Advice Note:

Considering Information Security Management

Supporting the *Public Service ICT Strategy*

September 2018

An Roinn Caiteachais
Phoiblí agus Athchóirithe
Department of Public
Expenditure and Reform

Preface

A key objective of the Public Service ICT Strategy[1] is improving governance around ICT in the Public Service. Effective governance ensures that projects are aligned, directed, and monitored to support the specific goals and objectives of a Public Body at a whole-of-government level[2]. This is in line with the goals of the Public Service Reform Plan and supports the unification approach envisaged in the Civil Service Renewal Plan. To support this approach to governance, policies and advice are required to inform Public Bodies on individual ICT issues.

The Office of the Government Chief Information Officer (OGCIO) in the Department of Public Expenditure and Reform develops policies and advice notes on key ICT issues to manage risk and support standardisation and integration[3]. The first such advice note was *Considering Cloud Services*[4]. This advice note, *Considering Information Security Management*, aims to assist Public Bodies in making informed, risk-based decisions in relation to the improvement of Information Security within their organisation.

Office of the Government CIO
Department of Public Expenditure and Reform
September 2018

Feedback is welcome and can be sent by email to egov@per.gov.ie.

[1] http://ictstrategy.per.gov.ie/
[2] In this context “whole-of-government” refers to non-commercial public bodies.
[3] It is also important to recognise that these advice notes are complimentary to other policies such as codes of ethics, standards and behaviours etc. for the Public Service.
[4] http://www.per.gov.ie/wp-content/uploads/Considering-Cloud-Services-December-2015.pdf

Table of Contents

1. Executive Summary

Information Security Management is now, more than ever, an essential activity in any organisation, large or small. Developments in technology and processes as well as the drive towards digital services mean that organisations capture and process more data and information than ever before. Some of this data and information can be sensitive and/ or personal and therefore its confidentiality, integrity and availability is paramount in particular in the context of the General Data Protection Regulation.

The complexity of modern computer-based systems means that they risk being inherently insecure and vulnerable and therefore must be developed in line with best practice and may also require on-going attention and regular remedial attention. The highly mobile nature of access to systems via smartphones, laptops and tablets, means that it is essential to protect both the physical and digital boundaries of an organisation. In addition, the frequency and widespread media reporting of malicious attacks reflects the continuing growth in borderless cybercrime where criminal acts are committed from far away shores.

A focus on Information Security Management should form one dimension of any organisation's efforts to ensure continuity of operations, protection of customer data, citizen and business, and the reputation and confidence of the service provided by an organisation. It is important to remember that not all information security-related risks arise from human intervention or behaviours, i.e. challenges to continuity of ICT/ digital service delivery can come from a wide variety of sources such as a building fire or leak, vulnerabilities in computer chips and operating systems software code, natural disaster, weather events, or global warming.

The objective of this document is to provide advice to enable public service bodies build on and develop robust and standards-based Information Security Management Systems. Section 2 introduces the topic while Section 3 explains Information Security in more detail and the potential legal obligations may exist. Section 4 sets out the importance of establishing an Information Security Management System (ISMS) accompanied by suggestions on important areas to be the focus of that system.

A series of Appendices provide additional insight in relation to suggested strategies and activities and provide more detailed information on terminology and definitions, legal obligations, Information Security frameworks, and sources of information in relation to threats and vulnerabilities of your ICT enabled and digital systems.

This advice note is intended to assist in a greater understanding of the extent to which Information Security Management is an essential activity to ensure the confidentiality, integrity and availability of your organisation's important information assets. Protection of such digital assets can, in some part, be achieved by the implementation of the suggested strategies and activities which are aimed at enhancing your organisation's Information Security management approach.

However, it is important to realise that Information Security Management is an on-going endeavour and not something that is point-in-time or once-off. Ongoing reviews and/or updates are essential as is user awareness raising and training. Furthermore, an Information Security management policy should complement other corporate policies such as acceptable usage policies, codes of standards and behaviour, ethics, Official Secrets, etc.

Note: As Information Security Management is directly relevant to a number of areas in every organisation, right up to and including senior management, this advice note should be read, and acted upon, as a cross-functional programme within your organisation.

2. Introduction

This advice note, *Considering Information Security Management*, lays a foundation for a shared understanding of information security in Government. It is based on the generally accepted information security principles of confidentiality, integrity and availability as the most effective means for an organisation to effectively secure its digital information assets.

Information, which encompasses data, is a corporate asset like any other that needs to be managed, maintained and protected. An Information Security Policy and System are essential elements in any organisation's efforts to ensure continued availability of and trust in its systems.

There is an increasing dependence on information and communications technologies (ICTs) in all aspects of society, including the provision of public services. Through a series of initiatives, action plans and strategies, eGovernment has fundamentally changed the way in which Governments conduct business. Governments are dependent on ICTs to deliver services to citizens and businesses, and to efficiently manage internal Government operations.

However, the infrastructure underpinning these services often has significant inherent risks, resulting in unprecedented levels of threats to information security and privacy in recent years in both public and private organisations. The following chart shows the percentage of breaches per type of breach action over a number of years[5]:

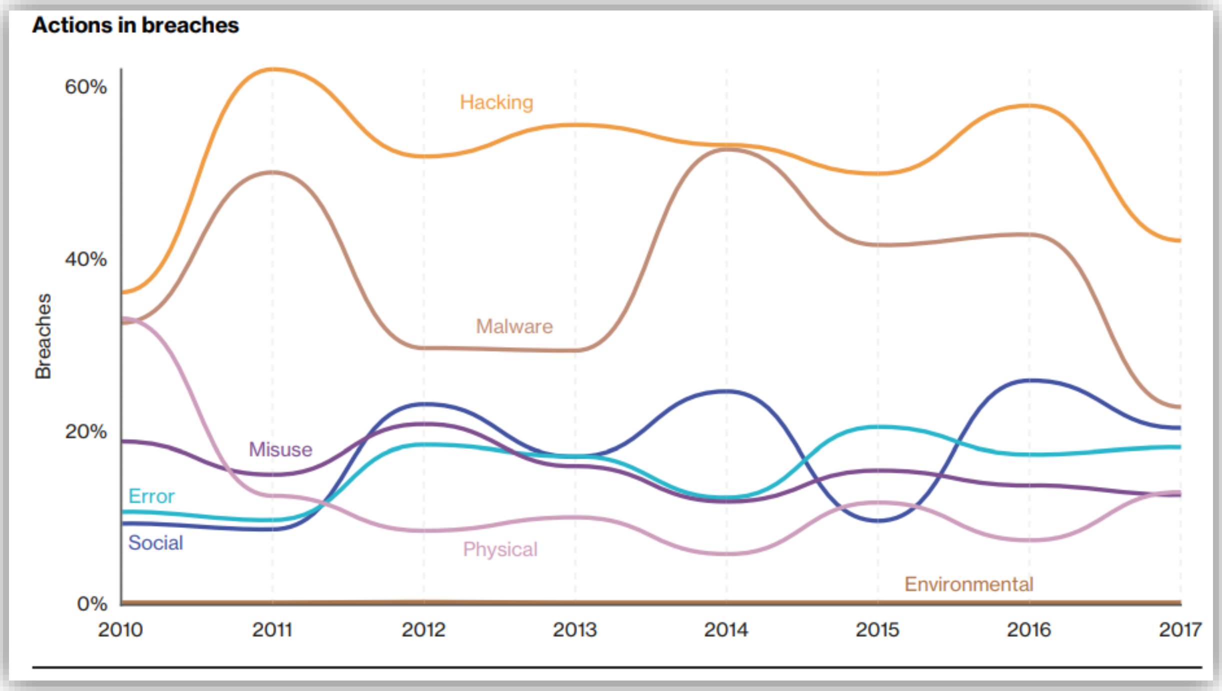


Figure 1 - Percentage of breaches per threat action category over time

[5] Chart courtesy of Verizon 2018 Data Breach Investigations Report http://www.verizonenterprise.com/verizon-insights-lab/dbir/

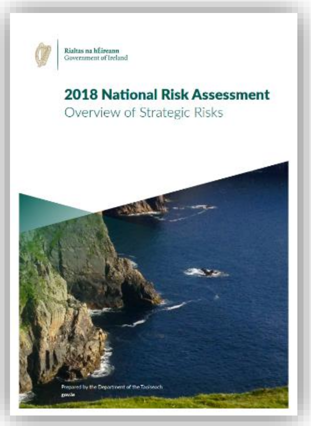


Figure 2 National Risk Assessment for 2018

The Government's National Risk Assessment for 2018[6] highlights *"The public service is also a major collector and processor of data. A specific risk is the targeting of public service data repositories, and the theft or compromising of that data. If successful, this would reduce confidence in public service administration and the use of technology for public services."* This and the continuing drive to digital government services and the EU's eGovernment Action Plan 2016-2020 – Accelerating the Digital Transformation of Government[7] suggests that it is timely to review our approach to protecting the data and information assets entrusted to us by citizens and businesses.

