



Sultanate of Oman
Information Technology Authority



Security Assessment Services Standard 1.0

Information Technology Authority

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 1
-----	----------------------------------	---	--------------------	-----------------	----------------------------	---------



VALIDATION & DISTRIBUTION:

	Name	Email	Issue date
Issued by	Governance & Compliance Division	IT.accreditation@ita.gov.om	2019
Verified by			
Approved by	Steering Committee		

Distribution List	
1.	ITA
2.	IT Service Providers
3.	Online Publishing

DOCUMENT REVISION HISTORY:

Version	Date	Author	Remarks
1.0	2019	Governance & Compliance Division	Creation of document



Contents

Introduction	4
Purpose	4
Audience	4
General Requirements	5
1. Organization.....	5
2. Security Clearance.....	5
3. Scope of Services.....	5
4. Technical Scope of Engagement	6
4.1 Methodology.....	6
4.2 Security Controls	6
4.3 Reporting structure.....	7
5. Team Skills and Competencies.....	7
6. Service Level Agreements	11
6.1 Quality of Service	11
7. Contractual Obligations	13
7.1 Roles & Responsibilities	13
7.2 Non-Disclosure Agreement	13
8. Arrangement for Compliance and Maintenance of these Requirement.....	13
Appendix	14
A. Roles & Responsibilities	14
B. Glossary.....	17
References	18

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 3
-----	----------------------------------	---	--------------------	-----------------	----------------------------	---------



Introduction

Security assessments are an essential part of understanding an organisation’s security posture. The main objectives are to:

- Identify where vulnerabilities may exist within an organisation’s infrastructure
- Validate the effectiveness of existing security controls
- Assess an organisations security posture and provide actionable information to make improvements
- Confirm that security implementations are in line with industry recognised best practice and national standards.

This document is designed to provide a detailed set of requirements for organisations to conduct those security assessment services. These requirements shall form the basis of an accreditation scheme within an Oman Government context

Related Documents

- “Web and Hosting Policy”, ITA
- “ITA’s Guidelines on Securing Websites”, ITA
- “Basic Security Controls”, ITA, Oman
- “Government Application and E-Services Security Architecture Framework”, ITA

Purpose

The purpose of this document is to set the minimum standards for delivering a security assessment service within Oman’s Government context.

Other supporting guidelines and frameworks have been developed to facilitate the implementation of this standard by guiding both government organizations and service providers.

Audience

This standard is designed to provide all service providers with a set of requirements that must be adhered to prior to delivering a security assessment service to government administrative units and Critical National Infrastructure organizations in Oman

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 4
-----	----------------------------------	---	--------------------	-----------------	----------------------------	---------



General Requirements

This section provides a set of requirements that Service Providers shall need to satisfy to conduct security assessments for government organizations.

1. Organization

As an organisation, service providers providing security services to government organisations shall achieve the following requirements prior to conducting any assessments:

- Holds and provide evidence of a valid and in-date ISO 27001 certification for the service(s) they are providing
- Confirm that they conduct regular, internal and independent reviews as part of their certified management system
- Adhere to Oman Law
- Provide formal documentation and evidence to support the Service Provider’s capabilities:
 - Testing methodology (see section 4.1)
 - Reporting structure (see section 4.3)
 - The Service Provider shall have performed the service under the company name for a minimum of 12 months
 - Lead Assessor shall provide evidence of the previous 12 months of penetration tests (Penetration Testing service only)
 - Lead assessor shall provide a technical CV
 - Lead Assessor shall provide 2 redacted reports that he/she has authored within the last 12 months (Penetration Testing service only)
 - The Service Provider shall provide descriptions of recent engagements similar to the scope of the assessments to be provided.

2. Security Clearance

As per the national security addressed requirements, IT Service Providers will undergo a security background check and only those who will be granted security clearance will continue delivering the security assessment services to the government administrative units. The security clearance covers both the organization (service provider) and its registered team members under this accreditation program. Hence, Service Providers may need to employ vetting mechanism for the employment of its team members or contractors who will be delivering security assessment services to the government administrative units.

3. Scope of Services

This standard is focused on the two following security assessments services:

- Penetration testing
- Technical assessments

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 5
-----	----------------------------------	---	--------------------	-----------------	----------------------------	---------



Depending on the security assessment, recognized certifications will be required by the Service Providers team members for delivering the service to government entities to ensure a standard level of competency. Assessment certification requirements are listed in section 5.

