مركز أبوظبي للأنظمة الإلكترونية والمعلومات
Abu Dhabi Systems & Information Centre

Information Security Programme

The Emirate of Abu Dhabi

GUIDE

CERTIFICATION & ACCREDITATION

Version 1.0

أبوظبي
abudhabi

GUIDE

CERTIFICATION & ACCREDITATION

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

Certification and Accreditation (C&A) is the fourth phase of the Risk Management process and is a means for Abu Dhabi Government Entities (ADGEs) to endorse the effectiveness of their overall risk management. During certification, management and functional security controls are assessed to determine their effectiveness in providing security for Abu Dhabi Government services. Certification is a formal declaration that the security controls implemented on a system are adequate to reduce security risks to an acceptable level. During accreditation, the Designated Approval Authority (DAA) then makes a decision to authorise a service to operate and accept its residual risks. The same official can also make a decision to stop the operation of the information service if they decide that the information service has an unacceptable level of security risks. Certification and Accreditation plays a critical role in successfully implementing the Risk Management process.

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

This document is a guide that enables readers to perform Certification and Accreditation of their service's information security efforts. Certification and Accreditation is the final phase of the Risk Management process and aims to ensure that all security controls are implemented properly and justly approved by management - in accordance with the *Abu Dhabi Information Security Policy* and *Abu Dhabi Information Security Standards.* It is therefore essential that each entity allocates the appropriate resources to successfully implement the Certification and Accreditation process based within this guide.

The *Certification and Accreditation Guide* is supported by additional accompanying Risk Management guidance (e.g., *Risk Assessment Guide, Information Security Planning Guide, Security Testing & Evaluation Guide, and Information Security Standards*[1]). These documents will provide the necessary guidance to help ADGEs 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 more detailed explanation of the Abu Dhabi Risk Management process, please refer to the *Abu Dhabi Risk Management Guide.*

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

1.2 SCOPE

The *Certification and Accreditation Guide* approaches security from an information perspective, beyond the traditional focus of information technology, ensuring 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, with the main goal of directing the programme to assure Government missions rather than only security. Each of these related assurance discipline areas are included within this programme and contain specific activities to ensure integration under a mission assurance umbrella.

1.3 APPLICABILITY

The *Certification and Accreditation 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 the *Abu Dhabi Information Security Policy*, compliance with the Risk Management process is mandatory[3] and Certification and Accreditation *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. Certification is the means by which all ADGEs can have assurance that proper diligence has been applied to the implementation of security controls for each service. Accreditation is then the means by which all ADGEs can have assurance that residual risk is accepted by the Designated Approval Authority and that someone is ultimately accountable for the operations of the service.

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

1.5 DOCUMENT LAYOUT

After reading this document, the user should have a clear understanding of his/her responsibilities with regard to certifying and accrediting services. This document also gives an overview of the Risk Management process and where Certification and Accreditation fits into the overall process. It will provide the reader with the information and tools needed to begin Certification and Accreditation and ensure the security of Abu Dhabi Government services.

---

[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.*

This document has three main sections:

- **Section 1** provides the overview, background, and purpose for this document. This section answers the question, “Why should Government services be certified and accredited?”
- **Section 2** answers some of the frequently asked questions about Certification and Accreditation.
- **Section 3** describes Certification and Accreditation methodology, and answers the question, “How to certify and accredit a service?”
- **Appendices** provide templates and references for Certification and Accreditation, including Summary of Security Risks Report and templates for Authority to Operate, Denial to Operate, etc.

2. FREQUENTLY ASKED QUESTIONS

2.1 WHAT IS THE PURPOSE OF CERTIFICATION AND ACCREDITATION?

Certification and Accreditation provides a means for ADGEs to endorse the effectiveness of their overall Risk Management process. A consistent application of Certification and Accreditation across ADGEs will make Abu Dhabi Government systems more secure and will provide more complete, consistent information for senior officials about the Government services and its supporting systems to facilitate accreditation decisions.