In order to reduce the chance of these risks occurring, Public Service Bodies (PSBs) need to establish appropriate management systems, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and enhance information security.

This paper aims to enable a consistent whole-of-government approach to establishing a security framework for the protection of digital information assets across the Irish Public Service. It outlines an approach for managing digital information and digital information systems and aims to help PSBs manage business risks and assure continuity of service delivery. It also sets out what PSBs should consider to ensure they are managing information security effectively.

Information Security is an important issue for many parts of an organisation, including senior management, and does not simply fall within the scope of its ICT function, as will be explained later. Consequently, this advice note should be read and acted on as appropriate by a number of areas of responsibility within your organisation including:

- Senior Management Team / Management Board / Chief Information Officer
- Internal Audit Personnel, Corporate Risk Management, and Data Protection Officers
- Data / Information Owners and Information Systems Owners, in particular those responsible for personal data.
- Chief / Information Security Officers (C/ISOs) and Information Security Practitioners
- ICT Managers
- Human Resource Personnel
- Facilities Management Personnel

[6] 16 July 2018 – Government Press Release - Government publishes National Risk Assessment 2018 https://www.taoiseach.gov.ie/eng/News/Government_Press_Releases/Government_publishes_the_National_Risk_Assessment_2018.html

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0179

While not an exhaustive guide, implementing the recommendations in this advice note will assist PSBs in providing assurance that they have appropriate and effective measures in place to protect State, business and citizen digital information. These will form one element of an organisation's set of Information Security policies along with, for example, acceptable usage policies and codes of conduct (Civil Service Code of Standards and Behaviour[8], Civil Service Disciplinary Code[9], and the Guidelines on Compliance with the Provisions of the Ethics in Public Office Acts 1995 and 2001[10]), the Official Secrets Act and the data protection legislative framework[11].

[8] http://www.sipo.gov.ie/en/Codes-of-Conduct/Civil-Servants/

[9] http://hr.per.gov.ie/discipline/

[10] http://www.sipo.gov.ie/en/Guidelines/Guidelines-for-Public-Servants/

[11] See the Data Protection Commission website at https://www.dataprotection.ie/

3. What is Information Security?

3.1. Information Security

Information security, sometimes shortened to InfoSec, is the practice of defending information/data from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Information security encompasses three main elements: confidentiality, integrity and availability (often referred to as the C-I-A triad):

- Confidentiality – to uphold authorised restrictions on access to and disclosure of information including personal or proprietary information.
- Integrity – to protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.
- Availability – to provide authorised users with timely and reliable access to information and services.

3.2. Cyber Security

Information Security and Cyber Security are often incorrectly used interchangeably. Cyber Security is concerned with managing the security of an organisation's information assets from attack from outside the organisation through the cyber or internet world.

The scope of Information security extends wider than that of just Cyber Security as risks and threats to an organisation's information assets exist from not just the Internet world. Risks such as accidental loss, physical theft, fire, sabotage (including from internal sources) could lead to damage to your organisation's information assets.

3.3. Legal Obligations

Organisations should also be aware of their legal obligations and required compliance with relevant legislation and regulations as well as internal codes of conduct, acceptable usage policies etc.

Relevant data retention and data protection legislation and regulations such as:

- EU Regulation 2016/679 (new) General Data Protection Regulation (GDPR) as a replacement of the current Data Protection Acts
- The Data Protection Acts of 1988, 2003 and 2018
- National Archives Act, 1986 and the associated National Archives Regulations, 1998

should be adhered to in the context of Information Security. Further information is available in Appendix B.

Any Information Security failure can have serious repercussions for....

1) citizen's personal data,
2) your organisation's business operations,
3) the reputation and confidence of the service being provided.

4. Suggested Strategies and Activities to Enhance your Information Security Posture

4.1. Introduction

The importance of enhancing your organisation's information security posture so as to protect its information assets has been identified already. Therefore, not dissimilar to any other initiative within your organisation, you enhance your security environment through a systematic approach. In that regard, the existence of an Information Security Management System (ISMS) is recommended.

4.2. Establish an Information Security Management System (ISMS)

4.2.1. Overview

An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. An ISMS is a systematic approach to enhancing an organisation's information security to achieve business objectives. It is based upon a risk assessment and the organisation's risk acceptance level designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS:

a) awareness of the need for information security
b) assignment of responsibility for information security
c) incorporating management commitment and the interests of stakeholders
d) enhancing societal values (e.g. privacy of citizen data)
e) risk assessments determining appropriate controls to manage acceptable levels of risk
f) security incorporated as an essential element of information networks and systems
g) active prevention and detection of information security incidents
h) ensuring a comprehensive approach to information security management
i) a continual reassessment of information security and making of modifications as appropriate
j) information security should not be an afterthought, but ought to be embedded in the design, development and implementation phases of an ICT enabled project.

4.2.2. Industry Frameworks and Standards

It is recommended that an already established and proven internationally recognised framework be used in order to reduce the effort and resources in establishing an ISMS. Indeed many PSBs already have an ISMS which have generally been developed using internationally recognised standards and frameworks. Some of the following well-known

Information Security frameworks should be considered by organisations developing their ISMS:

- ISO/IEC 27001:2013 Information technology – Security Techniques – Information security management systems — Requirements
- European Union Agency for Network and Information Security (ENISA) - Technical Guideline on Security Measures
- National Institute of Standard and technology (NIST) Risk Management Framework (RMF)
- National Institute of Standard and technology (NIST) Cybersecurity Framework (CSF)
- Information Systems Audit and Control Association (ISACA) COBIT 5 for Information Security

You may wish to use any of these frameworks as a basis for, or as complementary advice to any new or existing Information Security programme within your organisation. Further information on each of these frameworks is set out in Appendix C.

4.3. Priority Focus Areas in the Establishment of an ISMS

As in any Management System, an Information Security Management System is composed of many elements and activities. This Advice Note shall provide additional detail on 3 focus areas it considers important to any successful ISMS implementation. Note, this does not mean that other elements within an ISMS programme should be ignored.

Establish an Information Security Management System (ISMS)

Have a systematic approach to enhancing your organisation's information security posture through the implementation of an ISMS.

ISMS Focus Area 1	ISMS Focus Area 2	ISMS Focus Area 3
Ensure the Existence of Good Governance	Adopt a Risk Management Approach	Stay Informed of the Latest Threats and Vulnerabilities
Through good governance, ensure the existence of appropriate senior management roles, ownership and leadership in relation to Information Security.	Underpin your ISMS with an Information Security based Risk Management System.	Minimising your exposure to new information security threats and vulnerabilities in a constantly changing world.

4.4. ISMS Focus Area 1 – Ensure the Existence of Good Governance

ISMS Focus Area 1 - Through good governance, ensure the existence of appropriate senior management roles, ownership and leadership in relation to Information Security.

