Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

002 – Risk Management v1.0

2021

Prepared by Department of the
Environment, Climate & Communications
gov.ie/decc

Table of Contents

1 Foreword

The Electronic Communications Security Measures (ECSMs) have been produced by the Electronic Communications Security Measures working group convened by the Irish National Cyber Security Centre (NCSC), which forms part of the Department of the Environment, Climate and Communications (DECC); and with the support of the Commission for Communications Regulation (ComReg). Industry participation in the WG has involved network operators, including the Mobile Network Operators (MNO) which have been awarded 5G licences, and selected fixed line operators.

This ECSM is part of a series of documents listed below:

Title	Subject
ECSM 001	General
ECSM 002	Risk Management
ECSM 003	Physical and Environmental Security
ECSM 004	Training, Awareness and Personnel Security
ECSM 005	Network Management & Access Control
ECSM 006	Signalling Plane Security
ECSM 007	Virtualisation Security
ECSM 008	Network, Monitoring and Incident Response
ECSM 009	Supply Chain Security
ECSM 010	Diversity, Resilience & Continuity
…	…

2 Introduction

Ireland's modern digitally connected society and economy is highly dependent on reliable and secure electronic communications networks and services (ECN and ECS respectively). They form the backbone of much of Ireland's critical national infrastructure providing connectivity to the essential services upon which citizens rely, such as healthcare providers, energy providers, financial institutions, emergency services and public administration. It is of paramount importance that these vital networks and services are protected from the full range of threats with an appropriate level of technical and organisation security measures.

The ECSM Working Group convened on the 08th 09th and 10th of September to discuss matters concerning Risk Management. The group heard from experts in the field of risk management and held focussed discussions on the risks, challenges and best practices associated with Risk Management as it pertains to electronic communications networks. ECSM 002 –Risk Management has been developed by the NCSC informed by those meetings..

3 Scope

The risk assessment principles set out in this ECSM are applicable to all undertakings providing public Electronic Communications Networks and Electronic Communications Services.

The legislative basis for the ECSMs is set out in ECSM 001- General

4 References

Document	Title
ENISA	Guideline on Threats and Assets, Technical guidance on threats and assets in Article 13a
ISO 27005	Information technology — Security techniques — Information security risk management
ISO 31000	Risk Management- Guidelines
ISO 60812	Failure Modes and Effects Analysis (FMEA)

NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-39	Managing Information Security Risk

5 Definitions, Symbols and Abbreviations

5.1 Definitions

Document	Title
Board	A group of individuals appointed to represent shareholders in the governance of an organisation.
Senior Management	A group of individuals responsible for making the management and executive decisions of an organisation.
Risk Appetite	The amount and type of risk that an organisation is prepared to take.
Risk Assessment	The process of identifying, estimating and prioritising risks.
Risk Management	The programme and supporting processes to manage risk.
Risk Rating	An assessment of risk based on the likelihood of an event occurring (from most unlikely to most likely) and the severity of the impact if the event does occur (from trivial impact to major impact).

5.2 Symbols

Nil

5.3 Abbreviations

Document	Title
ComReg	Commission for Communications Regulation

DECC	Department of the Environment, Climate and Communications
ECN	Electronic Communications Network
ENISA	European Union Agency for Cyber Security
ECSM	Electronic Communications Security Measure
MNO	Mobile Network Operator
NCSC	National Cyber Security Centre

37

38

6 Overview of Risk

Working Every year there are hundreds of million telecommunications user hours lost in the EU due to outages caused by network incidents, in 2020[1] there were 2798 million user hours lost in 171 major incidents. Electronic Communications Networks are subject to a wide range of risks and threats such as climate and severe weather events, physical attacks, cyberattacks, supply chain disruptions, power outages, hardware failures, failed software update processes, loss of skilled personnel, cable cuts, theft, vandalism, etc. Further information on these threats is available in ENISA's publication "Guideline on Threats and Assets"[2].

While some outages may be unavoidable, for example, those caused by severe climatic conditions, their impact can be greatly reduced, and other types of incidents can be entirely avoided, or their number greatly reduced by effective risk management processes being implemented by network operators.

Risk assessment is one of the fundamental components of risk management, a good risk assessment process ensures that all risks in scope are identified, rated, and prioritised. All identified risks are recorded and managed as part of the process; treatment of risk is guided by the operator's obligations and organisational risk appetite. An effective risk management process allows operators to approach their risks in a consistent and easily repeatable way, allowing the organisation to make informed decisions, and reduce the likelihood and impact of adverse events.