2.2 ARE CERTIFICATION AND ACCREDITATION THE SAME THING?

Certification and Accreditation are different activities. Certification is a comprehensive assessment of the management and functional controls. During certification, the Certifying Official verifies that the three initial phases of the Risk Management process were conducted properly and that management and functional controls are effectively implemented to provide the desired level of security commensurate to the categorisation of the service and its potential risk to the Abu Dhabi Government. The Certifying Official also highlights any remaining risks for Designated Approval Authority review. Certification results are then used to make a decision for accreditation.

Accreditation is the official management decision given by a senior entity official to authorise operation of an information service. Its purpose is to provide a means for senior Government officials to be informed of the security risks and to officially authorise a service to operate by accepting these residual risks to the service and the entity.

2.3 WHO IS A DESIGNATED APPROVAL AUTHORITY?

The Designated Approval Authority (DAA) is the person who formally accredits or accepts the remaining risks to the Government service and its supporting systems. The DAA is a senior Government official of the ADGE and is appointed by the Chairman. He or she is responsible for the security of all of the entity's services and its supporting systems.

2.4 WHEN DOES CERTIFICATION AND ACCREDITATION OCCUR?

Certification and Accreditation is the fourth phase of the Risk Management process and occurs after the Security Testing & Evaluation phase. The Risk Management process should be a part of the system development lifecycle from the very beginning and the earlier it is incorporated into the lifecycle, the easier it will be to incorporate security controls. Ideally, Certification and Accreditation should occur prior to the system's operations or "going live". After the service is granted accreditation, continuous monitoring of security controls is conducted for as long as the service is operational.

2.5 WHO IS RESPONSIBLE FOR CERTIFICATION AND ACCREDITATION?

The System Owner is ultimately responsible for shepherding the Government service through Certification and Accreditation. He or she is an official of the ADGE who is responsible for the procurement, development, maintenance, and operations of the information system. The System Owner is also responsible for the security of the Government service and ensures that resources are assigned.

2.6 DO ALL GOVERNMENT SERVICES AND ITS SUPPORTING SYSTEMS OF THE ABU DHABI GOVERNMENT ENTITY (ADGE) REQUIRE CERTIFICATION AND ACCREDITATION?

Yes. All Government services require Certification and Accreditation because Risk Management process is mandatory for all ADGE systems and Certification and Accreditation is a key component of this process. Only when this phase is complete will an official have reviewed the effectiveness of the security controls for the service, formally accepted associated risks, *and approved the* service *for operation.* Consistent application of Certification and Accreditation across ADGEs will make Abu Dhabi Government services more secure, provide more complete, consistent information to senior officials about their Government services, and facilitate security accreditation decisions.

2.7 WHAT IF THE GOVERNMENT SERVICE IS NOT CERTIFIED AND ACCREDITED?

If the Government service is not certified and accredited, it will not be approved for operation and should have all of its functions stopped or discontinued.

2.8 HOW OFTEN DOES A GOVERNMENT SERVICE NEED TO BE CERTIFIED AND ACCREDITED?

ADGE services 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 service. This ensures that information security is up to date with all current threats and vulnerabilities.

2.9 HOW DOES THIS RELATE TO ISO/IEC 27001:2005 CERTIFICATION?

The security standards that are assessed during Certification and Accreditation were developed using ISO/IEC 27001:2005 and 27002:2005 as a base reference. The *Abu Dhabi Information Security Standards* were developed to be more compatible with Abu Dhabi Government environment. The Risk Management process is based on security controls that are defined in the *Information Security Standards.* If ISO/IEC 27001:2005-based controls have been implemented, they should be very close to satisfying the controls that will be assessed if the service is categorised as 'LOW'. Some of the 'MODERATE' and 'HIGH' controls go beyond the ISO/IEC 27001:2005-based controls.

2.10 HOW DOES THE PROCESS DIFFER FOR HIGHER RISK SERVICES?

For services that are categorised as 'LOW', the entity can certify and accredit the services themselves. For services categorised as 'HIGH', however, Abu Dhabi Systems & Information Centre (ADSIC) must conduct the certification to validate the risk assessment report and the related Information Security Plan.

For a service categorised as MODERATE, the Designated Approval Authority makes the decision to either self-certify or ask ADSIC to certify.