Information security is an organisation-wide issue and requires an enterprise approach to ensure an effective information security posture is in effect. Information Security is not simply a matter for your ICT Division. ICT management is only one of many stakeholders with responsibility for the implementation of an effective information security posture within your organisation.

Due to the importance of an effective information security programme within your organisation, it is therefore essential that any implementation is underpinned by appropriate governance structures. Remember, any information security failure can have serious repercussions to your organisation's business operations, citizens' personal data and reputation and confidence in the service being provided.

For the development, implementation and ongoing operation of an Information Security Management System, good information security governance will ensure:

- Senior management are accountable (sub-committees can be formed with oversight from senior management)
- Senior management are confident that adequate management of information security is in place across the organisation.
- Your organisation meets its obligations in relation to any legislation, directive and regulations (e.g. Data Protection Acts)
- Information security is treated as an organisation-wide issue
- That a strong culture of information security is embraced by all parts of the organisation through the adoption of information security related staff policies and awareness building, through training and regular communication with staff.
- A good information security posture is a mandatory requirement for any organisation especially as most Public Service Bodies' risk appetite should be low in relation to the compromise of important information assets.
- Any approach is risk based.
- The necessary roles, responsibilities and segregation of duties are defined.
- Adequate resources are allocated.
- That any management system is planned, managed, measurable, measured, reviewed and audited.
- That cross divisional support is achieved. A good information security programme requires the assistance of many stakeholders in your organisation. For example:
  - Senior Management – ownership of an information security programme by Senior Management provides clear leadership within your organisation. It facilitates where required, organisational change management and develops a strong culture of information security at all levels.

- All Staff – Staff are key part of any information security programme. Through continuous education and awareness, staff play a key role in collectively ensuring that an organisation’s information security policies are adhered too.
- ICT Division – for governance of policies in relation to the ensuring secure and appropriate access to an organisation electronic information assets.
- Human Resources - for governance of policies in relation to behaviours and ensuring appropriate usage of organisation assets (noting that not all organisation assets are electronic).
- Facilities Management – for governance of policies in relation to the ensuring secure and appropriate physical access to the organisations offices.
- Audit Divisions – for ensuring compliance with organisation information security policies.

4.5. ISMS Focus Area 2 – Adopt a Risk Management Approach

ISMS Focus Area 2 - Underpin your ISMS with an Information Security based Risk Management System.

4.5.1. Overview

As part of enhanced corporate governance[12] within the Public Service, all PSB’s should now be operating some form of a corporate Risk Management system. To assist PSB’s with this objective, the following guidance and handbook were published by the Department of Public Expenditure and Reform (D/PER):

RISK MANAGEMENT GUIDANCE
for Government Departments and Offices

February 2016

Figure 3- Risk Management Guidance for Government Departments and Offices (February 2016)

- Risk Management Guidance for Government Departments and Offices (February 2016)[13]
- Risk Management Handbook[14]

The guidance from D/PER on corporate Risk Management is based on international best practice through the adoption of the principles of the **ISO 31000 – Risk Management**[15] standard.

Therefore, similar to corporate risk governance, good governance of Information Security risk is underpinned by the implementation of a suitable Risk Management methodology relevant to the domain in question (in our case Information).

[12] Corporate Governance Standard for the Civil Service - http://www.per.gov.ie/en/corporate-governance-standard/
[13] http://govacc.per.gov.ie/risk-management/
[14] http://www.reformoffice.per.gov.ie/resources/
[15] https://www.iso.org/iso-31000-risk-management.html

4.5.2. Risk Management within an Information Security Management System

As already identified, in the establishment of an ISMS, Risk Management is usually a cornerstone of any such system. This is because the main philosophy of most ISMS is to find out what information security incidents could occur (assess) and then find the most appropriate way to prevent or avoid if necessary such incidents (by treatment) from affecting your organisation and related stakeholders.

In line with the ISO/IEC 27000 series of standards for Information Security, ISO has developed the **ISO 27005 - Information Security Risk Management** standard as a framework to implementing this aspect of an ISMS.

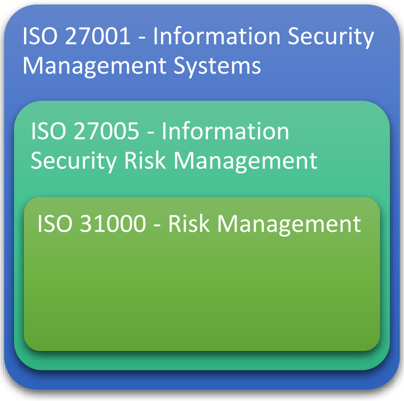

ISO 27001 - Information Security Management Systems
ISO 27005 - Information Security Risk Management
ISO 31000 - Risk Management

Figure 4- ISO Hierarchy re risk

The ISO 27005 standard is also aligned with the ISO 31000 Risk Management standard (which in turn is used as the basis for the Risk Management Guidance for Government Departments and Offices).

Therefore it is preferable to use the ISO 27005 standard as a basis for an Information Security Risk management systems as it uses many of the same concepts and vocabulary.

This will assist in securing buy-in for your Information Security Risk Management system with Senior Management owing to the functional overlap with your existing corporate Governance Risk Management methodology.

Figure 5 sets out the ISO 27005 Risk Management workflow:

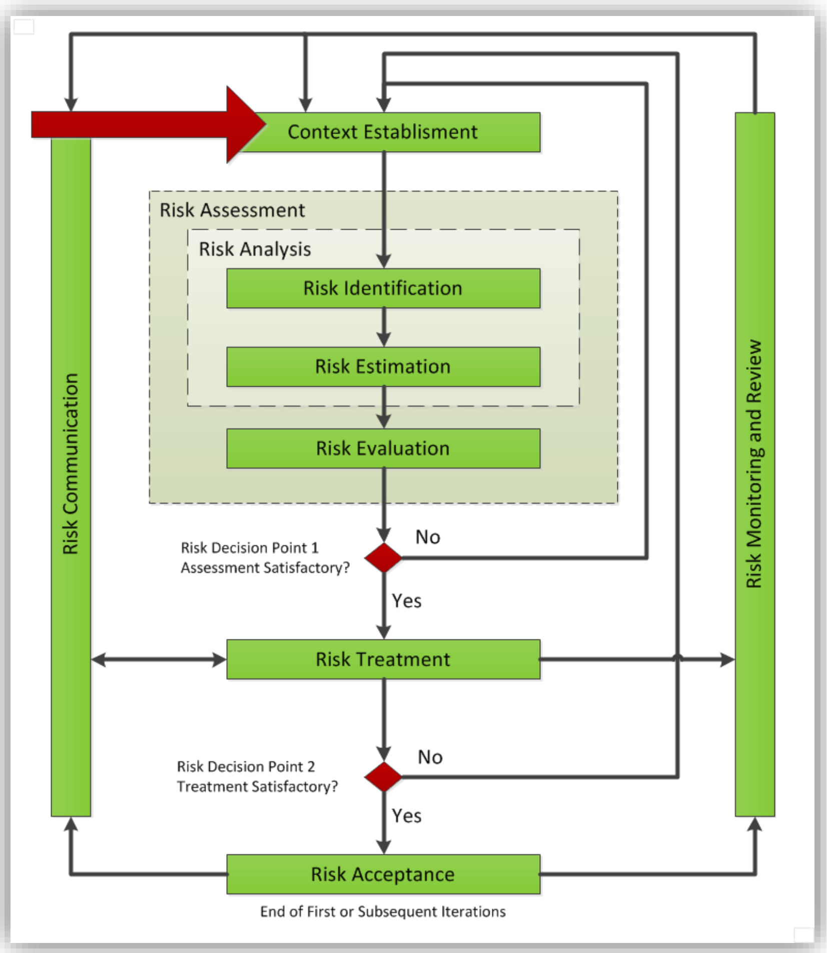


Figure 5 - ISO 27005 Risk Management Workflow

Note, other Risk Management frameworks can be used that you may know of or already use within your own organisation. However, it should align to the general principles and objectives outlined here.

