Sultanate of Oman
Information Technology Authority

e.oman

Information Security Management Framework

Governance and Compliance Division

Document control:

Version	Author	Date	Changes
1.0	Rasha Al Abdali	30.07.2017	Initial draft

1 Contents

2 Related Documents

- Information Security Management Policy, 2019
- IT Governance Policy, 2018
- IT Risk Management Framework, 2017
- OeGAF, 2018
- Basic Security Controls, 2017
- IT Service Continuity Framework, 2018
- Government Network Security Architecture framework, 2015
- Government Application and E-Services Security Architecture Framework, 2016
- Endpoint Security Architecture Framework, 2017

Related Regulatory and Legislations

- Oman e-Transaction Law
- Circular of Establishing the Security Offices in Government Organizations, 3367/102/أ ع م و
- Royal Decree 118/2011 for Data Security Classifications

3 Introduction

Information Security Management Framework captures the best practices and previous experience on this domain to assist government entities in running their information security program successfully while supporting the overall journey in achieving their business objectives. The aim is to produce an effective tool that delivers a real value for the government that could be measured, maintained, and continually improved.

4 Purpose

This framework has been designed to assist in managing information security program across a government organization and maintain ensure that all operations, people, processes, and systems are protected while delivering business activities and achieve the organizational objectives.

5 Targeted Audience

The targeted audience for the framework are Information Security Officers who are in Charge to run the Information Security inside the organization. It could be also used by security professionals at management levels to build a solid understanding of the main components that are required to adopt good practices of information security.

6 Scope

This framework is covering all aspects related to establishing and managing an information security program for organizations and sets the main elements to be considered to ensure effectiveness and sustainability. Since organizational security is not a one day journey, the framework has included all the factors that ensure proper protection at different layers (such as: people, processes, structure, and technology) which will be the dynamics that need to be maintained all day long.

7 Information Security Principles

The three principles of Information Security are confidentiality, Integrity, and availability. These three principles are used as main objectives to achieve in any information security program.

The following defines each principle:

- **Confidentiality**

  Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

- **Integrity**

  Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity

- **Availability**

  Ensuring timely and reliable access to and use of information.

8 Organization of the Information Security

8.1 Key Stakeholders

The main objective of security is to ensure that the primary business of the organization is on and running. In other words, security`s main job is to enable and support the business to achieve its objectives without interruption, ensuring that right security measures are in place to protect organization’s critical information assets. Hence, internal stakeholders play critical role in building an effective security program.

Key stakeholders who are very important when setting the information security program and needs to be involved throughout the process are:

- Information Security Office
- Top Management
- IT
- HR
- Legal
- Admin & Finance
- Contract & Procurement

There could be other relevant stakeholders within the organization that could be considered. For example, in some organizations, the involvement of t strategic planning team might add a big value especially when setting the security strategy that needs to be aligned with organization`s goals and direction.

8.2 Organizational Structure

In order to run a well-governed information security program in the organization, a well-defined structure has to be defined in the first place. The three main layers to ensure successful implementation consists of the below:

1. **Information Security Office** reports to the highest authority of the organization. This office should be an independent unit that doesn’t fall under any other business or technical unit. Many organizations have failed here by either setting ISO office directly under IT, or consider IT Security (the technical team who is responsible for implementing the technical controls) for running the information security program for the organization. The roles and differences between IT Security and Information Security are different and needs to be segregated. The below table summarizes the difference between the two roles:

Comparison criteria	Information Security	IT Security
Reporting to	Head of the unit (CEO/or Minister office)	IT Director
Team Size	Small (1-3)	Medium/Big (+3)
Required Skills	Leadership/ Business/ Technical	Technical
Main Duties	Supervises and coordinates the implementation of the Information Security Management program, ensure general security policy is in place, conduct risk assessment, conduct regular auditing to check required controls are in place, report progress of the ISMS program to Security Committees	Implements Security Controls and recommendations as agreed and directed by security committees

2. **ISMS Steering Committee:** is the top management in the organization represented by the respective key stakeholders mentioned in the above section.

3. **Working Committee:** is represented by middle management from key stakeholders departments in the organization who will ensure the implementation of the security controls by their teams as required by the Information Security Program.