2.11 CAN A VENDOR CERTIFY A GOVERNMENT SERVICE?

While ADGEs can hire an outside vendor to handle some risk management activities, the Certifying Official and Designated Approval Authority must be Government officials. The Designated Approval Authority is a senior Government official appointed by the Chairman of the entity and the Certifying Official for MODERATE and LOW services is assigned by the entity's Designated Approval Authority. ADSIC must certify services categorised as HIGH.

The Certifying Official can assign a third party or a contractor to conduct Step 1: Initiation or Step 4: Continuous Monitoring of the Certification and Accreditation. However, Step 2: Security Certification and Step 3: Security Accreditation must be conducted by a Government official.

3. CERTIFICATION AND ACCREDITATION STEPS

Methodology

Certification and Accreditation encompasses four steps.

STEP 1: Initiation

STEP 2: Security Certification

STEP 3: Security Accreditation

STEP 4: Continuous Monitoring

All steps are mandatory. Each relies upon output from the previous step and must be done in order. The sequence of these steps is shown in following figure:

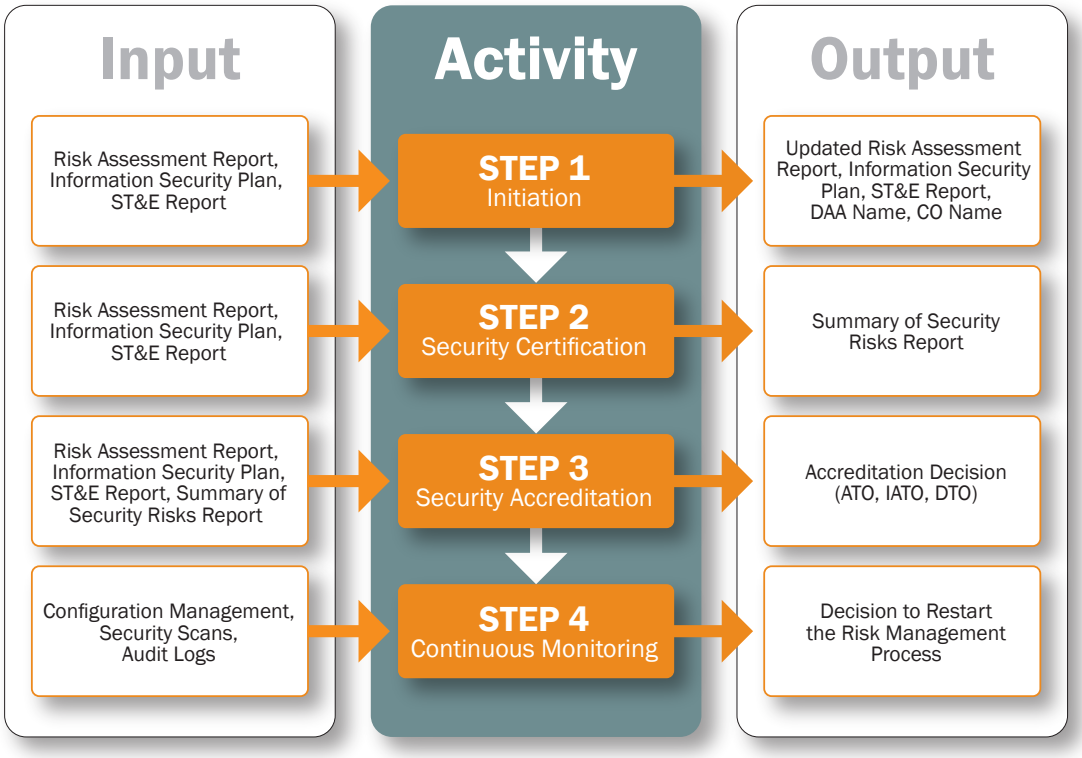

Figure 2: Certification and Accreditation Steps

3.1 STEP 1: INITIATION

Figure 3: Initiation

Step 1 Input: *Risk Assessment Report, Information Security Plan, Security Testing & Evaluation Report*

The purpose of the initiation phase is to communicate Certification and Accreditation activities to all key parties and also gather necessary information. The Certifying Official (CO) can assign a vendor, contractor, or third party to conduct initiation activities. In the initiation phase, key parties of the Certification and Accreditation activity are notified to make them aware that the service is about to be formally authorised to operate by the Designated Approval Authority. At a minimum, the key parties should include the System Owner, Designated Approval Authority, Certifying Official, ADSIC, and ADG-ISO. The Designated Approval Authority is appointed by the Chairman for all levels of services (i.e., LOW, MODERATE, and HIGH). For HIGH services, a Certifying Official is assigned by ADSIC to conduct certification activities. For MODERATE and LOW services, the entity's Designated Approval Authority assigns a Certifying Official.