4.6. ISMS Focus Area 3 – Staying Informed of the Latest Threats and Vulnerabilities

ISMS Focus Area 3 - Minimising Your Exposure to New Information Security Threats and Vulnerabilities in a Constantly Changing World.

As stated previously, a risk based management approach is a cornerstone of any ISMS. Any risk based management system will involve *Risk Identification* and potential mitigation of those risks thought some *Risk Treatment* process.

Risk Identification is the process of identifying threats and vulnerabilities across all your information assets.

Threats can be of various categories such as:

- deliberate physical attack (theft, unauthorised physical access, sabotage)
- unintentional damage (information leakage due to human error by employees, loss of devices, storage media and documents)
- natural / environmental disaster (water, fire)
- failure / malfunction (power supply outage, failure of systems, failure of service providers)
- nefarious activity / abuse (identity theft, denial of service, spyware, ransomware)
- legal (violation of data protection laws)
- lack of understanding by system users
- lack of change control

A vulnerability is an existing weakness that can be exploited by a threat of the types identified above. An existing vulnerability for example to these threats could be:

- lack of physical security / monitoring
- a weak password policy
- lack of security awareness to social engineering / phishing
- insufficient system hardening
- insufficient system maintenance and patching
- out-of-support Software
- excessive privilege access to systems

As part of the risk assessment process of the threats and vulnerabilities to your information assets, you may decide to mitigate the risk by taking corrective action by the implementation of certain security controls (safeguards and countermeasures).

Therefore it is vital that your Information Security personnel keep themselves abreast of all the available security controls relevant to your organisation’s infrastructure. Note this necessary activity of constant knowledge gathering in this field is in the context of a constantly changing and incessant manifestation of new threats and vulnerabilities occurring almost daily. Appendix D offers some potential information sources to stay abreast of latest threats, vulnerabilities and potential security control options.

5. In Conclusion

In the current climate of increasingly sophisticated, pervasive and potentially very damaging cyber security attacks materialising across the globe, the continued prioritisation and development within your organisation of a robust Information Security Management programme cannot be understated. This is particularly true for Public Service Bodies who in many cases process and store important personal data about citizens and businesses.

Therefore Public Service Bodies should consider enacting, as many already have, the principles and objectives outlined previously.

Public Service Bodies should also take note of Appendices A-D as these provide additional insight in relation to the suggested strategies and activities by providing more detailed information on terminology and definitions, legal obligations, Information Security frameworks, and sources of information in relation to potential threats and vulnerabilities to your ICT enabled systems.

Finally, Information Security Management must not be perceived as an issue for your ICT Division to resolve and manage alone. Information Security Management is about how your organisation as a whole constantly manages risk to its own information assets. Any information security incident that could affect your organisation's ability to function or result in the loss of citizen and business data to nefarious individuals, organisations or states is a matter for your organisation as a whole to manage.

Appendices

Appendix A - Key Terminology and Definitions

For the purposes of this document, the following key important terms and definitions apply.

Note, many of the definitions are extracted from the ISO 27000 – Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary Standard).

Information

Information is an asset that, like other important business assets, is essential to an organisation's business and consequently needs to be suitably protected. Information can be stored in many forms, including: digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as unrepresented information in the form of employee knowledge. Information may be transmitted by various means including: courier, electronic or verbal communication. Whatever form information takes, or the means by which the information is transmitted, it always needs appropriate protection.

Government is dependent upon information and communications technology. This technology is often an essential element in the organisation and assists in facilitating the creation, processing, storing, transmitting, protection and destruction of information. [16]

Security Posture

The security status of an enterprise's networks, information, and systems based on information architecture resources (e.g. people, hardware, software, policies) and capabilities in place to manage the defence of the enterprise and to react as the situation changes [17].

Management

Management involves activities to direct, control and continually improve the organisation within appropriate structures. Management activities include the act, manner, or practice of organizing, handling, directing, supervising, and controlling resources. Management structures extend from one person in a small PSB to management hierarchies consisting of many individuals in PSB's.

In terms of an Information Security, management involves the supervision and making of decisions necessary to achieve business objectives through the protection of the PSB's information assets. Management of information security is expressed through the formulation and use of information security policies, procedures and guidelines, which are then applied throughout the organisation by all individuals associated with the organisation. [18]

[16] ISO 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary. Section 3.2.2.

[17] National Institute of Standards and Technology (NIST) - https://www.nist.gov/publications/glossary-key-information-security-terms-1

[18] ISO 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary. Section 3.2.4.

Management System

A management system uses a framework of resources to achieve an organisation's objectives. The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources. In terms of information security, a management system allows an organisation to:

a) Satisfy the information security requirements of customers (and/or citizens) and other stakeholders;
b) Improve an organisation's information security plans and activities;
c) Meet the organisation's information security objectives;
d) Comply with regulations, legislation and industry mandates; and
e) Manage information assets in an organised way that facilitates continual improvement and adjustment to current organisational goals. [[19]]

Risk

Risk is often expressed in terms of a combination of impact (or consequences) of an event and the associated likelihood (or frequency) of occurrence.

Therefore in relation to Information Security, a risk is said to exist when there is an identifiable likelihood of an identified threat exploiting an identified vulnerability of an Information asset, and where that compromise will have a quantifiable impact to the organisation. Without likelihood and impact, there is no risk.

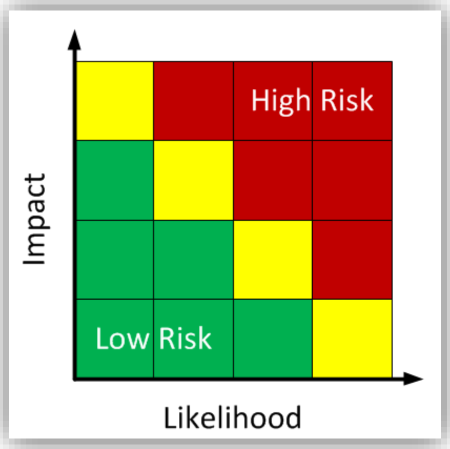


Figure 6 - Example Risk Heat Map

[19] ISO 27000 – Information technology – Security techniques – Information security management systems – Overview and vocabulary. Section 3.2.5.

Appendix B - Example Legal Obligations in Relation to Information Security

EU Regulation 2016/679 - General Data Protection Regulation (GDPR)

The purpose of EU Regulation 2016/679[20] is to unify and enhance data protection laws within the European Union. It was formally adopted by the European Commission in April 2016 and came into effect in May 2018. It is often referred as the General Data Protection Regulation (GDPR) and replaces EU Directive 95/46/EC[21].

The aim of the GDPR is to implement a harmonised data protection regime within the EU. It includes much greater accountability and a much stricter data protection compliance environment for data controllers and data processors.

As stated in the Data Protection Commissioner's 2017 Annual Report[22]:

> *"The GDPR's focus is on demanding accountability from organisations in how they collect and process personal data. The best results for data subjects are secured when organisations of all types deliver on their obligations to be fair and transparent."*

Data Protection Act 2018

Although the GDPR is directly applicable as a law in all Member States, it allows for certain issues to be given further effect in national law. In Ireland, the Data Protection Act 2018, amongst other things, gives further effect to the GDPR.

While the Data Protection Act 2018 doesn't set out specific security measures to protect personal data, it does require that "the data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against— (i) unauthorised or unlawful processing, and (ii) accidental loss, destruction or damage"[23].

It further states that "In determining appropriate technical or organisational measures …, a controller shall ensure that the measures provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned"[24].