Below is an example of a common Information Security Organizational Structure:

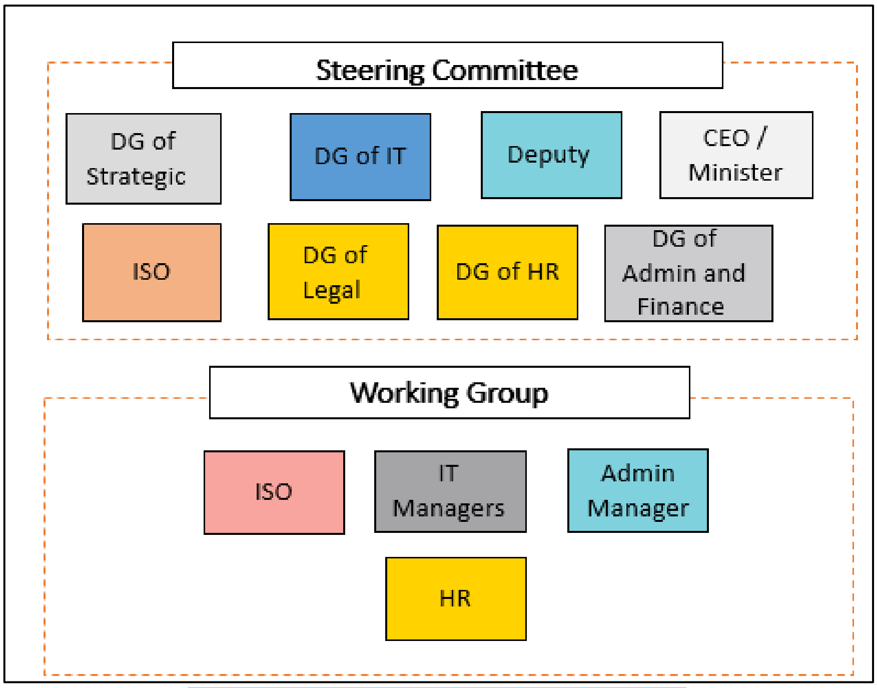


Diagram 1: Security Organizational Structure*

*Please note that this structure is customizable where other relevant stakeholders could be added under each committee as mentioned above.

8.3 Roles and Responsibilities

In order to ensure effective implementation and management of the information security program, clear roles and responsibilities have to be defined at each layer. The below table lists the main responsibilities for each role mentioned in the previous section:

Roles	Responsibilities
Senior executives	• Institute processes to integrate security with business objectives. • Ensure that roles and responsibilities include risk management in all activities. • Monitor regulatory compliance. • Require business case studies of security initiatives and value of information protected. • Require monitoring and metrics for reporting security activities. • Ensure processes for knowledge capture and efficiency metrics.

Steering committee	• Review and assist security strategy and integration efforts, ensure that business unit managers and process owners support integration. • Identify emerging risks, promote business unit security practices, and identify compliance issues. • Review and advise adequacy of security initiatives to serve business functions and value delivered in terms of enabled services. • Review and advise the extent to which security initiatives meet business objectives. • Review processes for knowledge capture and dissemination.
ISO	• Develop security strategy, oversee the security program and initiatives, and liaise with business unit managers and process owners for ongoing alignment. • Ensure risk and business impact assessments, develop risk mitigation strategies, and enforce policy and regulatory compliance. • Monitor utilization and effectiveness of security resources and reputation and the delivery of trust. • Develop and implement monitoring and metrics collection and analysis and reporting approaches. • Direct and monitor security activities. • Develop methods for knowledge capture and dissemination. Develop metrics for effectiveness and efficiency.
Working Committee	• Ensure technical controls are implemented as per security requirements • Ensure effectiveness of controls • Monitor and Maintain • Ensure operational auditing mechanism is in place • Report any risks • Provide sufficient training and resources to ensure proper implementation • Report Progress

8.4 Security Program Alignment with the Business Objectives

Once the security organizational structure is all set. The Information Security Manager /Officer has to develop a strategy for the information security program and reflect it in the Information Security Policy. The Security Program has to be aligned with the business objectives of the organization and address the business risks. The security objectives should serve the protection levels required to provide safe and secure environment to achieve organizational objectives and should be reflected in the security plans and the selection of security controls.

