Sultanate of Oman
Information Technology Authority

e.oman

Data and Information Systems Security Classification Mapping

Governance and Standards Division

VALIDATION & DISTRIBUTION:

	Name	Email	Issue date
Issued by	Governance & Standards Division	standards@ita.gov.om	30/7/2017
Verified by	Governance & Standards Team ISD		
Approved by	Steering Committee		

Distribution List	
1.	ITA
2.	All concerned government agencies
3.	Online publishing

DOCUMENT REVISION HISTORY:

Version	Date	Author	Remarks
1.0	30/7/2017	Governance & Standards	Creation of document

1 Table of Contents

2 Glossary

Availability	Ensuring timely and reliable access to and use of information.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
Impact Level	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Risk Managment	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
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals

Security Level	A hierarchical indicator of the degree of sensitivity to a certain threat. It implies, according to the security policy being enforced, a specific level of protection.

Related Documents

This document is to be used in accordance to the below list of documents:

- Royal Decree 118/2011 o Security Classification
- Risk Management Framework issued by ITA
- Business Reference Model (BRM-OeGAF) released by ITA

3 Intorduction

The emerging needs to safeguard the information's assets in any organization has become crucial and classifying those assets is the basis for identifying the required protection levels and controls. Data and Information Systems Security Classification Mapping guidelines have been designed for government entities to fulfill their data and information systems` security classification requirements. The mapping process has been defined with a given logical structure to address all aspects related to mapping that civil organizations in particular needs to adopt for its information assets (data and systems) to the defined categories by the circular 118/2011.

4 Purpose

The purpose of this document to assist government entities in classifying their data and information systems in accordance with Royal Decree 118/2011 on Security Classification. These guidelines provide a mechanism that facilitates the process of assigning proper sensitivity levels of the given data based on the common security objectives CIA (Confidentiality, Integrity, and Availability).

5 Risk Management

Government organization should adopt Risk Management Mechanism in order to define all its valuable assets and identify the associated risks for them. That will give a clear indication on the required level of protections and setting priorities for managing the identified risks.

This exercise is very essential and it simplifies Data Classification process implementation across the organization. Risk Management Framework published by ITA could be used as a good reference which covers all the main complements to achieve proper risk management in the organization.

Five risk impact levels have been defined as the following:

- Very High
- High
- Medium
- Low
- Very Low

Risk Impact Level	Description
Very High	**Very high** risk means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	**Very low** risk means that a threat event could be expected to have a **negligible** adverse effect on organizational operations,

	organizational assets, individuals, other organizations, or the Nation.

Table 1. Risk Impact Levels

6 Security Classifications

As defined by circular 118/2011, 4 data classification levels have been defined and should be followed by all government entities:

- Top Secret (سري للغاية)
- Secret (سري)
- Restricted (محدود)
- Confidential (مكتوم)

Government organization should need to include a fifth level for public or open data to fulfill the requirements of the Open Data Policy. The government organization should be able to assign a proper security classification level after conducting an impact analysis for its data.

7 Security Objectives and Potential Losses

These guidelines address the below defined security objectives as basis for the impact analysis with given potential loses.

Security Objective	Definition	Potential Loss
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity	System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system

		availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
Availability	Ensuring timely and reliable access to and use of information.	If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

Table 2. Security Objectives and Potential Losses

8 Mapping Process to Security Classification

Government organization could use the mapping process provided in these guidelines to help in classifying its information to the defined security classification levels in Circular 118/2011. The below diagram summarize the mapping process for assigning the right security classification level.

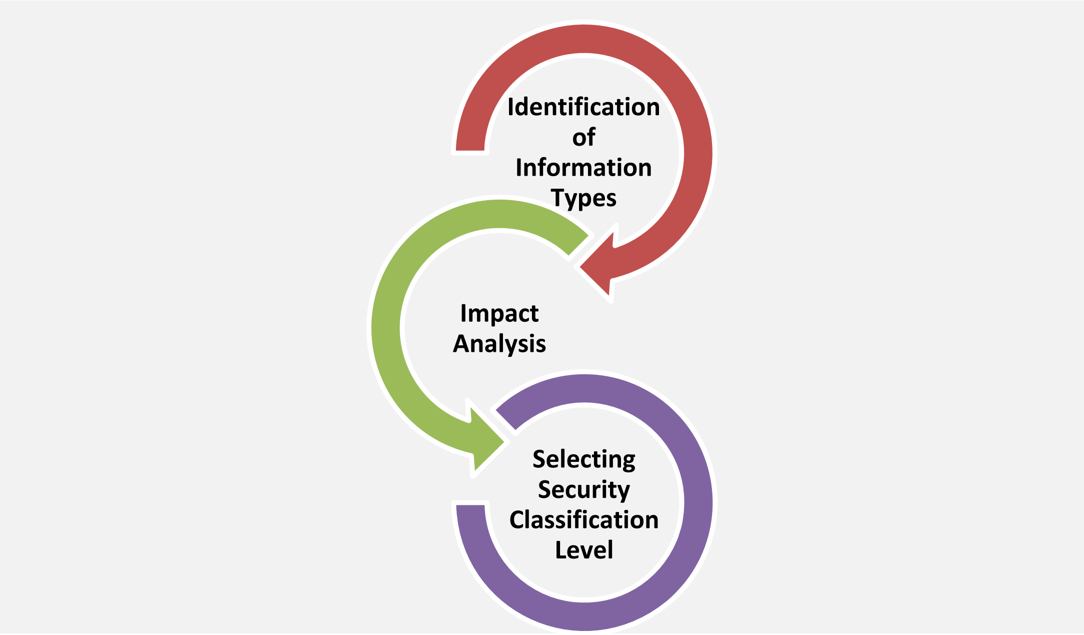
Identification of Information Types
Impact Analysis
Selecting Security Classification Level