Once the key parties of the Certification and Accreditation activity are notified, the risk management documents developed in the previous three phases are gathered. These include the following:

- **Risk Assessment –** From Phase 1 of the Risk Management process
- **Information Security Plan –** From Phase 2 of the Risk Management process
- **ST&E Report –** From Phase 3 of the Risk Management process
- **Certification Recommendation Letter –** Applies only to MODERATE and HIGH services, and is provided by the independent organisation that conducted the ST&E

The Certifying Official reviews these documents to ensure that they are complete; if they are not complete, this phase cannot continue. At a minimum, they must contain the following information:

- Information security categorisation (LOW, MODERATE, HIGH) determined during risk assessment
- Vulnerabilities identified during risk assessment and ST&E
- Security controls compliance (all applicable Abu Dhabi Information Security Standard Controls are documented in the Information Security Plan)

Updates should be made if new security controls have been implemented, or if changes have been made to the security controls. Typically, the most current status of the security controls should be documented prior to Certification and Accreditation phase, but if new controls were implemented, this can affect the accreditation decision and it is the responsibility of the System Owner to communicate the new information to the Certifying Official. The Certifying Official must decide which method will be used to verify that controls have been properly implemented (e.g., request a document proof, redo the ST&E, etc). When all information has been updated, the Security Certification Phase takes place.

Step 1 Output: *Updated Risk Assessment Report, Information Security Plan, ST&E Report, Designated Approval Authority (DAA) Name, Certifying Official (CO) Name*

Note: information services should not go to Security Certification unless the System Owners are confident that the security controls will pass the ST&E.

3.2 STEP 2: SECURITY CERTIFICATION

Figure 4: Security Certification

Step 2 Input: *Updated Risk Assessment Report, Information Security Plan, ST&E Report*

In this phase, management and functional controls are assessed, with the Certifying Official essentially certifying that all activities in the previous three phases were conducted properly. The Certifying Official evaluates the documents for the following information:

- All controls from the *Abu Dhabi Information Security Standards* were properly assessed in all phases (i.e., Risk Assessment, Information Security Planning, ST&E).
- All controls assessed as "not applicable" were carefully reviewed.
- Consistency of findings – risks identified in the Risk Assessment are reviewed to ensure that they were addressed in the Information Security Plan. The ST&E Report should be reviewed for any **new risks** that were not identified during the previous phases.
- Verification that an independent ADSIC - appointed organisation conducted the Security Testing & Evaluation for 'MODERATE' and 'HIGH'' services.

At the end of this phase, the Certifying Official will determine which security controls are improperly implemented or missing and pose a threat to the service.

After all updates are made and all documents have been reviewed, an Accreditation Package is prepared that consists of the following:

- **Risk Assessment**
- **Information Security Plan**
- **ST&E Report**
- **Summary of Security Risks Report** (a template for this is provided in Appendix D of this document)

The **Summary of Security Risks Report** contains the following:

- **List of remaining risks or vulnerabilities**
- **Recommendations or plan to mitigate these remaining risks**

The Summary of Security Risks Report is compiled from the Risk Assessment, Information Security Plan, and the ST&E Report. It summarises the risks associated with the vulnerabilities identified during the first three phases of the Risk Management process.

The Summary of Security Risks Report is prepared by the Certifying Official, who uses the Risk Assessment Report, Risk Treatment Plan, and the Information Security Plan to list all of the non-mitigated vulnerabilities in the table that follows the template of Table 1. All vulnerabilities from

the ST&E report are also listed in this table to capture all remaining risks and vulnerabilities in one place. If vulnerabilities are mitigated as the Certification and Accreditation process progresses, and the results of the mitigation are confirmed, they can be deleted from the list. The Certifying Official must decide which method to be used to verify that controls have been properly implemented (e.g., request a document proof, redo the ST&E, etc.).