A proper understanding of the business objectives is an important step that results in adequate security strategy and guarantees the top management buy-in and support for information security program`s initiatives. Moreover, KPIs have to be set to monitor the progress towards achieving the objectives of the strategy of the information security program.

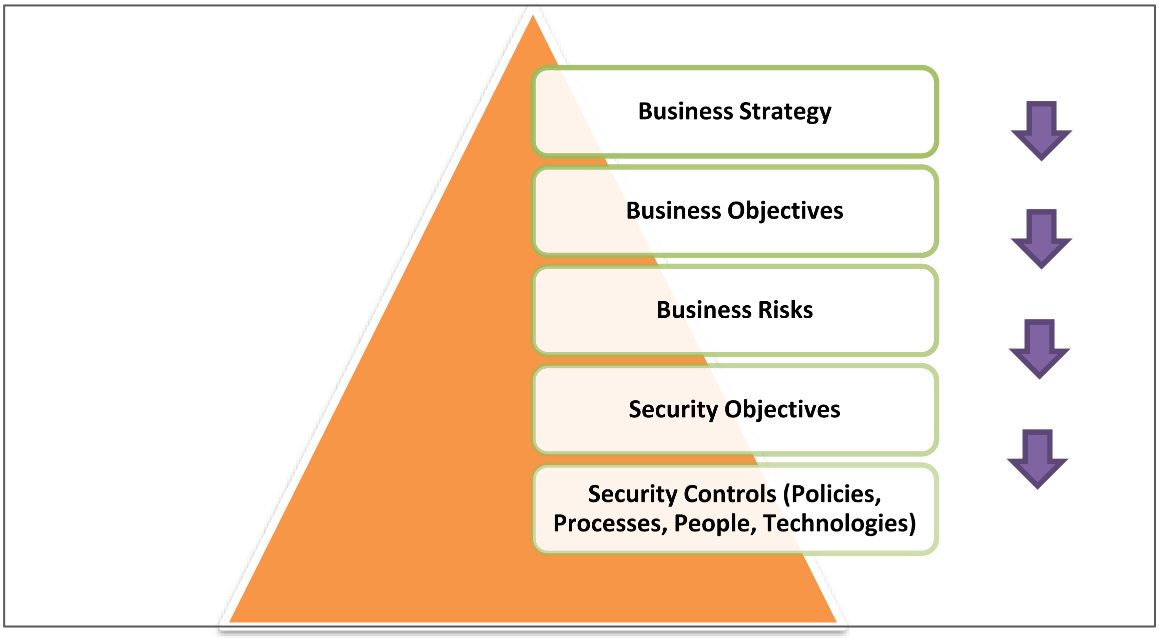


Diagram 2: The above pyramid describes building Security Strategy and Information Security Program Elements based on Business Strategy

9 Misperceptions

There has been common misperceptions drawn around the establishment of the information security office and its role within the organization, which are highlighted below:

1. Information Security Officer`s role includes the implementation of the technical security controls
2. The ISO has the authority to approve or disapprove security related initiatives.
3. The ISO intercept the business from doing its job if it doesn’t follow certain security requirements and it is perceived as a stopper.

In practice, these are not true. The information security officer shouldn’t participate in the implementation of the security controls as it creates a conflict of interest. The next section clarifies the differences between who should do the implementation and who should oversee it. At the same time, the steering committee is the only authorized one to approve or disapprove the security related projects and initiatives, including policies; Whereas ISO`s role is to assess the associated risks from a security perspective and provide recommendations based on that, then draft any required policies or proposals to be reviewed and approved by the steering committee. Moreover, the ISO shouldn’t be intercepting the business from doing its business, rather he/she should align with business objectives and work with the business owners to build effective security controls. The ISO cooperation with the different teams will build a positive culture that guarantees success of the information security program.