Diagram 1. Mapping Process to Security Classifications

8.1 Identification of Information Types

starting any classification process. It needs to have a comprehensive list of information types that reflects all their business related information (for example: civil data and records, financial information, Healthcare records, etc.).

OeGAF Business Reference Model (BRM)

Government organizations can refer to the Business Reference Model (BRM) that defines different lines of business and the associated government functions of the Oman Government that cuts across the boundaries of different agencies. BRM covers all domains of government business along with the underlying business functions.

BRM provides an overall map for all the government business that was used to instantiate Data Sets of Oman`s government Data. The data sets have been categorized into two main layers just like how the lines of businesses were categorized in the BRM document:

A. Information related to Mission Critical Areas (Services to Citizens, Residents, & Commercial Establishments)
B. Information related to Internal Corporate and Support Services

These data sets could be used as a good reference identify the core national information types and enable organizations to address them while implementing data classifications. The provided information types might though cover only few information types that are processed by IT Systems. At the same time, organizations may list some information types that might not covered on the provided data sets and information types that are listed in the appendix of these guidelines. Furthermore a single information system could process multiple information types that all need to be identified and listed for the impact analysis.

8.2 Impact Analysis

Impact analysis a critical step to help assigning a proper risk level for a given information asset. To do so security objectives should be outlined and impact level should be studied and selected. The below table provides a scheme to conduct the impact analysis and defines each impact level for each security objective after addressing potential threats (Risk Management Framework provides a list of threats that could be used for this impact analysis).

Security Objective / Impact Level	**Very Low**	**Low**	**Medium**	**High**	**Very High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	The unauthorized disclosure of information could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **multiple severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring	The unauthorized modification or destruction of information could be expected to have a **negligible** adverse effect on organizational	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational	The unauthorized modification or destruction of information could be expected to have a **multiple severe or catastrophic** adverse effect on organizational

information non-repudiation and authenticity	operations, organizational assets, or individuals.	operations, organizational assets, or individuals.	operations, organizational assets, or individuals.	operations, organizational assets, or individuals.	operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **multiple severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 3. Impact Analysis

8.3 Assign Information Security levels

After information types have been identified, the next step is to take each and every single information type and assign its impact level against each security objective as in the below formula:
Security Category $_{\text{information type}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)}
The maximum value will be always considered. For example, If any of the given variables above contains a “High” value, the overall result would be “High”, the same is applicable for the “Very High”. In some cases the value of impact level might be “not applicable (N/A)” against one of the security levels, in many cases confidentially for instance.

Examples

Below are some examples that clarify how to assign security levels that could be mapped to the security classifications.

- If the identified Information type is administrative, applying the defined impact analysis scheme should look like the following:

Security Category $_{\text{administrative information}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, VERY LOW)}.

- If the identified information type is legal, applying the defined impact analysis scheme should look like the following:

Security Category $_{\text{Legal}}$ = {(confidentiality, VERY HIGH), (integrity, HIGH), (availability, HIGH)}.

8.4 Assign Systems Security Classification

After information types have been identified, the next step is to take each and every single information type and assign its impact level against each security objective as in the below formula:

Security Category $_{\text{information type}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)}

The maximum value will be always considered. For example, If any of the given variables above contains a “High” value, the overall result would be “High”, the same is applicable for the “Very High”. In some cases the value of impact level might be “not applicable (N/A)” against one of the security levels, in many cases confidentially for instance.

Examples

Below are some examples that clarify how to assign security levels that could be mapped to the security classifications.