4. Technical Scope of Engagement

The technical scope of engagement should be clearly defined and approved prior to performing the security assessment and should include the below:

4.1 Methodology

- The organisation shall have a defined and documented assessment methodology (covering the assessment services provided¹) that shall be shared with the government organisation
- The service provider has to specify within the agreed scope with the customer what type of assessment is to be delivered, such as:
 - Penetration testing:
 - White box
 - Black box
 - A combination of the two above (grey-box)
 - Technical assessments
- The assessment team should be physically present at the premises of the assigned organisation when conducting the assessment
- Remote Access should not be used for conducting the security assessment unless specifically requested by the requesting organisation
- The service provider could may different sets of tools to run the assessment. However, they need to provide a list with tools to be used for the security assessment to the government organization and obtain an approval form that organization`s ISO (Information Security Officer) or equivalent to use only the approved tools for the assessment.
- The service providers are responsible to ensure that technical controls are thoroughly checked to ensure that existing vulnerabilities on the given scope are not overlooked, especially when using an automated tool. They may to refer to the list of controls defined in the published Basic Security Controls Guidelines by ITA for Government Administrative Units, and ITA`s Guidelines for Security Websites when assessing web security.
- In cases where service providers are assessing a new system, they need to consider the Security design requirements documented within the Security Plan of that system to identify what controls should be validated. The security assessor could also use the Government Application and E-Services Security Architecture Framework, as a reference to address the required controls needs to be verified on that system.

4.2 Security Controls

Service providers should be following the best security practices while and after delivering the security assessment to ensure acceptable levels of protection of customer`s data and information assets.

- **Data Confidentiality:** some security controls might need to be implemented by the service provider to keep customer`s Data from being exposed to any

¹ The two assessment services are penetration testing and technical assessments.

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 6
-----	----------------------------------	---	--------------------	-----------------	----------------------------	---------



un-authorized persons. Only assigned members to the assessment team can have access and handle that data. Assessment team members are responsible to comply to their contractual obligations. At the same time, the service provider may need to apply some encryption on the data storage and transmission.

- **Authorized Testing:** the assessors shall not deviate from the agreed scope with the customer while conducting the assessment. The appropriate assessment tools shall only be used within a defined timeframe as agreed with the customer (this includes what times during the day and the week testing shall be conducted).
- **External Media:** when using external media for storing customer`s data, the Service Provider shall take the necessary precautions to keeping that media safe from any unauthorized access and shall use encrypted media. External media used for assessment should be free from viruses and malware. The devices shall be scanned before used as part of the assessments.

4.3 Reporting structure

The following elements shall be included in the reporting structure:

- Executive Summary, emphasising the business impact of any issues identified
- Summary of technical findings prioritised by risk level
- Detailed technical report of findings emphasising the risk, business impact and threats
- Detailed evidence demonstrating any unauthorised access achieved
- Detailed recommendations prioritised by risk level
- Estimate of resources required to implement recommendations.

5. Team Skills and Competencies

5.1 The assessment team members shall maintain the required skillset that is required to deliver the procured service. This shall include possessing sufficient technical knowledge and experience in different IT domains such as:

- Networks and Infrastructure
- Database
- Applications
- Physical Security.

5.2 The Service Provider shall form a team that consists of a team lead and technical assessors. A team lead should ensure the overall quality of the delivered service and meeting the assessment objectives while technical assessors focus on conducting the assessment.

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 7
-----	----------------------------------	---	--------------------	-----------------	----------------------------	---------



5.3 Certain certifications are required when recruiting team members for delivering the service to the government administrative units in order to ensure standard level of competencies.

5.4 Depending on the security assessment, recognised certifications will be required by the Service Providers team members for delivering the service to government administrative units to ensure a standard level of competency. Assessment certification requirements are listed in the following tables.

A. Penetration testing

When conducting penetration testing or vulnerability assessments, the team members are required to satisfy the following requirements.

The assessor(s) must possess at least one of the certifications in the table below.