10 Information Security Office Vs. IT Security Team

Comparison criteria	Information Security	IT Security
Reporting to	- Head of the organization (CEO, Undersecretary, etc)	- IT Director
Team Size	- Small (1-3)	- Medium/Big (+3)
Required Skills	- Leadership/ Business/ Technical	- Technical
Main Duties	- Supervise and coordinate the implementation of the Information Security Management program - Ensure general security policy is in place, - Conduct risk assessment - Conduct regular security audits - Report progress of the ISMS program to Security Committees	- Implement Security Controls and recommendations as directed and agreed by security committees - Provide updates on the control implementations to the ISO and provide any audit related documents.

The below table compares between the different roles and functions of Information Security Office and IT Security Team.

11 Information Security Program Components

A. Risk Assessment

The role of information security in managing risk from the operation and use of information systems is very critical to the success of organizations in achieving their strategic goals and objectives. Historically, senior leaders/executives have had a very narrow view of information security either as a technical matter or in a stovepipe that was independent of organizational risk and the traditional management and life cycle processes. This extremely limited perspective often resulted in inadequate consideration of how information security risk, like other organizational risks, affects the likelihood of organizations successfully carrying out their missions and business functions. Thus conducting risk Assessment is one of the key components for running an information Security Program. The identified gaps resulted from this exercise determine decisions related to selecting controls for protecting the organization`s valuable information assets, approving changes made to the environments and other initiatives affect the security of the organization. In addition, those gaps could have various risk levels where at which the steering committee may need to focus on the risks that represent high levels and approve the strategies suggested by the ISO to overcome the gaps and ensure that the proper controls are implemented by the respective stakeholders in the organization. A comprehensive Risk Assessment should be conducted on annual basis covering all information assets owned by the organization.

Oman Government IT Risk Management Framework provides detailed guidance on Risk Assessment.

B. Controls Implementations

The control environment consists of both technical and non- technical controls (in other words, administrative controls) that are implemented to ensure measures are in place to detect and prevent security threats and protect the environment. Technical controls could cover implementing a firewall in the network with proper configurations to monitor the incoming/outgoing traffic and stop any suspicious communication, or could be installing an anti-virus in the systems to detect viruses and malwares and prevent them from harming the systems and spreading to other devices and networks. Non-technical or administrative controls includes internal security policies, creating processes and procedures that aid in setting clear understanding of how people should handle the information assets in the organization and who is responsible for each processes at what stage. There are many example of the types of controls that are listed in ISO 27002 standard that could be used as a good reference by the Information Security Officers while managing the information security program for their organizations.

C. Training and Awareness

There is a common saying in the security world that is often mentioned in the conferences and trainings, which is "people are the weakest link in any organization". Many major hacks and attacks find easier ways through people who are not aware of security threats that could compromise them, their organization and lead to big losses. Some organizations focus more on building high-tech advanced security solutions and forget to empower the human knowledge and experience with handling suspicious situations.

It is very essential to have a good training and awareness plan as part of the Information Security Plan that should include all levels in the organization to build a strong culture about security best practices. Trainings and awareness cover three main groups:

- Management Team
- Technical Teams
- End Users

It is not enough to just run security awareness sessions and get all people in one room to talk about security and how things could go wrong if they fail to act in a certain way. People need to be educated in an innovative way to buy-in their commitment and engage them fully to follow security policies and procedures. Hence, creative tools and methods need to be used to deliver an effective program and elevate the level of their awareness towards protecting their organization.

D. Auditing and Compliance

Now that the organization has established it`s information security office to manage the security program inside the organization, set all required policies, and design all it`s security controls, comes the fourth key important component, which is assuring that controls have been implemented, implemented effectively, and policies are followed to maintain a secure environment.

Regular auditing to check controls implementations and effectiveness is very critical. Audit plans should be developed with various types and timeframes (monthly, quarterly, semi-annually). It depends on the size of the organization and the audited scope.

Different auditing tools could be used for validating controls implementations, starting with system-logs to using technical mechanisms that identify vulnerabilities whithin the environment.

Audited observations should be recorded, analyzed, and reported to the management after informing the responsible teams to take corrective actions. Good auditing report indicate common patterns and help in identifying internal issues that could be solved at early stages and prevent a potential attack.

Compliance to security policies is another critical aspect that should be checked to ensure that all employees in the organization are adhering to the rules and expected actions to protect their organization and it`s valuable information.

