, the nature of loan information processed by an entity that might cause it to be targeted for unauthorised modification. Records retention requirements should also be considered, if applicable.

How the GSS or application is employed in the business process must also be included in the decision. If data contained in the GSS or application is not the sole source of input into the business process, and the normal course of business is to check data provided electronically against the original source, the need for data integrity would be lower than if the data were relied upon to complete the business function. But merely having a backup source of data does not fit this criteria; the data check must be a regular part of the business process.

The following examples can be used as guidance in determining the appropriate rating for integrity.

Examples of integrity considerations:

HIGH

The application is a financial transaction system, and unauthorised or unintentional modification of the information it contains could result in fraud, under- or over-payments of obligations, fines, or penalties resulting from late or inadequate payments. Loss of public confidence could also result.

MODERATE

Assurance of the information's integrity is required to the extent that destruction would mandate significant time and effort devoted to its replacement. While corrupted information could inconvenience staff, most information—and all vital information—is backed up by either paper documentation or on disk.

LOW

This category of GSS or application primarily contains messages and reports. Staff would know if this information were modified by unauthorised, unanticipated, or unintentional means, and these modifications would not be of major concern for the organisation.

Availability

To determine the appropriate level for availability, consider the need for the information to be accessible in a timely manner to meet mission requirements or avoid substantial losses. Availability also includes ensuring that resources are used only for their intended purposes.

The availability requirement must be based on the period of operation during which the GSS or application is most critical to the business function it enables. For instance, if a GSS or application operates only one month out of a year, consider the availability requirement for that month.

The following examples can be used as guidance in making this determination.

Examples of availability considerations:

HIGH

This category of application contains personnel and payroll information relating to employees from various user groups. The application's unavailability could result in the inability to meet payroll obligations and might cause work stoppages and the failure of entities to meet critical mission requirements. It requires 24-hour access.

MODERATE

Information availability in this category is of moderate concern to the mission. Availability would be required within the four- to five-day range, and backups maintained at an off-site storage facility would be sufficient to facilitate limited office tasks.

LOW

In this category, the GSS or application has a duplicate from which the information can be accessed and processed, causing no interruption in the continuity of business functions.

By using these principles to categorise identified assets, the entity can complete an asset inventory list in accordance with the asset inventory template found in Appendix G of this document. The summary from the completed template can be used to populate the impact assessment column of the risk assessment template, as shown in Figure 12.

Step 3 Output:

- *A completed asset inventory (as per the Asset Inventory Template found in Appendix G)*
- *An asset categorisation, based on impact assessment, for each system in terms of confidentiality, integrity, and availability*

Impact Assessment: Enter the rating for the assets which best fits the description of Low, Moderate or High for Confidentiality, Integrity and Availability (as captured in the Asset Inventory Template from Appendix G)

IDENTIFY SUPPORTING ASSETS		IMPACT ASSESSMENT	
STEP 2		STEP 3	
SUPPORTING ASSETS	ADDITIONAL ASSET INFORMATION	IMPACT ASSESSMENT	ASSET INVENTORY
Database server	<doc>	C - H I - L A - L	<doc>
Application servers	<doc>	C - M I - M A - M	<doc>
Front-end clients (desktops)	<doc>	C - H I - L A - L	<doc>
Criminal tracking user group	<doc>	C - M I - H A - M	<doc>
HostingCo Data Centre	<doc>	C - L I - L A - H	<doc>
HostingCo network for hosting clients' services	<doc>	C - H I - H A - H	<doc>

Assessment Inventory: The Asset Inventory Template from Appendix G will help yield the impact ratings insert document referenced in this column

Figure 12: Preliminary Risk Assessment Rating Output for an Asset

3.4 STEP 4: IDENTIFY THREATS

Figure 13: Identify Threats

STEP 4.1: Identify Threat Sources and Actions

Step 4.1 Input: *An inventory of assets that support the processes and services within the scope of the risk assessment.*

A threat is a person, event, or technological function (i.e., threat actor) that can breach the security of an information system. This breach can affect the confidentiality, integrity, or availability of information.

Threat sources can be grouped into three broad categories:

- Human
- Environmental control failures
- Natural disaster

Threat sources that breach security can be either intentional or the by-product of an inadvertent act. For example, the flooding of a data centre may result from intentional malice to water pipes or from inadvertent heavy rain. Figure 14 shows the differences between these concepts.