Many of the security measures set out in the subsequent ECSM series rely on operators having a comprehensive, coherent, and consistent risk management process. Thus, an effective risk management process is the cornerstone to a successful implementation of the security measures set out in this series of documents.

[1] https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

[2] Technical Guideline on Threats and Assets — ENISA (europa.eu)

7 Security Measures

The operator should implement the Risk Management Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
RA.01	Risk management shall be fully supported at Board level, support decision making and be an integral part of day-to-day operations. It shall be implemented uniformly and the level of governance and oversight shall be appropriate and proportionate to the priority of identified risks.
RA.02	Risk management shall be implemented according to best practice, aligned to internationally recognised standards and guidance, adapted to the needs of the organisation, with a clearly documented methodology that is communicated to all levels in the organisation.
RA.03	Board, senior management and key personnel shall develop and communicate a clear understanding of the organisation's risk appetite to relevant personnel, both to determine which objectives to pursue and to manage those objectives within the organisation's appetite for risk.
RA.04	Risks at operational level shall be identified, assessed, managed, and recorded in a standardised format and where necessary these risks should be escalated to Board or senior management as appropriate for a decision on risk treatment.
RA.05	Risk assessment(s) shall be carried out by a cross functional team relevant to the area being assessed, with diverse knowledge of the equipment, process, product, or service in order to base the work on the best possible information.
RA.06	Stakeholders shall be identified, and roles and responsibility shall be defined within the team carrying out the risk assessment.
RA.07	The scope of individual risk assessments within a risk management process shall be clearly defined.
RA.08	Risks arising from vulnerabilities in and threats to systems, processes or equipment within the scope of the risk assessment shall be identified.

RA.09	Risks shall be rated and scored using a consistent methodology based on the likelihood of a threat event occurring and its impact.
RA.10	Risk treatment plans (Accept, Avoid, Mitigate, Share, Transfer) shall be put in place and implemented.
RA.11	All risk management activity shall be communicated and reported upon effectively within the organisation to ensure that awareness of risk is brought to the attention of the appropriate personnel and management.
RA.12	Risk assessment shall be implemented on a regular basis but at least once a year to take into account the dynamic nature of risk.

68

69

8 Implementation Guidance

8.1 Risk Management Standards

There are a number of risk management standards available to operators that provide methodologies to assess and rate risks posed to the security and integrity of their networks including but not limited to those covered in this section. The underlying principles for all of these standards are largely the same, risks are identified, assessed, rated, treated, mitigated, and monitored. Risk Assessment is an ongoing process that requires frequent review and updating as operating conditions and demands on networks change and evolve.

The security measures set out in the ECSM series rely on operators having a comprehensive, coherent, and consistent risk management process. Thus, an effective risk management process is the cornerstone to a successful implementation of the security measures set out in this series of documents.