RISK/ VULNERABILITY	SOURCE	LIKELIHOOD	IMPACT	DETERMINE RISK	RATE RISK
e.g., password policy not enforced making system vulnerable	i.e., Risk Assessment, ST&E Internal, ST&E External, other	e.g., L, M, H	e.g., L, M, H	e.g., H/H, H/M, L/M, etc.	Scale of 1-6

Table 1: Remaining Risks/Vulnerabilities

After the Remaining Risks/Vulnerabilities table is completed, the Total Number of Risks/ Vulnerabilities Table will show the number of risks/vulnerabilities.

OVERALL FINDINGS						
Risk Levels	1	2	3	4	5	6
Number of Findings						

Table 2: Total Number of Risks/Vulnerabilities

The Certifying Official will provide a recommendation to the Designated Approval Authority on what type of accreditation the service should receive: Authority to Operate, Interim Authority to Operate, Denial to Operate.

- ***Authority to Operate (ATO)*** is granted when the Designated Approval Authority officially accepts the remaining risks for the service and allows the service to operate for a period of up to 36 months. At the end of this period, the service will need to restart the Risk Management process from Phase 1: Risk Assessment. ATOs are typically granted to services without risks that are rated as HIGH (i.e., 4 or higher, although the Designated Approval Authority has discretion to grant an ATO regardless of risk rating). HIGH services should conduct annual testing to ensure that their security controls are still effective. Failure to conduct annual testing will result in the ATO becoming invalid. Services rated MODERATE or LOW are also at the discretion of the Designated Approval Authority.
- ***Interim Authority to Operate (IATO)*** is granted when the Designated Approval Authority officially accepts the remaining risks for the service and allows the service to operate for a period of up to six months. An IATO will list the reason why the service was not granted an ATO, as well as the conditions for an ATO to be obtained typically, to fix any moderate to high risks that remain. Before the specified period ends, the System Owner will need to resubmit the certification package to enable the service to be granted an ATO.
- ***Denial to Operate (DTO)*** is given when the Designated Approval Authority determines that the service has unacceptable risks. If a service receives a DTO, the Designated Approval Authority has the authority to stop its operation.

For MODERATE and HIGH services, the organisation that conducted the ST&E or the System Security Certification Testing (i.e., ST&E conducted by an independent organisation) will provide a Certification Recommendation Letter stating what type of accreditation (Authority to Operate, Interim Authority to Operate, or Denial to Operate) it recommends to the Designated Approval

Authority. The Certifying Official will also make a recommendation as to what type of accreditation the service should receive after reviewing the ST&E report and Certification Recommendation Letter. The Certifying Official provides a recommendation in addition to the independent organisation's Certification Recommendation in consideration of the Certifying Official potentially having a differing interpretation of the severity of vulnerabilities.

Finally, for all remaining low level risks, a mitigation plan should be outlined that provides at a minimum the information shown in the table below. This is to show the Designated Approval Authority that a plan is in place to fix and mitigate the remaining risks. Without the plan, the Designated Approval Authority may decide to grant the organisation a Denial to Operate instead of an Interim Authority to Operate because the lack of plan to mitigate remaining vulnerabilities can also be considered a risk.

RISK/ VULNERABILITY	RATE RISK	CORRECTIVE ACTIO	COMPLETION DATE	POINT OF CONTACT
e.g., password policy not enforced making system vulnerable	Scale of 1-6	Enforce password policy	10 Oct 2008	John.doe@ad.gov

Table 3: Sample Mitigation Plan

Finally, the **Summary of Security Risks Report** will be sent to the Designated Approval Authority. A template for this report is provided in Appendix D of this document.

Step 2 Output: *Summary of Security Risks Report*

3.3 STEP 3: SECURITY ACCREDITATION

Figure 5: Security Accreditation

Step 3 Input: *Updated Risk Assessment Report, Information Security Plan, ST&E Report*

In the Security Accreditation phase, the Designated Approval Authority reviews the accreditation package and formally accepts the remaining risks for the service. Typically, services will have some remaining risks either because they cannot be mitigated or the cost of fixing the risk outweighs the benefits. For example, an information system may have a risk that may not be technically feasible to directly address due to outdated technology.