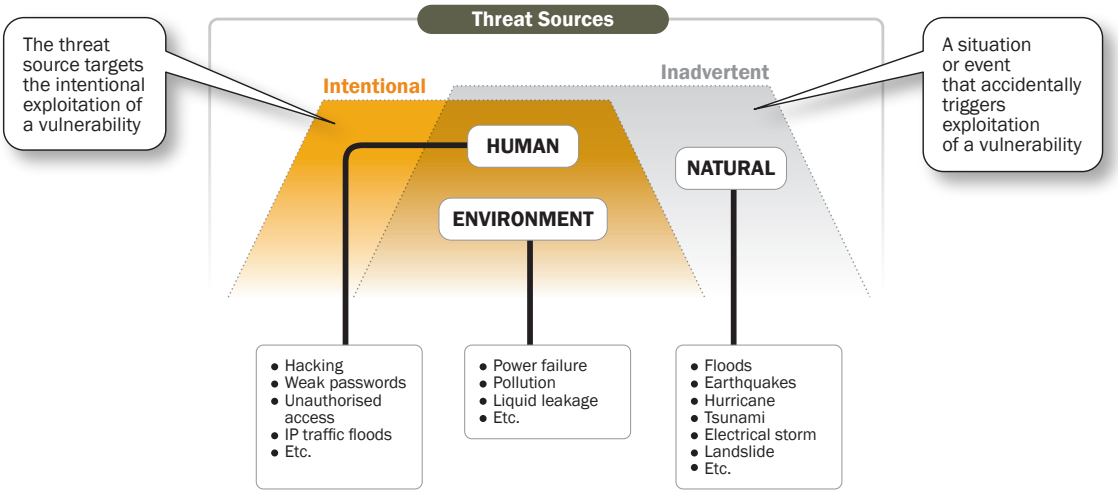


Figure 14: The Intentional and Inadvertent Nature of Threats

For each of the assets identified in Step 2, corresponding threats should also be identified. When identifying threat sources, actions that exploit vulnerabilities should be denoted.

Although it is impossible to exhaustively list all threats, the following table outlines a number of common threat sources and actions. These should be used as a guide when assessing threats to assets within the scope of a risk assessment.

NATURAL DISASTER			
Storm Damage (e.g., flood, snow, hurricane)	Fire	Lightning strikes	Earthquakes
ENVIRONMENTAL CONTROL FAILURE			
Long term power failure	Chemicals	Liquid leakage	Pollution
HUMAN			
Assault on an employee	Arson		Blackmail
Bomb or terrorism	Browsing of private and proprietary information		Civil disorder
Computer abuse	Corrupted data input		Falsified data input
Fraud	Hacking		Impersonation
Interception	Labour dispute or strike		Malicious code
Negligence or human error	Unauthorised disclosure of sensitive information		Password guessing (e.g., dictionary attack)
Vandalism	Sabotage		Social engineering
Spoofing	System tampering		Theft

Table 2: Categorised Examples of Threats

Step 4.1 Output: *Output: For each asset identified in Step 2, a corresponding threat source and action that could exploit any associated vulnerability*

Threat Source: Identify and note the source of threat that can exploit the vulnerability

Threat Action: Briefly describe what actions would lead to the threat source exploiting the vulnerability

IMPACT ASSESSMENT		IDENTIFY THREATS		
STEP 3		STEP 4		
IMPACT ASSESSMENT	ASSET INVENTORY	THREAT SOURCE	THREAT ACTION	COUNTER-THREAT CONTROLS
C - H I - L A - L	<doc>	Entity end user	Attempting to access data not intended for the malicious user	User access at the operating system level is logged so time-stamping may help reveal times of access
C - M I - M A - M	<doc>	Entity end user	Unauthorised access to services on application server	Application LAN firewall drops access to TCP ports 21, 25, and 80
C - H I - L A - L	<doc>	Entity end user	Unauthorised access to unlocked terminal	Application-level timeouts mitigate risk of unauthorised access from unlocked terminals
C - M I - H A - M	<doc>	Entity end user	Modification/ deletion of data	Write access is audited by user
C - L I - L A - H	<doc>	Fire	Overheating of components leading to fire/ malicious fire start/spread	-
C - H I - H A - H	<doc>	User or adversaries on other clients' networks	Routing through VLANs and entering the entity's network	-

Figure 15: Threat Sources and Corresponding Actions, Defined

STEP 4.2: Identify Counter-Threat Controls

Step 4.2 Input: *A list of threats that can exploit asset vulnerabilities*

This step will identify and analyse the controls that are in place to reduce the threats identified in Step 4.1.

Security controls may be technical or non-technical in nature. Examples of technical controls include network firewalls, password-protected access control, anti-virus software, etc.

Non-technical controls can be further divided into management and operational controls. Examples of management controls include security planning, processing authorisations, control sign-offs, etc., while operational controls can include data integrity, incident response, configuration management, and similar types of operations.

Both management and operational controls can be classed as being preventative, corrective, or detective.

- Preventative controls – Stop threats from exploiting a vulnerability (e.g., encrypting data to prevent it from being read by an adversary)
- Corrective controls – Restore systems to a secure state if an error or exploit is detected (e.g., using the restore function to reapply firewall restrictions)
- Detective controls – Raise an alert if a threat source attempts to exploit a vulnerability (e.g., an intrusion detection system)

The assessor should go through each threat defined in Step 5 to identify any technical, management, and/or operational control present to reduce threat impact.