- If the identified Information type is administrative, applying the defined impact analysis scheme should look like the following:

Security Category $_{\text{administrative information}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, VERY LOW)}.

- If the identified information type is legal, applying the defined impact analysis scheme should look like the following:

Security Category $_{\text{Legal}}$ = {(confidentiality, VERY HIGH), (integrity, HIGH), (availability, HIGH)}.

9 Appindex

9.1 Data Sets / Information Assets (based on the OeGAF Business Reference Model BRM)

A. Mission Areas and Information Types (Services to Citizens, Residents, & Commercial Establishments)		
1. Arts, Culture and Tourism *1.3 Arts and Culture Development & Promotion* *1.2 Tourism Development and Promotion* *1.3 Archives, Artworks, Cultural Artefacts, Heritage Buildings Preservation, Management and Public Display*	**2. City Planning, Development and Management** *2.1 City Planning and Development* *2.2 Land, Building and Public Facilities Development and Management* *2.3 Electricity and Water Distribution & Control*	**3. City Planning, Development and Management** *3.1 Civil Events Records Maintenance*
4. Community and Sports Development *4.1 Wilayats Affairs Administration* *4.2 Social Programs and Projects Development & Management* *4.3 Social Services and Donations* *4.4 Sports Development and Promotion*	**5. Economic Development** *5.1 Economy and Industry Development* *5.2 National IT Strategy Programs and Initiatives Implementation* *5.3 Oman Securities Market Regulation and Management*	**6. Education** *6.1 Preschool to High School Education* *6.2 Graduate and Postgraduate Education* *6.3 Continuing Education and Training* *6.4 Islamic Education*

7. Environment Management *7.1 Environmental Monitoring and Forecasting* *7.2 Environmental Pollution Prevention and Control* *7.3 Environment and Wildlife Protection & Conservation* *7.4 Waste Management*	**8. Health** *8.1 Public Health Monitoring, Control and Education* *8.2 Healthcare Facilities and Services Planning, Management & Administration* *8.3 Communicable Diseases Control and Prevention*	**9. International and Trade Relation** *9.1 Foreign Socio-Economic and Political Relation Development* *9.2 Trade and Investment Promotion & Facilitation* *9.3 International Treaties and Agreements Negotiation & Implementation*
10. Law and Justice Management & Administration *10.1 Judicial Affairs Management and Administration* *10.2 Review and Preparation of Laws, Regulations & Royal Decrees* *10.3 Advisory and Consultation on Subject of Laws*	**11. Manpower Development and Social Insurance Protection** *11.1 Manpower Development and Management* *11.2 Social Insurance Protection*	**12. Monetary Control and National Loans Management** *12.1 Monetary Control and Supervision* *12.2 Management of National Loans* *12.3 Public Funds Management*
13. National Defense and Security *13.1 National Defence* *13.2 Internal Security and Protection*	**14. Natural Resource and Food Reserve Management** *14.1 Natural Resource Development and Management* *14.2 Strategic Food Reserve Management*	**15. Religious Affairs** *15.1 Hajj Planning and Coordination* *15.2 Mosques Management*

16. Research and Development

16.1 Scientific Research and Development

16.2 Financial Assistance for Scientific Research

17. Transportation and Communication

17.1 Road Network and Traffic Planning & Development

17.2 Ports Planning, Development and Management

17.3 Telecommunication Network Planning and Development

17.4 Postal Services Provision

B. Internal Corporate and Support Services

18. Licensing and Regulatory Control

18.1 Licensing and Regulatory Control of Commercial Establishments

18.2 Licensing and Regulatory Control of Professionals

18.3 Licensing and Regulatory Control of Controlled Goods, Equipment & Drugs

18.4 Licensing and Regulatory Control to Import Livestock & Live Fish Stock

18.5 Licensing and Regulatory Control of Public Events & Activities

19. Monetary Collection

19.1 *Taxes and Duties Collection*

19.2 *Other Monies Collection*

20. Public Information Management and Communication

20.1 Government Information Management and Publication

20.2 Data and Statistics Management and Publication

20.3 News and Magazines Publication

21. Procurement of Goods and Services

21.1 Procurement of Large Value Goods and Services

21.2 Procurement of Small Value Goods and Services

10 References

1. Royal Decree 118/2011 on Security Classification of Records and Regulating Physical Security
2. “FIPS 199: Standards for Security Categorization of Federal Information and Information Systems”, Federal Information Processing Standards Publication, U.S. Department of Commerce, 2004.
3. “NIST 800-60 Vol I: Guide for Mapping Types of Information and Information Systems to Security Categories”, National Institute of Standards and Technology, U.S. Department of Commerce.
4. Kisse. R, “Glossary of Key Information Security Terms”, NISTIR 7298, Revision 2, 2013.