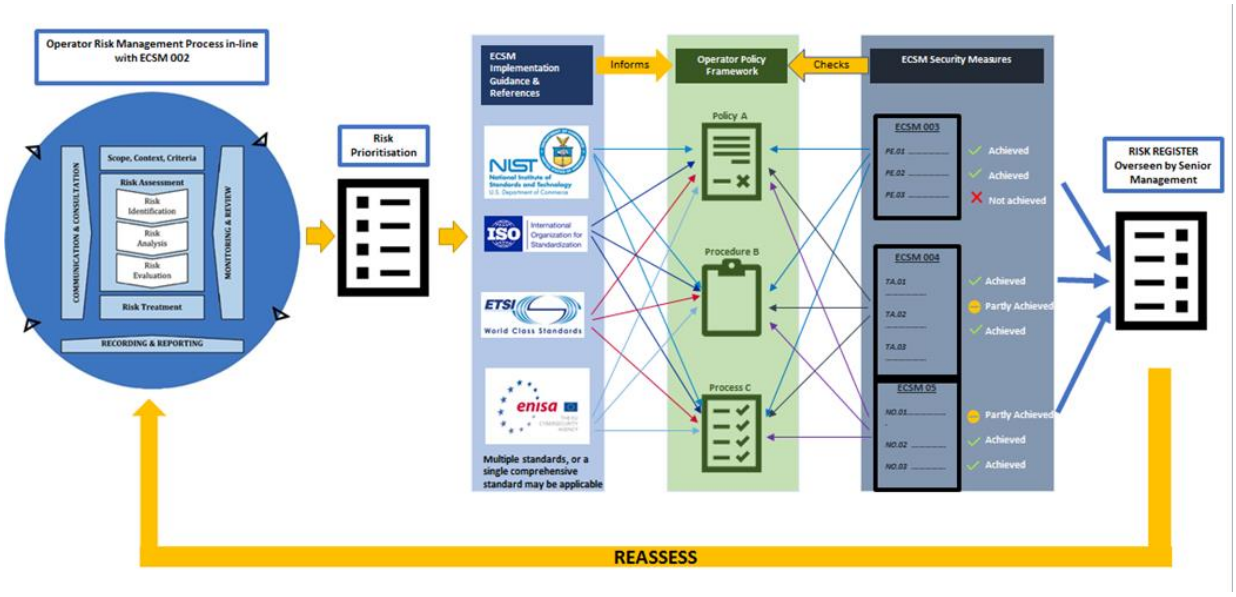


Figure 1 - The role of Risk Management in ECSM implementation

The following standards provide detailed guidance and may be used by operators in implementing the principles set out in section 7.

8.1.1 ISO 31000 Risk Management Principles and Guidelines

ISO - ISO 31000 — Risk management

A guide to the design, implementation, and maintenance of risk management. It provides principles and generic guidelines to assist organisations in establishing, implementing, operating, maintaining, and continually improving their risk management framework.

ISO 31000 § 4 outlines the principles that should be taken into consideration when setting up a risk management framework within an organisation. It states that risk management should be an integral part of an organisation and implemented at all levels within the organisation. It should be well structured, comprehensive, and applied in a manner proportionate to the organisation. The process should include all stakeholders transparently to get as wide as possible breath of knowledge and awareness of risk management. It needs to be dynamic and have the ability to adapt and improve as new risks emerge or lessons are learned from experience.

8.1.2 ISO 270xx Information Security Management Systems (Series of Documents)

ISO - ISO/IEC 27000 – International Standard for information security

This is a series of standards that provide requirements for establishing, implementing, maintaining, and continually improving an information security management system within an organisation.

ISO 27005 provides guidelines for information security risk management in an organisation. A summary of the main steps is given in this section; please refer to the document for the full text.

1. Establish the context of a risk management process (ISO 27005 § 7.1)

Specification of basic criteria, scope, boundaries, and the organisation of the information security risk management process.

2. Basic criteria to be considered (ISO 27005 §7.2)

Basic criteria include risk management approach, risk evaluation criteria, impact criteria and risk acceptance criteria.

3. Scope and boundaries (ISO 27005 §7.3)

The scope of the risk management process needs to be defined to ensure that all relevant assets are considered in the risk assessment. In addition, the boundaries need to be identified to address those risks that can arise through these boundaries.

4. Organisation for information security risk management. (ISO 27005 §7.4)

The organisation and responsibilities for the risk management process should be set up, maintained approved and supported by the appropriate level of management in an organisation.

5. Risk Identification (ISO 27005 §8.2)

Determine what can happen to cause a potential loss and gain an insight into how, where, and why loss can happen. Identify assets, threats, existing controls, and consequences of possible incident scenarios.

6. Risk Analysis (ISO 27005 §8.3, Annex B,)

Analyse and score the impact of possible incidents and their likelihood, considering the value of the assets involved.

7. Risk Evaluation (ISO 27005 §8.4, Annex E)

Evaluate and prioritise risk based on scoring from risk analysis and risk acceptance criteria (decided at point 2 above).

8. Risk Treatment (ISO 27005 §9, Annex F)

Select controls to reduce, retain, avoid, or share the risks based on the outcome if the risk assessment considering cost and benefit. Define a risk treatment plan, it may involve a combination of controls. The output of this step is a risk treatment plan with residual risks subject to acceptance by management.

9. Risk Acceptance (ISO 27005 §10)

It may be necessary to accept levels of residual risk that do not meet risk acceptance criteria for reasons such as cost of risk modification. The decision to accept risks and responsibilities should be made and formally recorded.

The output of this step is a list of accepted risks with justification for those that do not meet the organisation’s normal risk acceptance criteria.

10. Communication and Consultation (ISO 27005 §11)

Information about risk management should be shared with all stakeholders to support decision making within the organisation. It also increases awareness of risk and collects new risk information for ongoing risk assessment. The goal of this step is to achieve an ongoing understanding of an organisation’s risk management process and results.

11. Monitoring and review (ISO 27005 §12)

Risks (threats, vulnerabilities, likelihood, and consequences) can change abruptly without warning. Therefore, constant monitoring to detect these changes and regular review of the risk assessment is needed.