Associated with these threats are the probabilities that the threat will occur with the mitigating controls in place. These can be quantified from historical data on a time-based scale. For example, just like the threat of rain may be three times a month, the threat of physical security breach may be once a year. Threats can be assigned a rating based on their expected occurrence. For the purposes of this risk assessment methodology and current maturity of the Abu Dhabi environment, it will be assumed that all threats can be realised within a time period that covers successive risk assessments. So numerically, this number will be 100% or 1 (based on a probability scale from 0 to 1, representing zero probability to certainty, respectively). The assessor can, however, override this guidance if further information is available at the time of the assessment that would improve the accuracy of the results. This will be discussed further in Step 6.1, Assess Likelihood of Attack.

Step 4.2 Output: *A list of existing controls that prevent, detect, or respond to threats, limiting their impact*

Counter-Threat Controls: Briefly describe any controls that may be present which help counter the threat. This should be borne in mind when determining the likelihood of successful attack.

IMPACT ASSESSMENT		IDENTIFY THREATS		
✓ STEP 3		STEP 4		
IMPACT ASSESSMENT	**ASSET INVENTORY**	**THREAT SOURCE**	**THREAT ACTION**	**COUNTER-THREAT CONTROLS**
C - H I - L A - L	<doc>	Entity end user	Attempting to access data not intended for the malicious user	User access at the operating system level is logged so time-stamping may help reveal times of access
C - M I - M A - M	<doc>	Entity end user	Unauthorised access to services on application server	Application LAN firewall drops access to TCP ports 21, 25 and 80
C - H I - L A - L	<doc>	Entity end user	Unauthorised access to unlocked terminal	Application level timeouts mitigate risk of unauthorised access from unlocked terminals
C - M I - H A - M	<doc>	Entity end user	Modification/ deletion of data	Write access is audited by user
C - L I - L A - H	<doc>	Fire	Overheating of components leading to fire/ malicious fire start/spread	-
C - H I - H A - H	<doc>	User or adversaries on other clients' networks	Routing through VLANs and entering the entities network	-

Figure 16: Identification of Counter-Threat Controls

3.5 STEP 5: IDENTIFY VULNERABILITIES

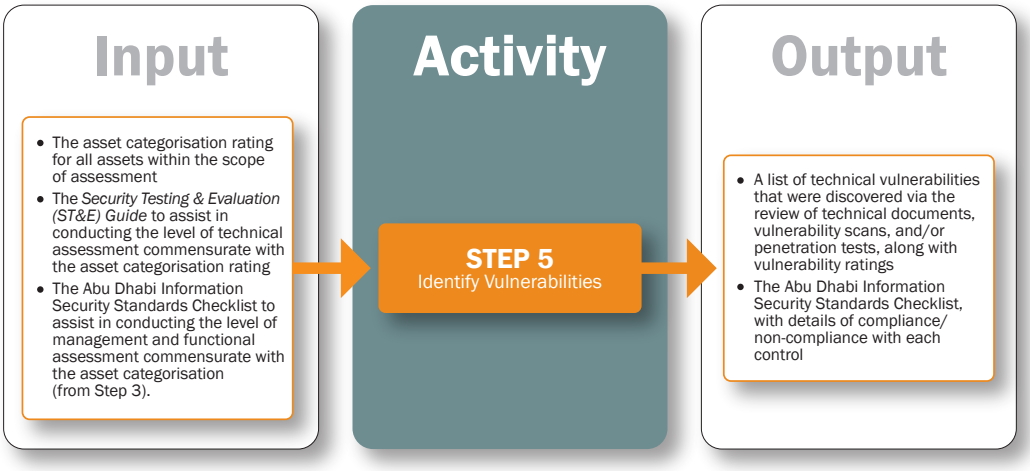


Figure 17: Identify Vulnerabilities

Step 5 Input:

- *The asset categorisation rating for all assets within the scope of the assessment*
- *The Security Testing & Evaluation (ST&E) Guide to assist in conducting the level of "technical assessment" commensurate with the asset categorisation rating*
- *The Abu Dhabi Information Security Standards checklist to assist in conducting the levels of "management" and "functional" assessment commensurate with the asset categorisation from Step 3*

The starting point for assessing asset vulnerability is the *Abu Dhabi Information Security Standards* document.

The Abu Dhabi Information Security Standards covers a range of controls that exist in an ISO/IEC 27001:2005-compliant security management system, most of which cover the management and functional domains of the service under test. For technical domains such as scanning for open ports on a Web server, a technical vulnerability assessment will need to take place. The *Abu Dhabi Information Security Technical Testing Guide* provides guidance on how this can be conducted to support the risk assessment.