Assessor	Certification
<p>1. Lead Technical Assessor</p>	<ul style="list-style-type: none"> • Web Application Testing <ul style="list-style-type: none"> - CREST Certified Web Application Tester - GIAC Web Application Penetration Tester (GWAPT) - Offensive Security Web Expert (OSWE) - GIAC Certified Web Application Defender (GWEB) - Licensed Penetration Tester (LPT) Master • Infrastructure Testing: <ul style="list-style-type: none"> - CREST Infrastructure Certification Examiner - Offensive Security Certified Professional (OSCP) certification - CREST Registered Tester Examination - GIAC Penetration Tester (GPEN) - Licensed Penetration Tester (LPT) Master
<p>2. Technical Assessor</p>	<ul style="list-style-type: none"> • Web Application Testing: <ul style="list-style-type: none"> - CREST Certified Web Application Tester



	<ul style="list-style-type: none"> - GIAC Web Application Penetration Tester (GWAPT) - Offensive Security Web Expert (OSWE) - GIAC Certified Web Application Defender (GWEB) - Certified Ethical Hacker (CEH) 10.0 or above. <ul style="list-style-type: none"> • Infrastructure Testing: <ul style="list-style-type: none"> - CREST Infrastructure Certification Examiner - Offensive Security Certified Professional (OSCP) certification - CREST Registered Tester Examination - GIAC Penetration Tester (GPEN) - Certified Ethical Hacker (CEH) 10.0 or above.
--	--

B. Technical assessments

The requirement for non-intrusive technical assessments (e.g. configuration reviews) may be required and as such, different skillsets are required. Below is a list of certifications where the assessor shall hold at least one, as a minimum for the necessary assessment type.

Assessment Type	Certification
1. Web Application Testing	<ul style="list-style-type: none"> ○ CREST Certified Web Application Tester ○ GIAC Web Application Penetration Tester (GWAPT) ○ Offensive Security Web Expert (OSWE) ○ GIAC Certified Web Application Defender (GWEB) ○ Certified Ethical Hacker (CEH) 10.0 or above.



<p>2. Infrastructure Testing</p>	<ul style="list-style-type: none"> ○ CREST Infrastructure Certification Examiner ○ Offensive Security Certified Professional (OSCP) certification ○ CREST Registered Tester Examination ○ GIAC Penetration Tester (GPEN) ○ Certified Ethical Hacker (CEH) 10.0 or above.
<p>3. Firewall reviews</p>	<ul style="list-style-type: none"> ○ Offensive Security Certified Professional (OSCP) certification ○ CREST Infrastructure Certification Examiner ○ Cisco Certified Network Associate (CCNA) Security.
<p>4. Configuration review</p>	<p>Web Application:</p> <ul style="list-style-type: none"> ○ CREST Certified (Web Application) Tester ○ Certified Application Security Engineer (CASE) EC – Council <p>GIAC Secure Software Programmer (GSSP)</p> <p>Infrastructure:</p> <ul style="list-style-type: none"> ○ CREST Certification (Infrastructure) Tester ○ CREST Registered Tester ○ Offensive Security Certified Professional (OSCP) certification ○ GIAC Systems and Network Auditor (GSNA)
<p>5. Code review</p>	<p>Web Application:</p> <ul style="list-style-type: none"> ○ CREST Certified Wed Application Tester ○ Certified Application Security Engineer (CASE) EC – Council <p>GIAC Secure Software Programmer (GSSP)</p> <p>Infrastructure:</p> <ul style="list-style-type: none"> ○ CREST Infrastructure Certification Examiner ○ Offensive Security Certified Professional (OSCP) certification



	<ul style="list-style-type: none"> ○ Certified Application Security Engineer (CASE) EC – Council ○ GIAC Systems and Network Auditor (GSNA)
<p>6. Architecture review</p>	<p>Infrastructure:</p> <ul style="list-style-type: none"> ○ Offensive Security Certified Professional (OSCP) certification ○ CREST Certification (Infrastructure) Tester ○ CREST Registered Tester ○ CREST Registered technical Security Architect (CRTSA) ○ CESG Certified Professional (CCP) IA Architect. ○ Certified TOGAF 9 Zachman Certified - Enterprise Architect <p>Web Application:</p> <ul style="list-style-type: none"> ○ CREST Certified (Web Application) Tester ○ Certified Application Security Engineer (CASE) EC – Council ○ GIAC Secure Software Programmer (GSSP) ○ GIAC Certified Web Application Defender (GWEB)

6. Service Level Agreements

6.1 Quality of Service

- Each security assessment should follow the defined scope, process and unified checklists as per the covered security areas to ensure standard quality on the deliverables.
- The methodology document should be kept up to date to ensure its applicability to the delivered service.
- The Assessors should not interrupt any running services of the organization (internal & External) while conducting the assessment.
- If the assessor has observed any evidences of previous breach or come across any major vulnerability that could be exploited, it should be immediately reported to customer or the project stakeholder.
- The Service Provider should clearly define and agree with the customer on the assumptions/limitations they have considered for each activities in scope prior to execution.