[20] Full title is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

[22] https://www.dataprotection.ie/docimages/documents/DPC%20Annual%20Report%202017.pdf

[23] Section 71(1)(f) http://www.irishstatutebook.ie/eli/2018/act/7/section/71/enacted/en/html#sec71

[24] http://www.irishstatutebook.ie/eli/2018/act/7/section/72/enacted/en/html#sec72

Data controllers and processors are required to "take all reasonable steps to ensure that—(a) persons employed by the controller or the processor, as the case may be, and (b) other persons at the place of work concerned, are aware of and comply with the relevant technical or organisational measures"[25].

Data Protection Acts of 1998 and 2003

The main Irish law dealing with data protection before the implementation of GDPR was the Data Protection Act of 1988. This was amended by the Data Protection (Amendment) Act 2003 to bring our laws into line with the EU Data Protection Directive 95/46/EC.

Note that although the GDPR came into effect in May 2018, in some circumstances the 1998 and 2003 Acts will still apply.

Note For advice on data protection issues, check with your own data protection officer or legal advisor. Further information on the data protection legislative framework can be found on website of the Office of the Data Protection Commission[26].

[25] *Ibid*

[26] https://www.dataprotection.ie/

Appendix C - Information Security Frameworks

This section provides further information in relation to several Information Security frameworks:

1. ISO/IEC 27001
2. ENISA – Technical Guideline on Security Measures
3. National Institute of Standards and Technology (NIST)
4. NIST Risk Management Framework (RMF)
5. NIST Cybersecurity Framework
6. ISACA COBIT 5 for Information Security

1. ISO/IEC 27001 and ISO/IEC 27K Series

The ISO/IEC 27001[27] is a globally recognised certifiable standard for an ISMS. It is published jointly by the International Organisation for Standardisation (ISO)[28] and the International Electrotechnical Commission (IEC)[29]. Organisations which meet the standard may be certified compliant by an independent and accredited certification body on successful completion of a formal compliance audit.

Due to it being a globally recognised standard, it is one of the most widely respected and adopted Information Security framework amongst IT enabled organisations. According to the International Standard Organisation (ISO), in 2016[30], the number of organisations globally accredited to the ISO 27001 standard was 33290 (a 21% increase from 2015) of which 175 organisations were in Ireland. Some of those accredited in Ireland are Public Sector Bodies.

ISO/IEC 27001 is part of a larger Information Security set of ISO standards – namely ISO 27000 Series. The most important standards of the series are as follows.

Terminology

ISO 27000 - Information security management systems — Overview and vocabulary.
This is an excellent introduction and overview of information security management systems, along with terms and definitions used in the ISO 27000 series. Also, it is **free** to download[31].

General Requirements

ISO 27001 - Information technology – Security Techniques – Information security management systems — Requirements.
This standard formally specifies an ISMS, a suite of activities concerning the management of information risks.

[27] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534
[28] http://www.iso.org/
[29] http://www.iec.ch/
[30] http://www.iso.org/iso/home/standards/certification/iso-survey.htm
[31] http://standards.iso.org/ittf/PubliclyAvailableStandards/

General Guidelines

ISO 27002 - Information technology — Security techniques — Code of practice for information security controls.

This guidance document recommends a set of 14 security control categories with 35 control objectives (see table below) with implementation guidance with each one. Example security control categories for instance are: Human resource security, Asset management, Access Control, Physical and environmental security, Operations security.

ISO 27003 - ISMS Implementation Guidelines.

This provides practical guidance on the implementation of an ISO 27001 aligned ISMS

ISO 27004 - Information Security Management – Measurement.

This guidance assists organisations to measure the effectiveness of an ISMS. An ISMS in a continuous change / improvement cycle and "what gets measured gets improved" (Peter Drucker).

ISO 27005 - Information Security Risk Management

ISO 27001 has a strong focus on risk based management activities. ISO 2005 builds on this to provide more guidance in relation to building an Information Security focused risk management system within your organisation.

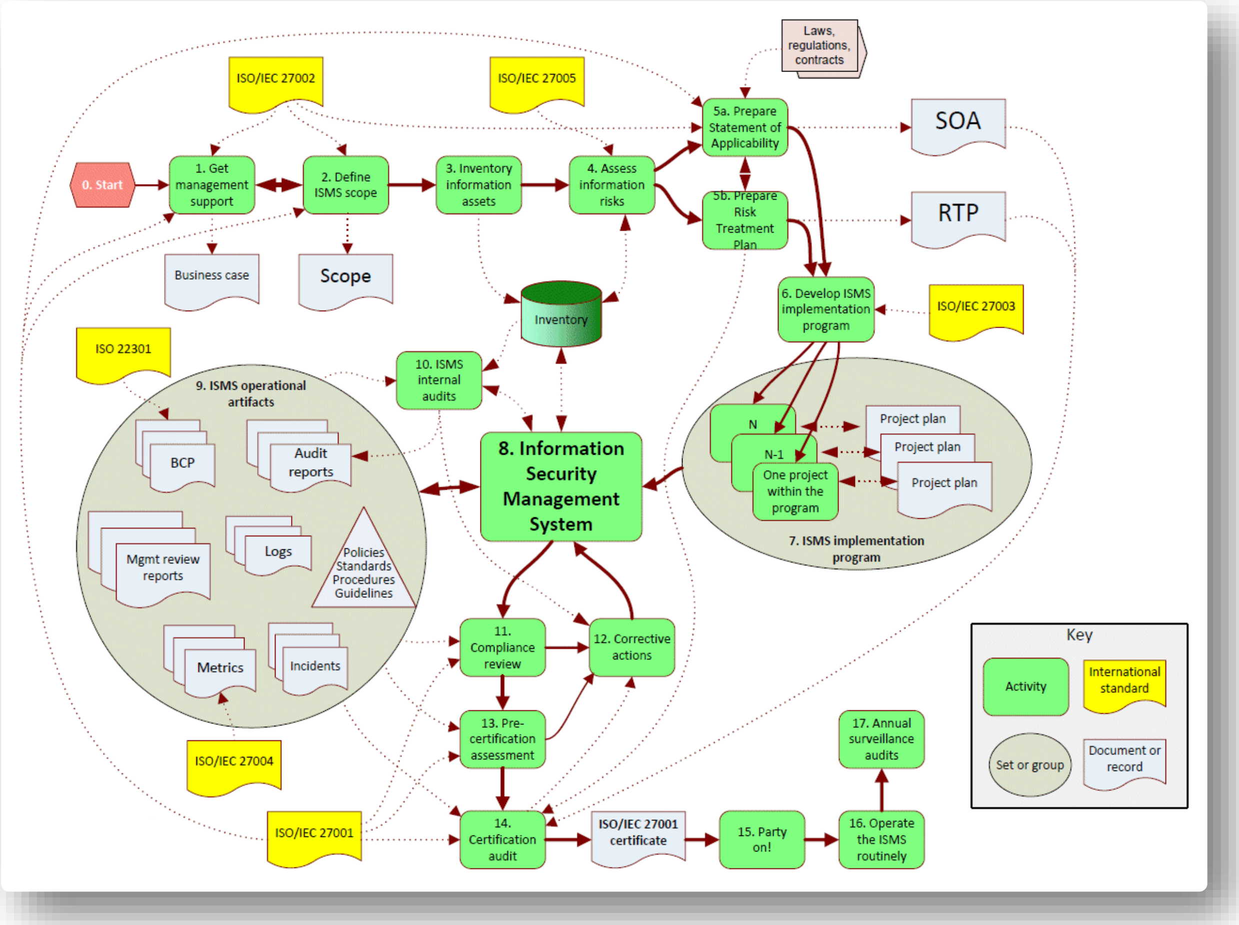

Laws, regulations, contracts
ISO/IEC 27002
ISO/IEC 27005
5a. Prepare Statement of Applicability
SOA
0. Start
1. Get management support
2. Define ISMS scope
3. Inventory information assets
4. Assess information risks
5b. Prepare Risk Treatment Plan
RTP
Business case
Scope
Inventory
6. Develop ISMS implementation program
ISO/IEC 27003
ISO 22301
10. ISMS internal audits
9. ISMS operational artifacts
BCP
Audit reports
8. Information Security Management System
N
N-1
One project within the program
Project plan
Project plan
Project plan
7. ISMS implementation program
Mgmt review reports
Logs
Policies Standards Procedures Guidelines
Metrics
Incidents
11. Compliance review
12. Corrective actions
Key
Activity
International standard
Set or group
Document or record
13. Pre-certification assessment
17. Annual surveillance audits
ISO/IEC 27004
ISO/IEC 27001
14. Certification audit
ISO/IEC 27001 certificate
15. Party on!
16. Operate the ISMS routinely