The figure below summarises the management, functional, and technical vulnerability assessment approaches of assets with regards to the use of the Abu Dhabi Information Security Standards checklist and the *Information Security Testing Guide.*

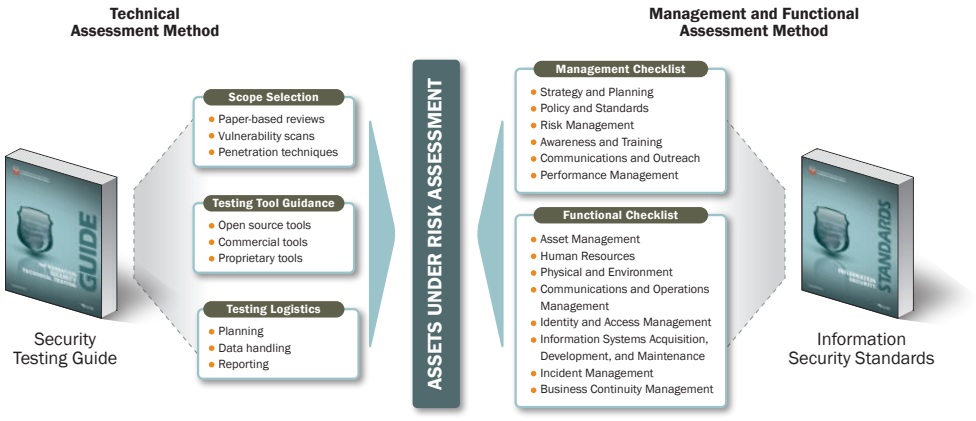


Figure 18: Approaches to Management, Functional, and Technical Vulnerability Assessments

It is expected that this step will produce numerous findings that cannot be easily represented as line items on a risk assessment table. For example, the output of a vulnerability scan may include—in addition to a number of vulnerabilities—the recommended controls. The assessor is advised to capture these details in a separate document, and insert a link to this document in the risk assessment table.

A rating of HIGH, MEDIUM, or LOW should be assigned to each vulnerability that is identified. To ascertain this rating, consider the following examples:

- **HIGH:** To exploit the vulnerability, a threat actor would require minimal resources and have maximum opportunity. An example of this would be a vulnerability on a Web server that has publicly available exploit code.
- **MEDIUM:**
  - To exploit the vulnerability, a threat actor would require minimal resources but have little opportunity. An example of this would be the interception of unencrypted e-mails from an organisation, which would require tapping communication links.
  - To exploit the vulnerability, a threat actor would require a high degree of resources and have ample opportunity. An example of this would be entering a building with an Radio Frequency Identification (RFID) card—something the attacker can try many times by trying to forge an ID card.
- **LOW:** To exploit the vulnerability, a threat actor would require a high degree of resources and have minimal opportunity. An example would be a vulnerability on a server hosted on a corporate Intranet, which would be difficult for an Internet-based attacker to penetrate because he or she would first have to subvert perimeter security.

It should be noted that automated tools used during technical vulnerability assessment may assign default vulnerability ratings. The assessor should check these ratings for consistency before proceeding with the next risk assessment steps.

Step 5 Output:

- *A list of the technical vulnerabilities discovered through the review of technical documents, vulnerability scans, and/or penetration tests, along with their vulnerability ratings*
- *The Abu Dhabi Information Security Standards checklist, with details of compliance/non-compliance for each control*

- **Vulnerabilities Found:** Briefly describe the vulnerabilities found in this column
- **Vulnerability Rating**: In terms of High, Medium or Low
- **Supporting Documentation:** This will be a link to the document containing the detailed findings of the vulnerabilities found in management, operations and technical assets. These documents, at minimum, with be the output of technical testing and a completed ADSIC Security Standards Checklist

IDENTIFY THREATS			IDENTIFY VULNERABILITIES		
STEP 4			STEP 5		
THREAT SOURCE	THREAT ACTION	COUNTER-THREAT CONTROLS	VULNERA-BILITIES FOUND	VULNERA-BILITY RATING	SUPPOR-TING DOCUMENT-ATION
Entity end user	Attempting to access data not intended for the malicious user	User access at the operating system level is logged so time-stamping may help reveal times of access	No user access control for database tables	M	<doc>
Entity end user	Unauthorised access to services on application server	Application LAN firewall drops access to TCP ports 21, 25 and 80	Unused TCP ports 21, 25, and 80 are open on application server	L	<doc>
Entity end user	Unauthorised access to unlocked terminal	Application level timeouts mitigate risk of unauthorised access from unlocked terminals	No user timeout for terminal access	L	<doc>
Entity end user	Modification/ deletion of data	Write access is audited by user	All users are granted write access, whereas most users need read access only	M	<doc>
Fire	Overheating of components leading to fire/ malicious fire		The data centre fire supression system uses water sprinklers	L	<doc>
User or adversaries on other clients' networks	Routing through VLANs and entering the entity's network		Multiple clients in the data centre are using the same switches and segregation relies on VLAN access controls	H	<doc>

Figure 19: Documentation of Vulnerabilities Found

3.6 STEP 6: IDENTIFY RISK

Figure 20: Identify Risk

Risk can be defined as being the product of the impact and likelihood that a security incident will occur. This is shown in the following diagram:

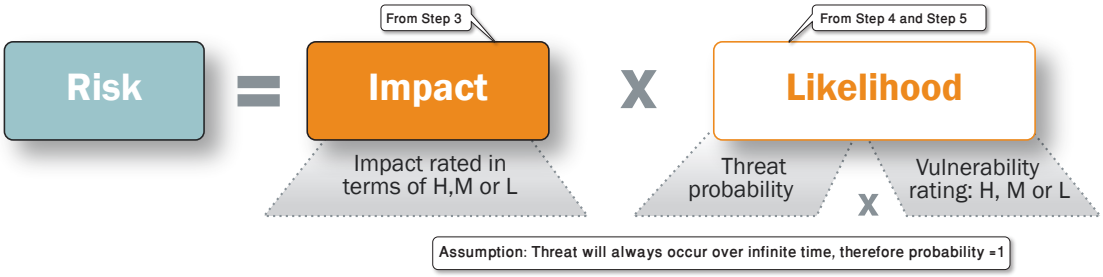


Figure 21: Calculating Risk

STEP 6.1: Assess Likelihood of Attack

Step 6.1 Input: *A list of threats, counter-threat controls for assets, and vulnerability ratings*

This step builds on Steps 4 and 5 to ascertain the likelihood of an attack. It is based upon multiplying the threat probability by the vulnerability ratings.

As discussed in Step 4, associated with threats are the probabilities of their occurrence when mitigating controls are in place. On a time-based scale, these probabilities can be quantified from historical data. For example, the threat of rain may be calculated at three times per month; the threat of physical security breach may be once a year; and the threat of a virus may be three times per year. Threats can be assigned a rating based on their expected occurrence. For the purposes of this risk assessment methodology and the current maturity of the Abu Dhabi environment, it will be assumed that all threats can be realised within a time period that covers successive risk assessments. So numerically, this will be 100% or 1 (based on a probability scale from 0 to 1, representing zero probability to certainty, respectively)[5].

The vulnerability rating that was defined in Step 5 will therefore represent the likelihood of an attack.

Step 6.1 Output: *A rating of the likelihood of a threat occurring for each threat identified for an asset under the risk assessment*

[5] *The assessor can, however, override this guidance if further information is available during the time of assessment. This would improve the accuracy of the results.*

Likelihood of Attack: Threat probability of 1 X vulnerability rating. The likelihood will therefore remain the same as the vulnerability rating, unless the assessor has sufficient information to override this.

IDENTIFY VULNERABILITIES			DETERMINE RISK			
STEP 5			STEP 6			
VULNERABILITIES FOUND	VULNERABILITY RATING	SUPPORTING DOCUMENTATION	LIKELIHOOD OF ATTACK	IMPACT RATING	DETERMINE RISK	RATE RISK
No user access control for database tables	M	<doc>	M	H	M/H	5
Unused TCP ports 21, 25, and 80 are open on application server	L	<doc>	L	M	L/M	2
No user timeout for terminal access	L	<doc>	L	H	L/H	4
All users are granted write access, whereas most users need read access only	M	<doc>	M	H	M/H	5
The data centre fire supression system uses water sprinklers	L	<doc>	L	H	L/H	4
Multiple clients in the data centre are using the same switches and segregation relies on VLAN access controls	H	<doc>	H	H	H/H	6

Figure 22: The Likelihood of an Attack

STEP 6.2: Assess Impact of Attack

Step 6.2 Input: *Impact values for assets from Step 3 (from the generated Asset Inventory List)*

In this step, the impact of an attack on the confidentiality, integrity, and availability of the information asset is assessed.

For the purpose of determining risk in the next step (Step 6.3, Determine Risk), the impact rated highest within the three categories of confidentiality, integrity, or availability should be used. This ensures that the assessment considers the worst-case scenario, and risks are not underestimated.

For example, although read-only access to sensitive data would cause a HIGH confidentiality breach and a LOW integrity breach, the overall impact should be treated as HIGH.

Step 6.2 Output: *Impact rating of highest value for each asset in the Asset Inventory List*

Impact Rating: Insert the highest impact rating level for either confidentiality, integrity or availability from Step 3

IDENTIFY VULNERABILITIES			DETERMINE RISK			
STEP 5			STEP 6			
VULNERABILITIES FOUND	VULNERABILITY RATING	SUPPORTING DOCUMENTATION	LIKELIHOOD OF ATTACK	IMPACT RATING	DETERMINE RISK	RATE RISK
No user access control for database tables	M	<doc>	M	H	M/H	5
Unused TCP ports 21, 25 and 80 are open on application server	L	<doc>	L	M	L/M	2
No user timeout for terminal access	L	<doc>	L	H	L/H	4
All users are granted write access, whereas most users need read access only	M	<doc>	M	H	M/H	5
The data centre fire supression system uses water sprinklers	L	<doc>	L	H	L/H	4
Multiple clients in the data centre are using the same switches and segregation relies on VLAN access controls	H	<doc>	H	H	H/H	6

Figure 23: Assigning Impact Ratings

STEP 6.3: Determine Risk

Step 6.3 Input: *Likelihood and impact ratings for each threat identified in this assessment*

An asset's risk is determined by combining the likelihood and impact of threats on specific vulnerabilities found as a result of Steps 4 and 5. Table 3 shows the possible combinations.