The Designated Approval Authority will then make a determination to issue one of the following types of security accreditation (consistent with the aforementioned definitions):

- Authority to Operate (ATO)
- Interim Authority to Operate (IATO)
- Denial to Operate (DTO)

As a rule, a service that has any risks with a rating of 6 should receive a DTO. If a service receives an IATO, the System Owner should provide a mitigation plan to the Designated Approval Authority that explains how the risks will be mitigated in a given time period. A service with risks at a scale of 4-5 should be given an IATO. A service with less than 10 vulnerabilities rated at 4 or 5 will be given an IATO of 12 months. A service with 10 or more vulnerabilities rated at 4 or 5 will be given an IATO of 6 months. However, these are general guidelines, and it is up to the Designated Approval Authority to decide what the acceptable and unacceptable risks to an entity are.

Step 3 Output: *Accreditation Decision (i.e., Authority to Operate, Interim Authority to Operate, Denial to Operate)*

3.4 STEP 4: CONTINUOUS MONITORING

Figure 6: Continuous Monitoring

Step 4 Input: *Configuration Management, Security Scans, Audit Logs*

After a service has gone through Certification and Accreditation, the entity must continue to follow the Risk Management process to maintain Certification and Accreditation status. The purpose of this phase is to continuously monitor security controls following accreditation.

The entity must determine and document configuration controls, monitor and ensure that security controls are in place, and continuously update the Information Security Plan if the information service goes through changes. A change management process should be in place to document changes that are made to the information system and these changes must be tracked and their impact analysed.

Information systems should be regularly assessed to identify new and emerging vulnerabilities. HIGH services should conduct annual testing to ensure that their security controls are still effective. Failure to conduct annual testing will result in their ATO becoming invalid. The most common approach during this phase to monitor technical controls is conducting periodic (e.g., quarterly) vulnerability scanning. Effective continuous monitoring also provides the benefit of making reaccreditation (i.e., when the ATO or IATO expires) an easier process.

Finally, if significant changes are made to the information system that affects the system's security (e.g., a new server to add functionality which exposes the system), the entity must go through the Risk Management process from Phase 1 – Risk Assessment to Phase 4 - Certification and Accreditation. The following lists a few examples that could potentially warrant a service to go through the Risk Management process:

- Operating system upgrade
- Addition of major new functionalities to the server
- Database migration
- Single sign-on implementation

When such a change is planned, the following questions must be asked:

- What is the change?
- Does it affect any of the security controls in the Information Security Standards in a way that will create new vulnerabilities?
- Does this change have any impact on the security functionality of the information system?

If the answer is yes, the Chief Information Security Officer must complete a table similar to Table 4 below to document the new risk/vulnerability. If any risk/vulnerability has a risk rating of 4 or above, the service will usually need to go through the Risk Management process again. However, it is for the Designated Approval Authority to decide whether the service will need to repeat this process.

RISK/ VULNERABILITY	SOURCE	LIKELIHOOD	IMPACT	DETERMINE RISK	RATE RISK
e.g., password policy not enforced, making system vulnerable	i.e., Risk Assessment, ST&E Internal, ST&E External, other	e.g., L, M, H	e.g., L, M, H	e.g., H/H, H/M, L/M, etc.	Scale of 1-6

Table 4: Risk Table for Changes

Satisfying the Certification and Accreditation phase completes the Risk Management process and gives the entity the assurance that appropriate security controls are in place to provide adequate security for its service.

Step 4 Output: *Decision to restart Risk Management process*

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 Information Security Planning Guide, December 2008.

Abu Dhabi Security Testing and Evaluation Guide, December 2008.

Abu Dhabi Information Security Technical Testing Guide, December 2008.

International Organisation for Standardisation / International Electrotechnical Commission 27001:2005 – Information Technology – Security Techniques – *Information Security Management Systems.*

International Organisation for Standardisation / International Electrotechnical Commission 27002: 2005 – Information Technology – Security Techniques – *Code of Practice for Information Security Management.*

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

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: TEMPLATE FOR SUMMARY OF SECURITY RISKS REPORT

I. EXECUTIVE SUMMARY

The Risk Assessment Report, Information Security Plan, and ST&E Report of ***[Service Name (ACRONYM)]*** were reviewed. An independent organisation also conducted a review of the management and functional security controls of **[Acronym]**. The following findings were discovered during the risk assessment:

- ***[Insert categories of findings here]***
- ***[The information system's operating system, database, and web servers had default configuration]***
- ***[The information system has a number of missing patches and no patch management process is in place]***
- ***[The information system lacks information security policies and procedures as required by the Abu Dhabi Information Security Standards]***

The following tables show the number of findings in each category below.