Figure 7 - Suggested ISMS Implementation and Certification Process Workflow.
Source - ISO27k Toolkit - http://www.iso27001security.com/html/toolkit.html
Distributed under the Creative Commons Attribution-Non-commercial-Share Alike 3.0 license

Table of ISO 27002 Security Control Categories and Control Objectives

ISO 27002 Control Reference	ISO 27002 Control Description
A.5	Information security policies
A.5.1	Management direction for information security
A.6	**Organisation of information security**
A.6.1	Internal organisation
A.6.2	Mobile devices and teleworking
A.7	**Human resource security**
A.7.1	Prior to employment
A.7.2	During employment
A.7.3	Termination and change of employment
A.8	**Asset management**
A.8.1	Responsibility for assets
A.8.2	Information classification
A.8.3	Media handling
A.9	**Access control**
A.9.1	Business requirements of access control
A.9.2	User access management
A.9.3	User responsibilities
A.9.4	System and application access control
A.10	**Cryptography**
A.10.1	Cryptographic controls
A.11	**Physical and environmental security**
A.11.1	Secure areas
A.11.2	Equipment
A.12	**Operations Security**
A.12.1	Operational procedures and responsibilities
A.12.2	Protection from malware
A.12.3	Backup
A.12.4	Logging and monitoring
A.12.5	Control of operational software
A.12.6	Technical vulnerability management
A.12.7	Information systems audit considerations
A.13	**Communications security**
A.13.1	Network security management
A.13.2	Information transfer
A.14	**System acquisition, development and investment**
A.14.1	Security requirements of information systems
A.14.2	Security in development and support processes
A.14.3	Test data

ISO 27002 Control Reference	ISO 27002 Control Description
A.15	**Supplier relationship**
A.15.1	Information security in supplier relationships
A.15.2	Supplier service delivery management
A.16	**Information security incident management**
A.16.1	Management of information security incidents and improvements
A.17	**Information security aspects of business continuity management**
A.17.1	Information security continuity
A.17.2	Redundancies
A.18	**Compliance**
A.18.1	Compliance with legal and contractual requirements
A.18.2	Information security reviews
A.18.3	Technical compliance review

2. ENISA – Technical Guideline on Security Measures

The European Union Agency for Network and Information Security (ENISA) published[32] guidance in October 2014 to assist National Regulatory Agencies (NRAs) in the Electronic Communications / Telco industry about the minimum security measures that providers must take to ensure security and integrity of their networks.

The guidance was developed by adopting many of the other international standards listed here. It lists 25 high-level security objectives, grouped into 7 domains as set out below.

ENISA Reference #	ENISA Domain and Security Objective Descriptions
D1	Governance and risk management
SO 1	Information security policy
SO 2	Governance and risk management
SO 3	Security roles and responsibilities
SO 4	Security of third party assets
D2	**Human resources security**
SO 5	Background checks
SO 6	Security knowledge and training
SO 7	Personnel changes
SO 8	Handling violations
D3	**Security of system and facilities**
SO 9	Physical and environmental security
SO 10	Security of supplies
SO 11	Access control to network and information systems
SO 12	Integrity of network and information systems

[32] https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures

ENISA Reference #	ENISA Domain and Security Objective Descriptions
D4	**Operations management**
SO 13	Operational procedures
SO 14	Change management
SO 15	Asset management
D5	**Incident management**
SO 16	Incident management procedures
SO 17	Incident detection capability
SO 18	Incident report and communication
D6	**Business continuity management**
SO 19	Service continuity strategy and contingency plans
SO 20	Disaster recovery capabilities
D7	**Monitoring, auditing and testing**
SO 21	Monitoring and logging policies
SO 22	Exercise contingency plans
SO 23	Network and information systems testing
SO 24	Security assessments
SO 25	Compliance monitoring

Per security objective, it lists the security measures which could be taken to reach the security objective. The measures are grouped into 3 levels of increasing sophistication (basic, industry standard and state of the art). It lists the types of evidence which could be taken into account by a supervisor or an auditor when assessing if security measures are in place. The overall security objectives and security measures are depicted in the diagram below.

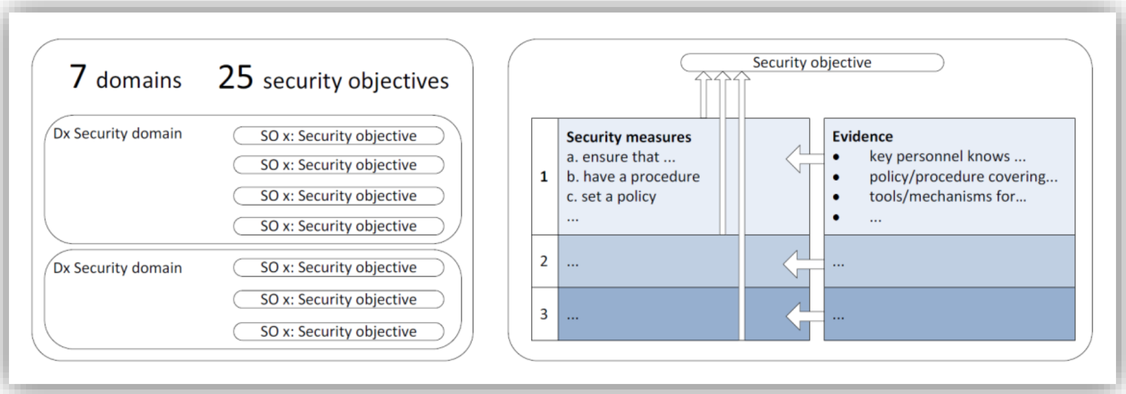


Figure 8 - ENISA – Technical Guideline on Security Measures Framework

Although this ENISA guidance is targeted at the Telecommunication industry, it can be applied to any ICT enabled organisation as it uses best practice from other Information Security frameworks. Currently there is no form of certification for complying with the ENISA guidance.

3. National Institute of Standards and Technology (NIST)

NIST [33] is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce.

Within the Computer Security Division at NIST, the Computer Security Resource Centre (CSRC) was established to publish[34] a set of standards, guidelines, recommendations and research on Information Security known as the NIST Special Publications (SP)[35]. The SP 800 subseries is a public available collection of 100+ guidelines, recommendations and reference materials.

The most well know publication from this series is the *NIST Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations*[36]. This is a catalogue of security controls (safeguards and countermeasures) prescribed as part of an ISMS.

NIST have also published 2 Information Security frameworks:

1. NIST Risk Management Framework – a mandatory framework for US Federal organisations within the scope of the FISMA Act. NIST SP 800-53 is now an element within this framework.
2. NIST Cybersecurity Framework – a voluntary framework developed by NIST in conjunction with the private sector to assist any organisation (not just federal) to better manage and reduce cybersecurity risk.

Currently no form of certification of compliance with either of NIST's Information Security frameworks is available.

4. NIST Risk Management Framework (RMF)

Following on from the publication of NIST SP 800-53, additional guidance was developed as part of the NIST FISMA Implementation Project. The NIST Risk Management Framework (RMF) was developed to provide a risk-based approach to the security controls as identified in NIST SP 800-53.