Table for Determining Risk

Likelihood of Risk Occuring \ Impact to Entity	HIGH	MEDIUM	LOW
HIGH	H/H	H/M	H/L
MEDIUM	M/H	M/M	M/L
LOW	L/H	L/M	L/L

Table 3: Combining Likelihood and Impact

Step 6.3 Output: *The combination of likelihood and impact*

Determine Risk: Combine the likelihood of an attack with the highest impact rating

IDENTIFY VULNERABILITIES			DETERMINE RISK			
STEP 5			STEP 6			
VULNERABILITIES FOUND	VULNERABILITY RATING	SUPPORTING DOCUMENTATION	LIKELIHOOD OF ATTACK	IMPACT RATING	DETERMINE RISK	RATE RISK
No user access control for database tables	M	<doc>	M	H	M/H	5
Unused TCP ports 21, 25, and 80 are open on application server	L	<doc>	L	M	L/M	2
No user timeout for terminal access	L	<doc>	L	H	L/H	4
All users are granted write access, whereas most users need read access only	M	<doc>	M	H	M/H	5
The data centre fire supression system uses water sprinklers	L	<doc>	L	H	L/H	4
Multiple clients in the data centre are using the same switches and segregation relies on VLAN access controls	H	<doc>	H	H	H/H	6

Figure 24: Risk Levels for Each Vulnerability and Threat Combination

STEP 6.4: Determine Risk Score

Step 6.4 Input: *A risk determination in terms of likelihood and impact*

Determining a risk score allows for a clearer picture of which risks are more prevalent and will require more attention when deciding upon treatment.

To determine the score of the risks identified in Step 6.3, a risk rating scale is used.

This scale, shown in the following figure, allows a numerical value to be assigned to the risks discovered in Step 6.3.

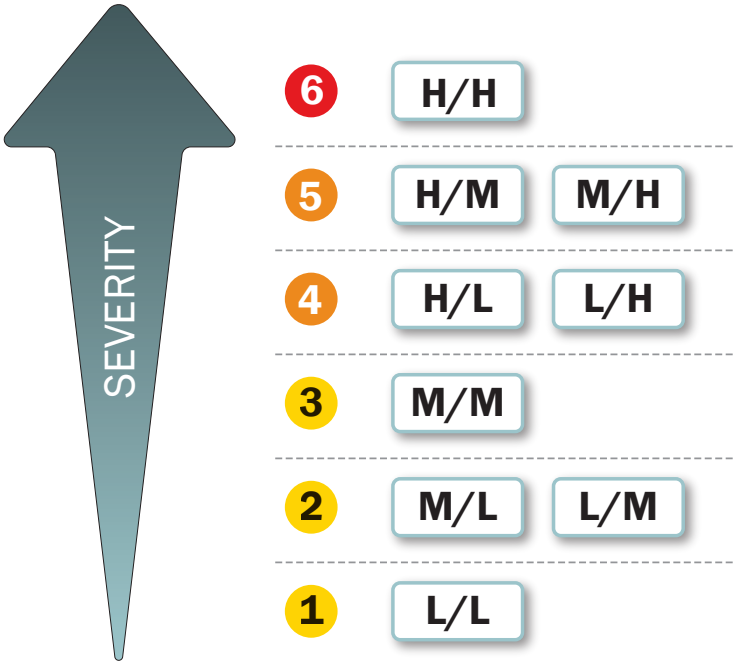


Figure 25: Risk Rating Scale

The risk rating scale ranges from “1 – L/L” denoting the lowest risk to “6 – H/H” being the most severe. Each likelihood/impact combination is assigned a number to allow for easy sorting in terms of severity.

Weighting of an H risk is considered proportionally higher than that of an M risk. Therefore, an H/L is higher than an M/M. Any risk that constitutes an H impact or likelihood will be classified as Level 4 or above.

Step 6.4 Output: *A list of risks based on a numerical risk rating scale*

Rate Risk: Transpose the risk to a number between 1 and 6 using the Risk Rating Scale

IDENTIFY VULNERABILITIES			DETERMINE RISK			
✓ STEP 5			STEP 6			
VULNERABILITIES FOUND	VULNERABILITY RATING	SUPPORTING DOCUMENTATION	LIKELIHOOD OF ATTACK	IMPACT RATING	DETERMINE RISK	RATE RISK
No user access control for database tables	M	<doc>	M	H	M/H	5
Unused TCP ports 21, 25 and 80 are open on application server	L	<doc>	L	M	L/M	2
No user timeout for terminal access	L	<doc>	L	H	L/H	4
All users are granted write access, whereas most users need read access only	M	<doc>	M	H	M/H	5
The data centre fire supression system uses water sprinklers	L	<doc>	L	H	L/H	4
Multiple clients in the data centre are using the same switches and segregation relies on VLAN access controls	H	<doc>	H	H	H/H	6

Figure 26: Risk Levels Aligned to Risk Scale

3.7 NEXT STEPS

This *Risk Assessment Guide* provides instructions on identifying assets that support the service identified by ADSIC for assessment, and identifying and prioritising these assets' risks.

Once the risk assessment template has been completed, the assessor should create a risk assessment report using the template found in Appendix E of this Guide. This report will draw upon the information from the currently completed steps.