12 Key Supportive Processes

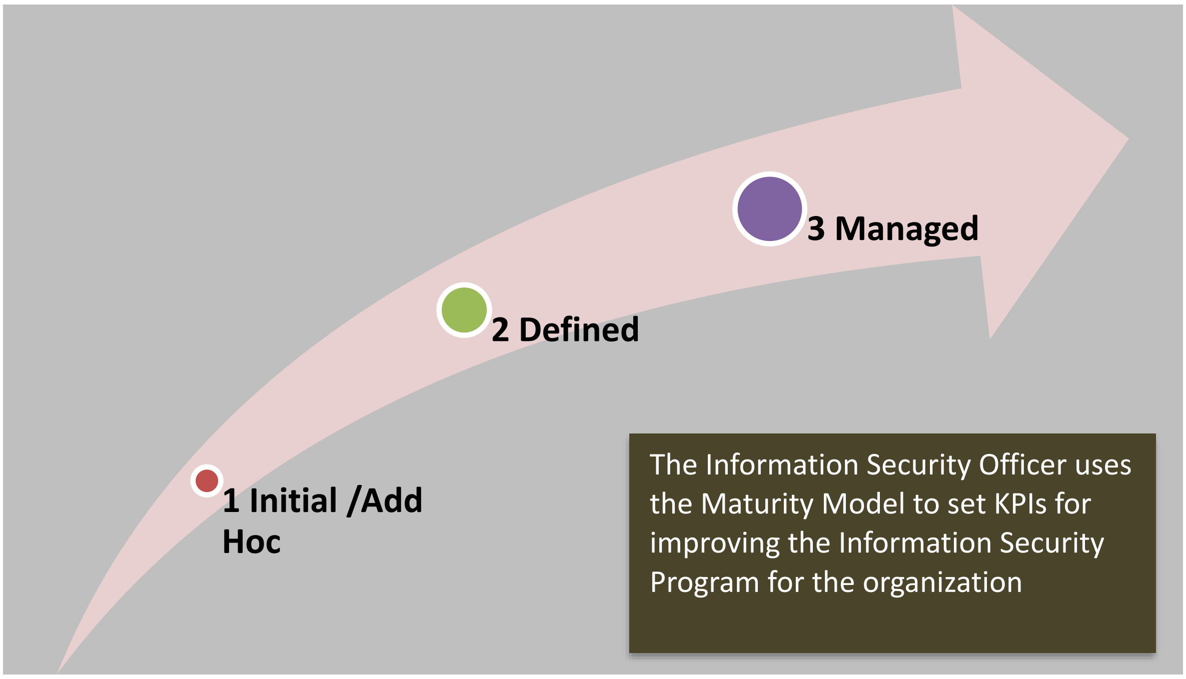
The information Security Officer works closely with the internal teams to ensure that key processes to support the information security program are in place. With the support of the management, the following processes should be established if not practiced before, or reviewed if not well managed to align with the needs of the information security program:

- **Asset Management:** this process will give great visibility on all the information assets owned by the organization, which will aid in identifying the valuable ones that will require certain levels of protections.
- **Risk Management:** as mentioned in the previous section risk is one of the critical factors to managing information security inside the organization. Having a comprehensive control over risk helps in making the right decisions to almost every aspect of the program, from analyzing threats effects on the organizational business to making investment decisions for new projects, or acquiring new technology.
- **Access and Identity Management**: having an effective control over access to the organization assets and resources contributes to saving the organization from a huge part of the threats. It helps greatly in detecting and preventing unauthorized access that could result compromising the organizations security. In addition, it could greatly assist in audit investigations.
- **Incident Handling:** The Information Security program should be equipped with defined incident handling plans and procedures to handle any security incident. All employees should be aware of who to contact and report incidents, and respective teams to respond should be trained in tackling the incidents in a fashionable manner. Timeframes for handling various severities and escalation matrix should defined and made available after obtaining the steering committee approval.
- **Business Continuity/Disaster Recovery:** Availability is one of the key elements of Information Security program. Having good plans and practices to keep the business going when there is any disaster or disruption, helps to maintain a secure environment where the flow of information and e-transactions is well managed and controlled.
- **Continual Improvement:** The Information Security Program is a journey where many lessons can be learnt at each stage and certain areas in the program could be improved. This process could be often missed while runing the program. However, it adds a big value towards having a mature environment and a supportive culture where security is maintained at higher levels. A defined process with a database to register all the feedback for enhancing the program contributes is one of the success factors.