OVERALL FINDINGS						
Risk Levels	1	2	3	4	5	6
Number of Findings						

MANAGEMENT AND FUNCTIONAL FINDINGS						
Risk Levels	1	2	3	4	5	6
Number of Findings						

TECHNICAL FINDINGS						
Risk Levels	1	2	3	4	5	6
Number of Findings						

II. SERVICE/SYSTEM DESCRIPTION

[This section provides a brief service/system description. It also provides the categorisation of the service/system and lists all systems that support the service]

III. FINDINGS AND REMAINING RISKS

[Provides information on findings and remaining risks]

The following table summarises findings from the risk assessment, Information Security Plan, and ST&E of the information service.

IV. MITIGATION PLAN

[Provides information on the mitigation plan for the remaining risks (if any)]

RISK/ VULNERABILITY	RATE RISK	CORRECTIVE ACTIO	COMPLETION DATE	POINT OF CONTACT
e.g., password policy not enforced making system vulnerable	Scale of 1-6	Enforce password policy	10 Oct 2008	John.doe@ad.gov

APPENDIX E: SAMPLE INTERIM AUTHORITY TO OPERATE MEMORANDUM

Date: ***[Insert date]***

From: Designated Approval Authority

To: Information System Owner

Subject: Interim Authority to Operate (IATO) for ***[Insert name]*** **service**

The following security documents for the information service were reviewed:

1. Risk Assessment
2. Information Security Plan
3. ST&E

After the review, I have determined that the risk this information service poses to the entity is acceptable. However, it includes a number of risks that pose a threat to the entity and need to be addressed. Therefore, ***[Insert name]*** service from ***[Insert name]*** entity is hereby granted Interim Authority To Operate (IATO) for a period of 6 months from the date of this memorandum.

During this period of 6 months, the following vulnerabilities must be mitigated:

1. ***[Provides information on vulnerabilities that must be mitigated]***
2.
3.
4.
5.

The responsible organisation must resubmit the certification package before the expiration of this IATO.

In addition, for this IATO to be valid, the entity must maintain the management and functional security controls that were validated during the Risk Management process.

Designated Approval Authority (DAA)

Signature

APPENDIX F: SAMPLE AUTHORITY TO OPERATE MEMORANDUM

Date: ***[Insert date]***

Subject: Authority to Operate (ATO) for ***[Insert name]*** **service**

The following security documents for the information service were reviewed:

1. Risk Assessment
2. Information Security Plan
3. ST&E

After the review, I have determined that the risks that the information service poses to the entity are acceptable. ***[Insert name]*** service from ***[Insert name]*** entity is hereby granted Authority To Operate (ATO) for a period of 36 months from the date of this memorandum.

In addition, for this IATO to be valid, the entity must maintain the management and functional security controls that were validated during he Risk Management process.

Designated Approval Authority (DAA)

Signature

APPENDIX G: SAMPLE DENIAL TO OPERATE MEMORANDUM

Date: ***[Insert date]***

Subject: Denial to Operate (DTO) for ***[Insert name]*** **service**

The following security documents for the information service were reviewed:

1. Risk Assessment
2. Information Security Plan
3. ST&E

After the review, I have determined that the risks this information service poses to the entity are unacceptable. ***[Insert name]*** service from ***[Insert name]*** entity will not be accredited and may not continue to operate. All operations must stop immediately.

The following vulnerabilities and threats are the major issues that pose significant risks.

1. ***[Provides information on vulnerabilities and threats that pose significant risks]***
2.
3.
4.
5.

These vulnerabilities and risks must be resolved immediately to mitigate the risks, and the Risk Management process must be repeated at the earliest possible date to obtain accreditation.

Designated Approval Authority (DAA)

Signature