The risk assessment report will be used to treat the identified risks in a prioritised manner, mitigating them to an acceptable level in accordance with the security requirements for Abu Dhabi Government e-Services.

The step-by-step process used to treat risks can be found in the *Information Security Planning Guide*. Risks that remain untreated or partially treated carry a residual risk (i.e., the risk that remains following treatment).

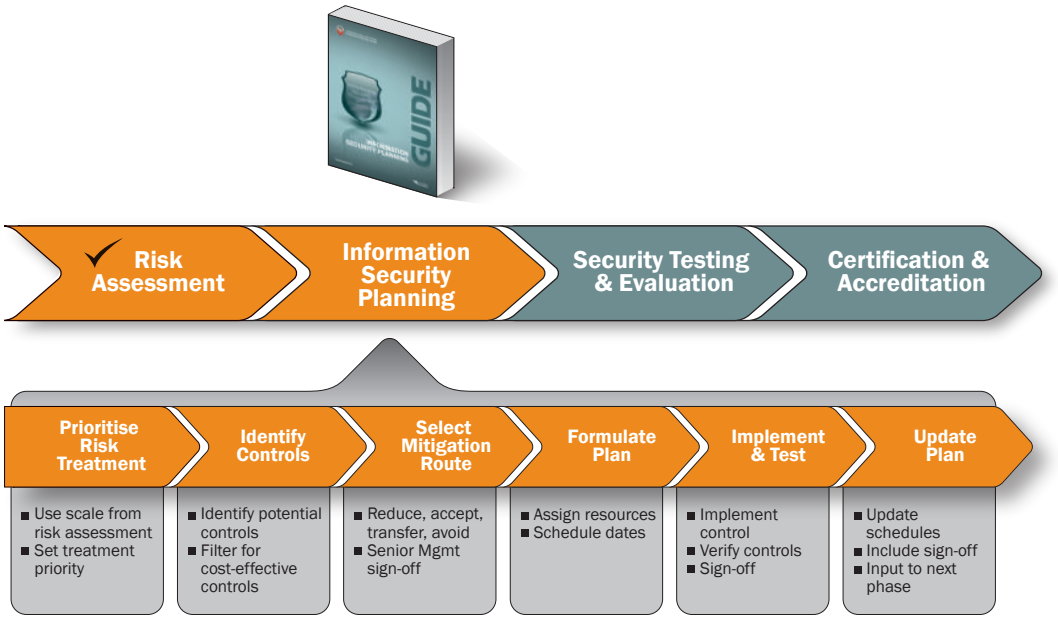


Figure 27: Overview of the Next Phase: Information Security Planning

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 Information Security Planning Guide, December 2008.

Abu Dhabi Security Testing and 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, December 2008.

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

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 ASSESSMENT TEMPLATE

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

APPENDIX E: RISK ASSESSMENT REPORT FORMAT

Once the risk assessment template has been completed by following the steps in this Guide, the following format should be used to complete the final report in accordance with this key:

Normal text – Include this text in your final report

<Italicised text> – Directions for creating and adding your content

[Blue Italicised text] – Provided as a placeholder for your content

RISK ASSESSMENT REPORT

FOR [NAME OF SERVICE]

1. EXECUTIVE SUMMARY

<Provide a high level summary of risk assessment methodology and findings that is suitable for a senior executive audience. Briefly describe assets categorisation, data gathering techniques, and ratings definitions from Step 3, and the asset inventory, and list the total number of 1-to-6 severity risks that were discovered in Step 6.4.>

2. INTRODUCTION

This risk assessment was conducted in response to the requirements of the following:

- Abu Dhabi Government ISGP requirements

<Include the following sections: purpose, background, scope, and structure.>

Purpose

<Explain the purpose of conducting a risk assessment for the entity (e.g., to comply with Abu Dhabi's ISGP requirements). Include the date of the most recent risk assessment. Reserve detail for scope statement below.>

Background

<Provide an overview of the system's categorisation (Step 3) and current development phase. Include a brief description of the risk assessment team and the analysis process.>

Scope

<Describe the elements of the network, architecture, system components, field site locations (if any), and any other details about the system considered in the analysis. References to appropriate diagrams included in the appendices should be inserted here, as they will assist others in understanding the scope of the project. The outputs of Step 1 will assist in documenting this.>

Structure

<Describe the organisation structure of the risk assessment report document.>

3. RISK ASSESSMENT APPROACH

<Define system boundaries, describe information gathering techniques, and outline steps taken to complete the risk assessment. Include ratings, definitions, and the risk-rating matrix used.>

4. SYSTEM CATEGORISATION

<Provide the fullest description of the system categorisation (from Step 3 and asset inventory) to identify system resources and information that constitute the system and its boundaries. The categorisation should provide a system overview and describe interfaces, users, data content, mission criticality, and information sensitivity. This will provide the foundation for the remaining steps in the Risk Management process. Use the system categorisation statement to give readers a detailed view of the hardware, software, and setup examined.>