13 Measuring Information Security Program Maturity

Implementing the information security program in any organization should be able to support the strategic goals of the organization as mentioned in the previous sections and to do so; the Information Security Officer along with the management and other stakeholders in the organization should focus on enhancing the maturity levels of the security program. They should study their current status and how well they are doing now and what they need to do to go to the next level. Many security practices in the organizations could start as Ad-hoc then with a dedicated effort they get mature day by day when the right plans with defined objectives and milestones are put in place. Risk assessment exercise might help identifying the gaps. However, the focus on building mature processes that would accelerate the performance and quality of the program should be based on certain parameters, and for that “Maturity Capability” Model is widely used.

The Maturity Capability Model is commonly known to have five levels from Non-existence of the practices to the optimized levels. The below figure represents a customized version of it that focuses more on the establishment of the Information Security management practices in the government administrative units and taking it to managed levels, thus three levels have been set to start the implementation of the Information Security Program. For more information and enlightenment on the further levels of maturity, we highly advise to refer to COBIT framework practices on the Information Security domain.



The Information Security Officer uses the Maturity Model to set KPIs for improving the Information Security Program for the organization

Maturity Model for Information Security Program

The following table describes the requirements for every maturity level that needs to be fulfilled in order to move the next level:

Level	Status	Description
0	Non Existent	• The organization does not recognize the need for Information security. • Responsibilities and accountabilities are not assigned for ensuring security. • Measures supporting the management of Information security are not implemented. • There is no Information security reporting and no response process for Information security breaches. • There is a complete lack of a recognizable system security administration process.
1	Initial /Add Hoc	• The organization recognizes the need for Information security, but awareness is fragmented and limited.

		• Information security is seen primarily as the responsibility and domain of IT and the business does not see Information security as within its domain. • Responsibilities and accountabilities for Information security are assigned to an Information security office, although the management authority of the information Security officer is limited. • Security policies are being developed, but skills and tools are inadequate. • Information security is addressed on a reactive basis, responses to Information security breaches are unpredictable. • Information security reporting is incomplete, misleading or not pertinent. • Security training is available but is undertaken primarily at the initiative of the individual.
2	**Defined**	• Security awareness exists and is promoted by management. • Information security procedures are defined and aligned with Information security policy. • Responsibilities for Information security are assigned and understood, but not consistently enforced. • An Information security plan and security solutions exist as driven by risk analysis. • Reporting on security does not contain a clear business focus. • *Ad hoc* security testing (e.g., intrusion testing) is performed • Security training is available for IT and the business, but is only informally scheduled and managed.
3	**Managed**	• Responsibilities for Information security are clearly assigned, managed and enforced. • Information security risk and impact analysis is consistently performed Security policies and procedures are completed with specific security baselines. • Exposure to methods for promoting security awareness is mandatory. • User identification, authentication and authorization are standardized. • Security certification is pursued for staff members who are responsible for the audit and management of Information security. • Security testing is completed using standard and formalized processes, leading to improvements of security levels.

		• Information security processes are coordinated with an overall organization of the security function. • Information security reporting is linked to business objectives. • Information security training is conducted for all levels: management, technical teams, and end users. • Information security training is planned and managed in a manner that responds to business needs and defined security risk profiles. • Goals metrics for security management are measured, collected and communicated. • Management uses these measures to adjust the security plan in a continuous improvement process.

14 Action Plan for establishing Information Security Program in the Organization

This section summarizes the initial steps towards establishing the information security program after appointing the information security office in the organization:

1. *Establish Steering Committee for Information Security Program or leverage existing Steering Committees.*
2. *Develop agency's own general "Information Security Policy" that is aligned with the business objectives of the organization.*
3. *Establish security organization structure.*
4. *Conduct initial comprehensive risk assessment and prepare Risk Treatment Plan.*
5. *Develop general (operational) security policies, establish Key Processes, and monitor controls implementation with the respective teams.*
6. *Conduct the Awareness Sessions to educate all employees in the organization about it.*