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 11
-----	----------------------------------	---	--------------------	-----------------	----------------------------	-------------



- The Service Provider shall conduct any necessary clean-up activities after the completion of penetration testing services, ensuring customer’s network environments are not impacted as a result of the penetration testing. The clean-up activities include but are not limited to the following:
 - Update and/or removal of test accounts added or modified during testing
 - Update and/or removal of database entries added or modified during testing
 - Uninstall test tools or other artefacts as applicable
 - Restoring security controls that have been altered for testing
 - Provide customers with necessary information and/or guidance on how to verify customer’s environments have been restored
 - Provide customers with confirmation that the environments have been cleaned and restored.

- Provide customers with confirmation that the environments have been cleaned and restored. The Assessors should highlight any modifications added to the environment under their scope during the assessment period (creating accounts, resetting accounts, switch config., etc.)

-
- A communication Plan for customer engagement shall be defined and shared with the government organization to establish the right channels of communication and reporting.
- Progress reports should be shared and with the customer to give updates on the projects schedule during the assessment and discuss any issues or obstacles related to the assessment.
- Assessment reports and updates shall be delivered within the agreed timeframe and defined deadlines with the customers.
- Assessors shall conduct analysis on all findings, including automated tools findings. This includes documenting the findings, providing recommendations to remediate and providing cross references with trusted sources
- Assessment reports shall include the key elements defined by this standard to maintain the quality of reporting results (section 4.3).

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 12
-----	----------------------------------	---	--------------------	-----------------	----------------------------	-------------



7. Contractual Obligations

7.1 Roles & Responsibilities

Roles and responsibilities should be clearly defined in the service contract and included within the scope of the service main document as well in order to set the right expectations with the customer. Assessor’s responsibilities are described in Appendix A at the end of this document.

7.2 Non-Disclosure Agreement

The third party should sign a Non-Disclosure Agreement document that mandates its obligation in protecting the confidentiality of the data that it’s been handled throughout the assessment process.

8. Arrangement for Compliance and Maintenance of these Requirement

Service providers shall comply with all of the requirements within this standard. They should keep records of all customer engagement’s activities and document the delivered service and associated processes as well for assurance purposes.

Accreditation of the service providers shall remain valid for three years provided they maintain their:

- ISMS Certification
- Security Clearance
- Required level of team skills and certifications.

An annual review shall be conducted for the Service Provider and the assessment individuals to retain their accredited status. Failure to maintain these requirements shall result in the organization and/or individuals’ removal from the accredited scheme for security assessment.

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 13
-----	----------------------------------	---	--------------------	-----------------	----------------------------	-------------



Appendix

A. Roles & Responsibilities

The below table describes the roles and responsibilities of both government organization and the service provider the security assessment life cycle.

Assessment Engagement Phase	Responsibilities of Government Administrative Units	Responsibilities of Service Provider
Pre-assessment	<ul style="list-style-type: none"> Establish the objectives and scope of work for information security assessment. Allow sufficient time and resources for 3rd party assessors to gather requirements. Allocate team members and resources (e.g. personnel, cost, time, etc) needed for the assessment (i.e. assisting 3rd party assessors). Appoint a point-of-contact (or team leader) for managing communications with 3rd party assessors. Evaluate criteria and capabilities of the 3rd party assessor. Select an independent 3rd party assessor based on the evaluation. Ensure all relevant policies, procedures, documents and records are in place and available for the assessment. Fill-up pre-assessment templates provided by 3rd 	<ul style="list-style-type: none"> Allocate team members and sufficient resources to conduct the assessment. Provide the team's background including relevant knowledge, skills, and certifications (either professional certifications or product or technology specific certifications) for verification. Establish effective communication mechanism with organization's point-of-contact (or team leader). Understand scope of work for conducting information security assessment provided by organization. Understand organization's structure of information system under scope of work of

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 14
-----	----------------------------------	--	--------------------	--------------	-------------------------	----------