5. SYSTEM OWNER(S)

<Complete a table for each system that supports the service.>

NAME:	*[Insert name of System Owner]*
TITLE:	*[Insert job title]*
ENTITY/ DEPARTMENT:	*[Insert entity/department]*
ADDRESS:	*[Insert address]*
TELEPHONE:	*[Insert telephone number]*
E-MAIL:	*[Insert e-mail address]*
RESPONSIBILITY:	The System Owner is responsible for defining the system's operating parameters, authorised functions, and security requirements. *<Note: The System Owner and the authorising official may be the same individual.>*

6. AUTHORISING OFFICIAL

NAME:	*[Insert name of authorising official]*
TITLE:	*[Insert job title]*
ENTITY/ DEPARTMENT:	*[Insert entity/department]*
ADDRESS:	*[Insert address]*
TELEPHONE:	*[Insert telephone number]*
E-MAIL:	*[Insert e-mail address]*
RESPONSIBILITY:	Senior management official who has the authority to authorise processing and accept the risk associated with the application. *<Note: The System Owner and the authorising official may be the same individual.>*

7. OTHER DESIGNATED CONTACTS

<Include other individuals who have significant responsibilities regarding the information system/ application. Examples include system administrator, security administrator, database administrator, and relevant site personnel. Provide a custom description for each individual's responsibilities. Create additional tables for as many individuals in this section as necessary.>

NAME:	*[Insert name of other designated contact]*
TITLE:	*[Insert job title]*
ENTITY/ DEPARTMENT:	*[Insert entity/department]*
ADDRESS:	*[Insert address]*
TELEPHONE:	*[Insert telephone number]*
EMAIL:	*[Insert e-mail address]*
RESPONSIBILITY:	*<Include custom description of the individual's responsibilities.>*

8. OVERALL SECURITY RESPONSIBILITY

NAME:	*[Insert system security manager's name]*
TITLE:	*[Insert job title]*
AGENCY/ DEPARTMENT:	*[Insert agency/department]*
ADDRESS:	*[Insert address]*
TELEPHONE:	*[Insert telephone number]*
E-MAIL:	*[Insert e-mail address]*
RESPONSIBILITY:	Assigned responsibility to ensure that the system has adequate built-in security measures.

9. SYSTEM OPERATIONAL STATUS[6]

[Insert system name] is currently in the *[Insert phase – see below]* phase in accordance with the system development life cycle (SDLC) *[Insert system name] [Insert "is targeted for deployment by" or "has been deployed since"] [Insert deployment date]*.

[6] *This section pertains to the operational status of the systems within the scope of this risk assessment. Note that the operational status of the systems has an impact on the operational status of the service. For example, if the system is in non-operational state then it is likely the service is also non-operational or operating at a reduced state.*

<Indicate status of the system:

- *Operational – the system is in production*
- *Under development – the system is being designed, developed, or implemented*
- *Undergoing a major modification – the system is undergoing a major conversion or transition.>*

<If the system is under development or undergoing a major modification, provide information about methods used to assure that up-front security requirements are being included. Include specific controls in the appropriate sections of the plan depending on where the system is in the security life cycle.>

10. THREAT STATEMENT

<Identify and explain existing threats to the service under assessment—both sources and actors—being considered when developing the threat and vulnerability pairs in the Findings section. Steps 5 and 6 will assist with this.>

11. FINDINGS

<Include a separate discussion for each threat and vulnerability pair resulting from an analysis of the threat statement and vulnerability list (from Step 4). This discussion should include the identification of existing mitigating security controls (from Step 6), impact analysis discussion (from Step 8), and risk rating (from Step 10).>

12. APPENDICES

<Include a few descriptive sections, such as system diagram, anticipated major changes/upgrades, glossary of terms, list of references, and a list of acronyms and abbreviations. The system diagram is particularly important, as it will provide staff and administration with an overall view of the architecture employed by systems supporting the service and the individual components mentioned in the report. Additionally, a list of key staff members (other than those identified above) with contact information to include telephone and e-mail is helpful.>

APPENDIX F: WORKED EXAMPLE

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

APPENDIX G: ASSET INVENTORY TEMPLATE

The template below is provided to record asset inventory information during risk assessment.

CATEGORY (CHECK ONE)		EXPLANATION	REFERENCE
AUTOMATED INFORMATION RESOURCE	• General Support System (GSS) • Major Application (MA) Identified as: ▫ Mission-critical or important; or ▫ Mission-supportive and an Information Sensitivity cate gory rated as “Moderate” or “High” • Application Identified as mission-supportive and all Information Sensitivity categories rated as “Low”	Business Function: Data: Hardware: Hardware Location: Software: Software Location: In development or operational:	Include business processes that the automated information resource accomplishes, such as the type of data it contains and technical information (hardware, hardware location, software, software location, etc.) Risk Assessment Guide: Step 2
INFORMATION SENSITIVITY	Confidentiality ▫ High ▫ Moderate ▫ Low		Risk Assessment Guide: Step 3
	Integrity ▫ High ▫ Moderate ▫ Low		Risk Assessment Guide: Step 3
	Availability ▫ High ▫ Moderate ▫ Low		Risk Assessment Guide: Step 3