8.1.3 ISO 60812 Failure Mode and Effect Analysis

IEC 60812:2018 | IEC Webstore

The purpose of failure modes and effects analysis (FMEA) is to establish how items or processes might fail to perform their function so that any required treatments could be identified. This document is applicable to hardware, software, processes including human action, and their interfaces, in any combination. ISO 60812 explains how failure modes and effects analysis (FMEA) is planned, performed documented and maintained.

A summary of the main steps in the process is given in this section, please refer to the document for the full text.

1. Team performing the FMEA (ISO 60812 §4.2)

Assemble a cross-functional team of people with diverse knowledge about the process, product, or service.

2. Plan the FMEA (ISO 60812 §5.2)

a) Identify the scope, boundaries, and scenarios of the FMEA,

b) Define decision criteria for treatment of failure modes,

c) Define the format of the output documentation,

d) Identify the resources needed to perform the analysis.

3. Perform the FMEA (ISO 60812 §5.3, Annex B)

a) Sub divide items or processes into elements,

b) Identify functions and performance standards for each element,

c) Identify failure modes,

d) Identify detection methods and existing controls,

e) Identify local and final effects of failure modes,

f) Determine ratings for Severity (S) and Occurrence (O) for each failure mode root cause,

g) Determine effectiveness of existing control measures to detect failures before the customer is affected (D),

h) Evaluate relative importance of failure modes based on S, O and D

Criticality = S x O

Risk Priority number = S x O x D

4. Document the FMEA (ISO 60812 §5.4, Annex C, Annex F.)

The analysis should be reported as agreed in the planning stage

An example of and FMEA report content is given in Annex C and Annex F

8.1.4 NIST SP 800-39 Managing Information Security Risk

Managing Information Security Risk | NIST

NIST Special Publication 800-39 is the flagship document in the series of information security standards and guidelines developed by NIST in response to the US Federal Information Security Management Act (FISMA).

A summary of the main steps in the process is given in this section, please refer to the document for the full text.

- **Components of Risk Management (NIST SP 800-39 § 2.1)**

Risk management is a comprehensive process that requires organisations to:

(i) Frame risk (i.e., establish the context for risk-based decisions).

(ii) Assess risk.

(iii) Respond to risk once determined.

(iv) Monitor risk on an ongoing basis using effective organisational communications and a feedback loop for continuous improvement in the risk-related activities of organisations.

(v) Consider external risk relationships (e.g., partner organisations, suppliers, customers)

- **Multi-tiered Risk Management (NIST SP 800-39 § 2.2)**

To integrate the risk management process throughout the organisation, a three-tiered approach is employed that addresses risk at the:

(i) Organisation level.

(ii) Mission/business process level.

(iii) Information system level.

The risk management process is carried out seamlessly across these tiers with the overall objective of continuous improvement in the organisations risk management activities.

Figure 2 - NIST Tiered approach to risk assessment

- **Tier 1 Organisation View (NIST SP 800-39 § 2.3)**

Governance is the set of responsibilities and practices exercised by those responsible for an organisation. It provides oversight for the risk management activities and includes:

(i) The establishment and implementation of a risk executive (function).

(ii) The establishment of the organisation's risk management strategy including the determination of risk tolerance.

(iii) The development and execution of organisation-wide investment strategies for information resources and information security.

- ***Tier 2 Mission/Business process View (NIST SP 800-39 § 2.4)***

Tier 2 addresses risk from a mission/business process perspective by designing, developing, and implementing mission/business processes that support the missions/business functions defined at Tier 1.

(i) Identification and establishment of risk aware mission/business processes,

(ii) Enterprise Architecture, create a disciplined and structured approach for managing information technology assets,

(iii) Information security architecture is an integral part of an organisation's enterprise architecture.

- **Tier 3 Information Systems View (NIST SP 800-39 § 2.5)**

In addition to the risk management activities carried out at Tier 1 and Tier 2, risk management activities are also integrated into the system development life cycle of information systems at Tier 3.

The risk management activities at Tier 3 reflect the organisation's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual information systems supporting the mission/business functions of organisations. Risk management activities take place at every phase in the system development life cycle with the outputs at each phase influencing subsequent phases.