[33] https://www.nist.gov/

[34] Driven by the FISMA Act of 2002, NIST in 2003 initiated a FISMA Implementation Project to develop security standards and guidelines to support US government organisations with the implementation of and compliance with the Act.

[35] http://csrc.nist.gov/publications/PubsSPs.html

[36] SP 800-53 Rev.4 - April 2013 (Updated 22/01/2015) - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST *SP 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach* was published[37] in February 2010 to provide guidelines to a 6 step process necessary to implement the NIST RMF.

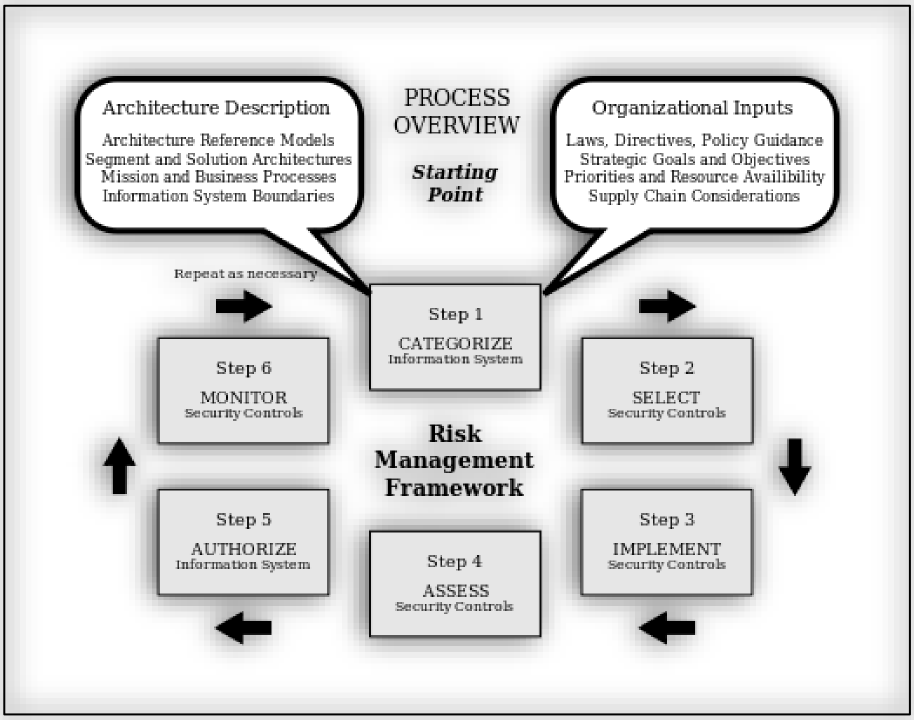

Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availibility
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
Risk Management Framework

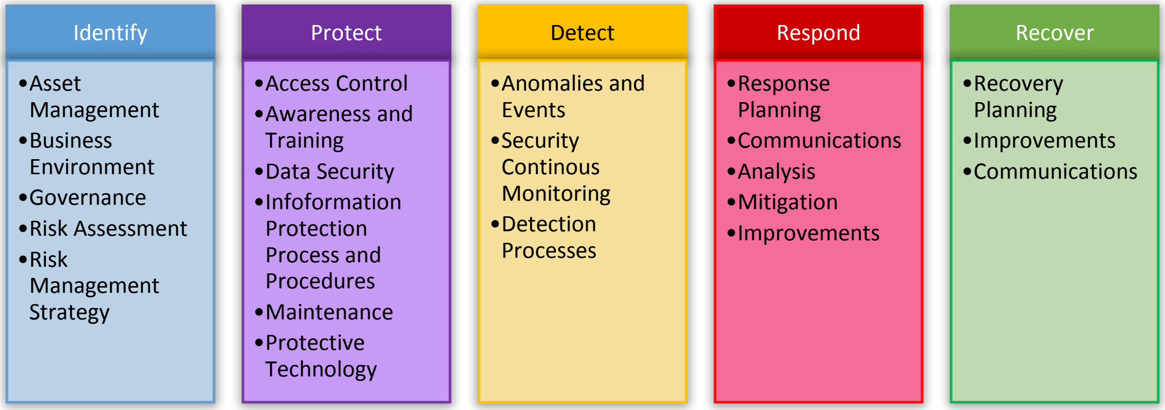
Figure 9 - NIST Risk Management Framework (RMF)

[37] SP 800-37 Rev.1 – February 2010 (Updated 05/06/3014) - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

5. NIST Cybersecurity Framework

While the NIST RMF was targeted at achieving compliance by US Federal Agencies with the FISMA Act of 2002, US federal government also wished to provide information security advice to a wider non-federal audience within the USA but is allowed to be used by any organisation who wishes to available of it.

In February 2013, initiatives at a federal level called on the NIST to develop a voluntary risk-based Cybersecurity Framework for the nation's critical infrastructure—that is, a set of industry standards and best practices to help organisations identify, assess, and manage cybersecurity risks. NIST issued the resulting framework[38] in February 2014.



Identify
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

Protect
- Access Control
- Awareness and Training
- Data Security
- Infoformation Protection Process and Procedures
- Maintenance
- Protective Technology

Detect
- Anomalies and Events
- Security Continous Monitoring
- Detection Processes

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communications

Figure 10 - NIST Cybersecurity Framework Overview

6. ISACA COBIT 5 for Information Security

COBIT 5[39] from ISACA[40] is an overall framework for the governance and management of enterprise IT. Part of the COBIT 5 framework is COBIT 5 for Information Security[41] (as seen in Figure 11). COBIT 5 for Information Security provides guidance to help IT and security professionals understand, utilize, implement and direct important information security-related activities, and make more informed decisions while maintaining awareness about emerging technologies and the accompanying threats. Its aim is to:

- Reduce complexity and increase cost-effectiveness
- Increase user satisfaction with information security arrangements and outcomes
- Improve integration of information security
- Inform risk decisions and risk awareness
- Reduce information security incidents

[38] https://www.nist.gov/cyberframework
[39] http://www.isaca.org/cobit/
[40] ISACA was previously known as the Information Systems Audit and Control Association but now goes by its acronym only. https://www.isaca.org
[41] http://www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx

- Enhance support for innovation and competitiveness

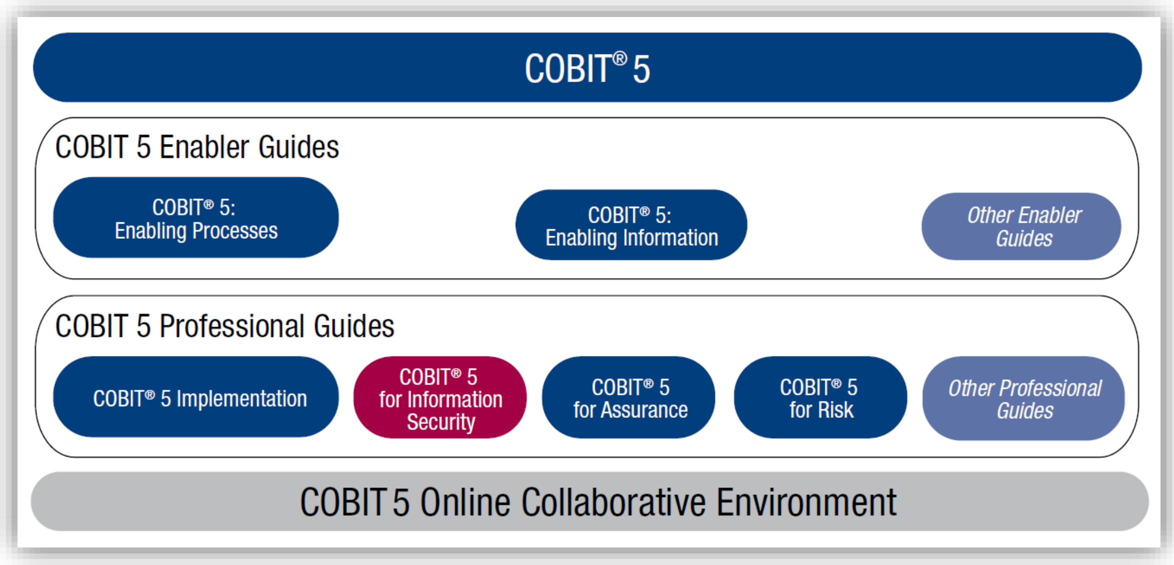

COBIT® 5
COBIT 5 Enabler Guides
COBIT® 5: Enabling Processes
COBIT® 5: Enabling Information
Other Enabler Guides
COBIT 5 Professional Guides
COBIT® 5 Implementation
COBIT® 5 for Information Security
COBIT® 5 for Assurance
COBIT® 5 for Risk
Other Professional Guides
COBIT 5 Online Collaborative Environment

Figure 11 - COBIT 5 Product Family

There is no method of organisational certification for COBIT 5 compliance, but your organisation's personnel can undergo COBIT 5 training[42] and independently assessed exams to demonstrate their knowledge. ISACA also provide various[43] well known[44] industry recognised professional certifications in IT audit, security, governance and risk.