	<p>party assessor (to do information gathering).</p> <ul style="list-style-type: none"> Review the information security assessment plan provided by the 3rd party assessor and approve the plan prior to the assessment. Ensure that a Non-Disclosure Agreement (NDA) has been signed by 3rd party assessor prior to the assessment. 	<p>the information security assessment.</p> <ul style="list-style-type: none"> Participate in initial orientation meetings. Acquire relevant documents and records for information gathering Provide pre-assessment templates to organization in order to do information gathering. Develop information security assessment plans and submit to organization for approval.
<p>During the Assessment</p>	<ul style="list-style-type: none"> Ensure key personnel are available during the assessment. Depending on the specific assessment, individuals in the following roles may be interviewed: <ul style="list-style-type: none"> Information system owners Information system security officer or CISO System/network administrator Database administrator 	<ul style="list-style-type: none"> Conduct assessment after obtaining approval. Protect organization's information collected during and after the information security assessment. Produce status report periodically or at planned interval time as agreed with the organization. <p>Present status report during</p>



	<ul style="list-style-type: none"> - Web administrator - Executives that are responsible for specific security functions - Head of departments/authorizing officials - Internal auditor - Risk management personnel <ul style="list-style-type: none"> • Monitor the overall assessment process to ensure information security is intact. • Hold discussions/meetings with 3rd party assessor to receive updates and resolves any issues. 	<p>discussion / meeting with the organization's point-of-contact (or team member).</p>
<p>Post-assessment</p>	<ul style="list-style-type: none"> • Review assessment reports produced by 3rd party assessor • Present the final assessment report to senior management to ensure the findings are made known to organizational officials and system owners • Develop remediable action plans to address findings and recommendations that are highlighted in the assessment report. • Update information security requirements with findings from assessment reports and remediable action plans. 	<ul style="list-style-type: none"> • Produce assessment reports that incorporate findings of the conducted assessment and recommendations for correcting current countermeasures (if any). • Assist organization in producing remediable action plans. • Conduct clean-up by removing data/log files that is created and/or stored on the organization's systems.



B. Glossary

▪ Risk Management

- The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:
 - 1) the conduct of a risk assessment;
 - 2) the implementation of a risk mitigation strategy; and
 - 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (SOURCE: FIPS 200)
- The coordinated activities to direct and control an enterprise with regard to risk
Scope Note: In the International Standard, the term "control" is used as a synonym for "measure." (ISO/IEC Guide 73:2002)
- One of the governance objectives. Entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the enterprise's risk appetite. (COBIT 5 perspective)

▪ Vulnerability

- A weakness in a system, application, or network that is subject to exploitation or misuse. (SOURCE: NIST SP 800-61)
- A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events. (ISACA)

▪ White Box

- A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as comprehensive testing. (NIST)

▪ Black Box

- A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as basic testing. (NIST)

▪ Gray-box testing

- Grey Box testing a combination of white-box testing and black-box testing, in which the tester has limited knowledge of the internal details of the program

▪ Virus

- A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. (SOURCE: CNSSI-4009)

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 17
-----	----------------------------------	---	--------------------	-----------------	----------------------------	-------------



- A program with the ability to reproduce by modifying other programs to include a copy of itself
Scope Note: A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network. (ISACA)

- **Malware**

- A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system of otherwise annoying or disrupting the victim. (SOURCE: NIST SP 800-83)
- Short for malicious software designed to infiltrate, damage or obtain information from a computer system without the owner’s consent.

Scope Note: Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes. (ISACA)

References

- “NIST Special Publication 800-53A: Assessing Security and Privacy Controls in Federal Information Systems and Organizations- Building Effective Assessment Plans”, Revision 4, National Institute of Technology, US Department of Commerce, December 2014.
- IRAP, https://www.asd.gov.au/infosec/irap/application_form.php, 2017.
- Pahri. N, Idris. N, “3rd Party Security Assessment Guidelines”, Cybersecurity Malaysia, 2010
- “Cybersecurity Fundamentals Glossary”, ISACA, 2016.
- Kisse. R, “Glossary of Key Information Security Terms”, NISTIR 7298, Revision 2, 2013.

ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 18
-----	----------------------------------	---	--------------------	-----------------	----------------------------	-------------



Sultanate of Oman
Information Technology Authority



ITA	Governance & Compliance Division	Document Name: Security Assessment Services Standard	Document ID: GC_S1	Version: 1.0	Issue Date: August 2019	Page: 19
-----	----------------------------------	---	--------------------	-----------------	----------------------------	-------------