(i) Initiation phase

(ii) Development /acquisition phase

(iii) Implementation phase

(iv) Operations maintenance phase

(v) Disposal phase

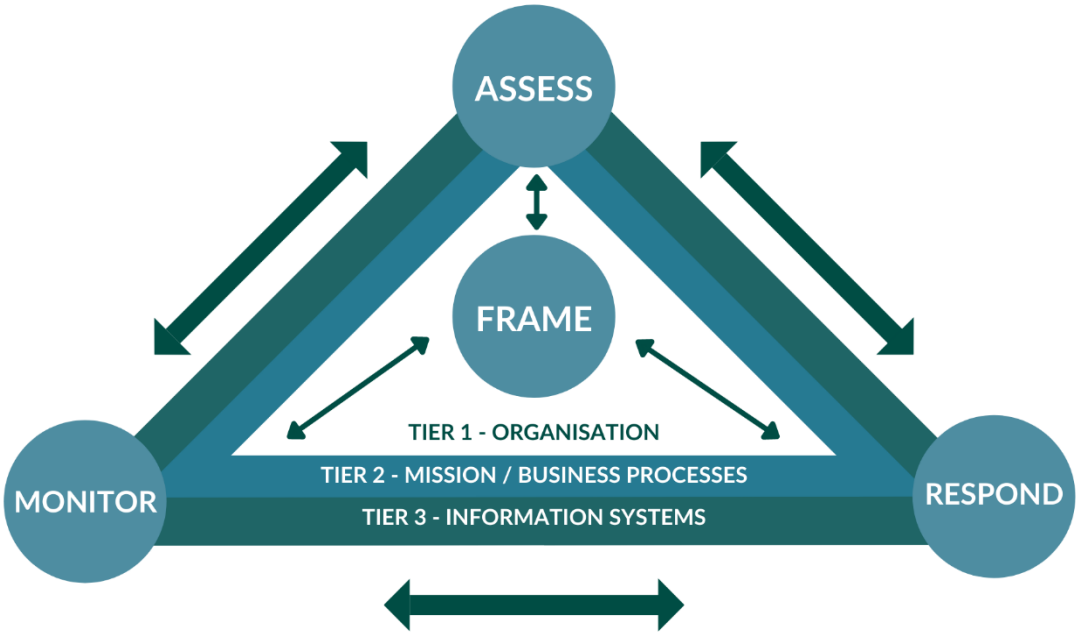
- ***Trust and Trustworthiness (NIST SP 800-39 § 2.6)***

Trust is an important concept related to risk management. How organisations approach trust influences their behaviours and their internal and external trust relationships.

(i) Establishing Trust among organisations

(ii) Trust worthiness of information systems

- **Organisational Culture (NIST SP 800-39 § 2.7)**



Organisational culture refers to the values, beliefs, and norms that influence the behaviours and actions of the senior leaders/executives and individual members of organisations.

There is a direct relationship between organisational culture and how organisations respond to uncertainties and the potential for near-term benefits to be the source for longer-term losses.

- **The Process**

The risk assessment process is given in chapter 3 of NIST SP 800-39 and is outlined below

Figure 3 - NIST Risk Assessment Process

- **Risk Framing**

1 Identify assumptions that affect how risk is assessed

2 Identify constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the organisation,

3 Identify the level of risk tolerance for the organisation

4 Identify priorities and trade-offs considered by the organisation in managing risk

- **Risk Assessment**

5 Identify threats to and vulnerabilities in organisational information systems and the environments in which the systems operate.

6 Determine the risk to organisational operations and assets, individuals, other organisations, and the Nation if identified threats exploit vulnerabilities using the likelihood and impact of an incident.

- **Responding to Risk**

7 Identify alternative courses of action to respond to risk determined during the risk assessment. (risk acceptance; risk avoidance; risk mitigation; risk sharing; risk transfer)

8 Evaluate alternative courses of action for responding to risk

9 Decide on the appropriate course of action for responding to risk

10 Implement the course of action selected to respond to risk

11 Develop a risk monitoring strategy for the organisation that includes the purpose, type, and frequency of the monitoring activities.

- **Risk Monitoring**

12 Monitor organisational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.

8.1.5 NIST SP 800-30 Guide for Conducting Risk Assessments

SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC (nist.gov)

This is a similar document to NIST SP 800-39, its purpose is to provide guidance for conducting risk assessments, amplifying the guidance in Special Publication 800-39.

Chapter 2 provides more detail on

- Key risk concepts such as threats, vulnerabilities, likelihood, and impact
- Approaches to assessment and analysis of risk
- Effects of organizational culture on risk assessments
- Application of tiered approach to risk assessment
- Risk communication and information sharing

Chapter 3 provides more detail on the risk assessment process as given in SP 800-39, this is supported by further information and guidance in appendices.

- Appendix D Threat sources
- Appendix E Threat events
- Appendix F Vulnerabilities and predisposing conditions
- Appendix G Likelihood of occurrence
- Appendix H Impact
- Appendix I Risk Determination
- Appendix J Informing Risk Response
- Appendix K Risk Assessment report templates
- Appendix L Summary of tasks.