[42] http://www.isaca.org/Education/COBIT-Education/Pages/COBIT-Training.aspx

[43] http://www.isaca.org/CERTIFICATION/Pages/default.aspx

[44] Certified Information Security Manager (CISM) - http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx

Appendix D - Sources of Information in Relation to Threats and Vulnerabilities

Government Bodies

Ireland

In Ireland, the National Cyber Security Centre (NCSC) acts as the State's national/governmental Computer Security Incident Response Team (CSIRT-IE).[45] The NCSC issues Cyber Security advisories via email. Check with the person in your organisation with the role of Chief Information Security Officer or similar to see if they are subscribed to these alerts.

European Union

At a central EU level, ENISA, the European Union Agency for Network and Information Security[46] is a centre of expertise for cyber security. It makes available many useful publications such as:

- ENISA (Annual) Threat Landscape (ETL) Report[47]: The ENISA Threat Landscape (ETL) provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends.
- ENISA Advisory Info Notes[48]: ENISA publishes regular articles in relation to the latest threats and vulnerabilities. Advisory notes on topics such as Locky Ransomware and Malvertising were made available in 2016.

enisa
ENISA
ETL 2017
ENISA Threat Landscape Report 2017
15 Top Cyber-Threats and Trends
FINAL VERSION
1.0
ETL 2017
JANUARY 2018

Figure 12 - ENISA Threat Landscape 2017 Report

USA

As discussed previously in relation to Information Security frameworks, the National Institute of Standards and Technology (NIST) publishes a set of standards, guidelines, recommendations and research on Information Security known as the NIST Special Publications[49]. The most well know publication from this series is the NIST Special Publication

[45] https://www.dccae.gov.ie/en-ie/communications/topics/Internet-Policy/cyber-security/national-cyber-security-centre/Pages/National-Cyber-Security-Centre.aspx

[46] https://www.enisa.europa.eu/

[47] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

[48] https://www.enisa.europa.eu/publications/info-notes

[49] https://csrc.nist.gov/publications/sp800

800-53 – Security and Privacy Controls for Federal Information Systems and Organizations. This is a catalogue of 200 individual security controls spread across 18 control families.

Table of 18 Security Control Families in NIST SP 800-53

ID	Family
AC	Access Control
AT	Awareness and Training
U	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
PM	Program Management
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity

In addition, the US-CERT – United States Computer Emergency Readiness Team[50] National Cyber Awareness System[51] publishes timely alerts and bulletins on current security issues and new vulnerabilities.

[50] https://www.us-cert.gov/

[51] https://www.us-cert.gov/ncas

Australia

The Australian Signals Directorate (ASD) as a Division of the Department of Defence, is an intelligence agency that provides Cyber and Information Security services to the Australian Government. It periodically publishes the Australia Government Information Security Manual (ISM)[52]. The ISM is composed of three documents targeting different levels within an organisations:

- ISM Executive Companion
- ISM Principles
- ISM Controls

Figure 13 - Australian Government 2017 ISM Controls

ASD also publishes various publications to assist in improving your information security posture:

- Strategies to Mitigate Cyber Security Incidents[53].
- Protect notices from the Australian Cyber Security Centre[54].

Other Useful Sources

Some private institutions and commercial organisations publish valuable and industry recognised advice in relation to information security controls. Some suggestions are set out below. These and/or other similar sources should be monitored for newer versions or updates.

[52] http://www.asd.gov.au/infosec/ism/index.htm
[53] http://www.asd.gov.au/infosec/mitigationstrategies.htm
[54] http://www.asd.gov.au/publications/index.htm

The Center for Internet Security (CIS) in collaboration with the SANS Institute periodically produces "The CIS Critical Security Controls for Effective Cyber Defence"[55]. The CIS Critical Security Controls are a set of controls that they deem are minimums to have an effective security posture.

Since 2008, Verizon has being publishing the Verizon Data Breach Investigations Report (DBIR)[56]. The DBIR report provides valuable information into the latest and common information security vulnerabilities from over 100,000 incidents with contributions from security service providers, law enforcement and government agencies. In addition it offers suitable security controls to mitigate against those vulnerabilities.

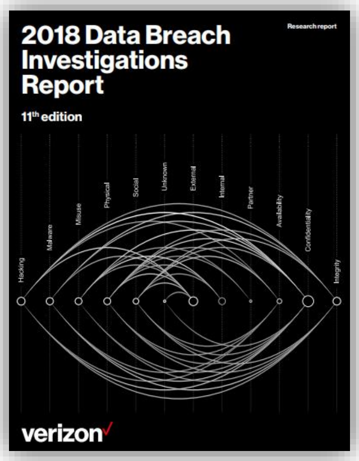


Figure 14 - Verizon 2018 DBIR Report

Software Development

As stated previously, Information Security should not be an afterthought, but ought to be embedded in the design, development and implementation phases of an ICT enabled project.

Therefore, it is important to be cognisant of the latest security techniques to avoid vulnerabilities in the development of new solutions.

For example, the Open Web Application Security Project (OWASP)[57] is an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. Its OWASP Top 10 Proactive Controls[58] are a list of security techniques they suggest should be included in every software development project. Also, due to the massive increased popularity of mobile applications, OWASP have also recently initiated an OWASP Mobile Security Project[59] to give developers and security teams the resources they need to build and maintain secure mobile applications.

Therefore, you are encouraged to include such security techniques as an integral part of the life-cycle development process of web-based applications.

Hardware and Software Vendors

Your own information assets are usually dependent on an underlying ICT Infrastructure composed of various products from various commercial vendors. Most vendors are now becoming more proactive and transparent in announcing vulnerabilities and solutions to their

[55] https://www.sans.org/critical-security-controls/
[56] http://www.verizonenterprise.com/verizon-insights-lab/dbir/
[57] https://www.owasp.org/index.php/Main_Page
[58] https://www.owasp.org/index.php/OWASP_Proactive_Controls
[59] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

products. Also, leading vendors of Information Security products usually have very proactive knowledge bases via blogs and social media feeds like Twitter.

For example:

- Microsoft issues notifications on Security Updates[60] and Advisories[61] for its various products and services.
- Cisco Security Center[62] provides Security Advisories to its range of network devices.
- Symantec Security Center[63] is an active source of general Information Security issues along with publications such as its annual Internet Security Threat Report[64].

Therefore it is recommended that your Information Security personnel and ICT system owners should consider subscribing to / monitoring bulletins and advisories from the various vendors of products within your own environment.

[60] https://portal.msrc.microsoft.com/en-us/security-guidance

[61] https://technet.microsoft.com/en-us/security/advisories

[62] https://tools.cisco.com/security/center/home.x

[63] https://www.symantec.com/security_response/

[64] https://www.symantec.com/security-center/threat-report