An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)

June 2023

Prepared by the Department of
the Environment, Climate and Communications
gov.ie

Table of Contents

Section 1: Introduction 3

1.1. Objectives 3

1.2. Disclaimer 4

1.3. Scope 4

1.4. Methodology 4

1.5. Procurement Context 4

1.6 Acronyms and Abbreviations 6

Section 2: Guidelines on Cyber Security Specifications for Public Service Bodies 7

2.1 Source Stage 11

2.2 Manage Stage 13

Annex 1: Laws and Industry Standards per ICT Component 15

Annex 2: Threat Taxonomy 16

Annex 3: ICT Components and Categories 23

Annex 4: Cyber Security Requirements Overview 26

Annex 5: Worked Example of ICT Risk Management Methodology based on ISO/IEC 27005 30

Annex 6: Security Assessment Sheet 31

Annex 7: References 33

Annex 8: National/EU Public Procurement, Data Protection & Cyber Legislation 35

Annex 9: Relevant Industry Standards and Guidelines 37

Annex 10: Acknowledgements 38

Section 1: Introduction

Ireland's National Cyber Security Strategy 2019-2024 sets out key objectives to continuously develop and protect the State and its critical national infrastructure, as well as the general public. Among the key objectives are to:

- Continue to improve the ability of the State to respond and manage cyber security incidents including those with a national security component.
- Improve the resilience and security of public sector IT systems to better protect data and the services that our people rely upon.
- Raise awareness of the responsibilities of businesses around securing their networks, devices and information, and to drive research and development in cyber security in Ireland, including by facilitating investment in new technology.

In November 2022, the Department for the Environment, Climate, and Communication (DECC) and the National Cyber Security Centre (NCSC), published Revision1 of the Cyber Security Baseline Standards which set a minimum-security baseline standard and formed a broad framework of measures that are expected to be revised and improved in line with legislative proposals such as the NIS2 Directive[1] (A high common level of cybersecurity in the EU). The publication of the Baseline Standards was followed by the publication of a Cyber Security Baseline Standards Self-Assessment form which is a checklist that Public Service Bodies can use internally to assess their cyber security posture against the Cyber Security Baseline Standards. Security control assessments can be challenging, and this form provides a ready-made solution across the various operating environments and organisational frameworks of the Public Service.

Further to this, and recognising the need of Public Service Bodies (PSBs) for guidance in the context of cyber security specifications when procuring Information and Communications Technology (ICT) goods and services via public procurement processes from a range of suppliers, DECC and the NCSC engaged Grant Thornton Ireland to assist in developing the **"**Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)**"**.

1.1. Objectives

These guidelines aim to reinforce the Cyber Security Baseline Standards, the Network and Information Security (NIS) Directive, the NIS Directive revision (NIS2) and the EU Cyber Security Act Regulation[2]. The publication also considers ongoing EU legislative proposals including the Cyber Resilience Act, which aim to address market needs and protect consumers from insecure products by expanding cybersecurity rules to increase security on hardware and software products.

The recommendations aim to provide organisations with an improved understanding of the cyber security risks and challenges to be addressed when specifying their requirements for ICT goods and services, thereby helping raise the level of awareness in this area.

[1]https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

[2]Regulation (EU) 2019/881

1.2. Disclaimer

This document is designed to provide cyber security guidance and information as part of any Cyber Security technical specification process. It is not an interpretation of any legal provisions governing public procurement. Legal or other professional advice should be obtained if there is doubt about the interpretation of legal provisions or the correct application of such provisions. It should also be noted that the content of this document is subject to the evolution of national policy, EU, and Irish law including the revision of the Procurement Directives and case law of the European Court of Justice. For comprehensive guidance on the application of the public procurement rules in relation to the purchase of goods and services please see the National Public Procurement Policy Framework.

1.3. Scope

This document "Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)" applies to Ireland's Public Service Bodies (PSBs). It provides cyber security technical procurement guidance to the public sector in conjunction with NCSC specific public sector guidance[3].

The guidelines provide an easily understandable set of specifications that can be referenced by PSBs when they are planning the procurement of ICT goods and services. It addresses a range of cyber security domains including organisational practices, supply chain security (including risks such as data leaks, supply chain breaches, and malware attacks), evaluation considerations, and attestation information that may be required from suppliers when procuring ICT goods and services throughout the 'Plan, Source and Manage' phase of the procurement process.

1.4. Methodology

The methodology used included a series of interviews and workshops with key stakeholders (see Annex 10) from Government, PSBs, policymakers, regulators, ICT product suppliers, service providers, and procurement-focused cyber security professionals.

1.5. Procurement Context

Public procurement is governed by EU and National Rules. For more detailed information on the procurement framework and different aspects of procurement, please refer to the specific policy section of the Office of Government Procurement (OGP) website.

Refer to Annex 1: Laws and Industry Standards per ICT Component for the detailed mapping of applicable legislation and standards against ICT components/procurement type. The most relevant international standards and good practices which try to harmonise the minimum requirements for a safe design, manufacture and risk management are listed below. Annex 5 contains an ISO27005 information security risk management worked example as a suggested risk management approach. This includes a high-level risk matrix based on Likelihood/Impact to determine the Risk Rating in each stage of the cyber security specification process for the ICT components. Annex 8 contains a brief overview and description of the most relevant National/EU Public Procurement, Data Protection & Cyber Legislation.

[3]https://www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf

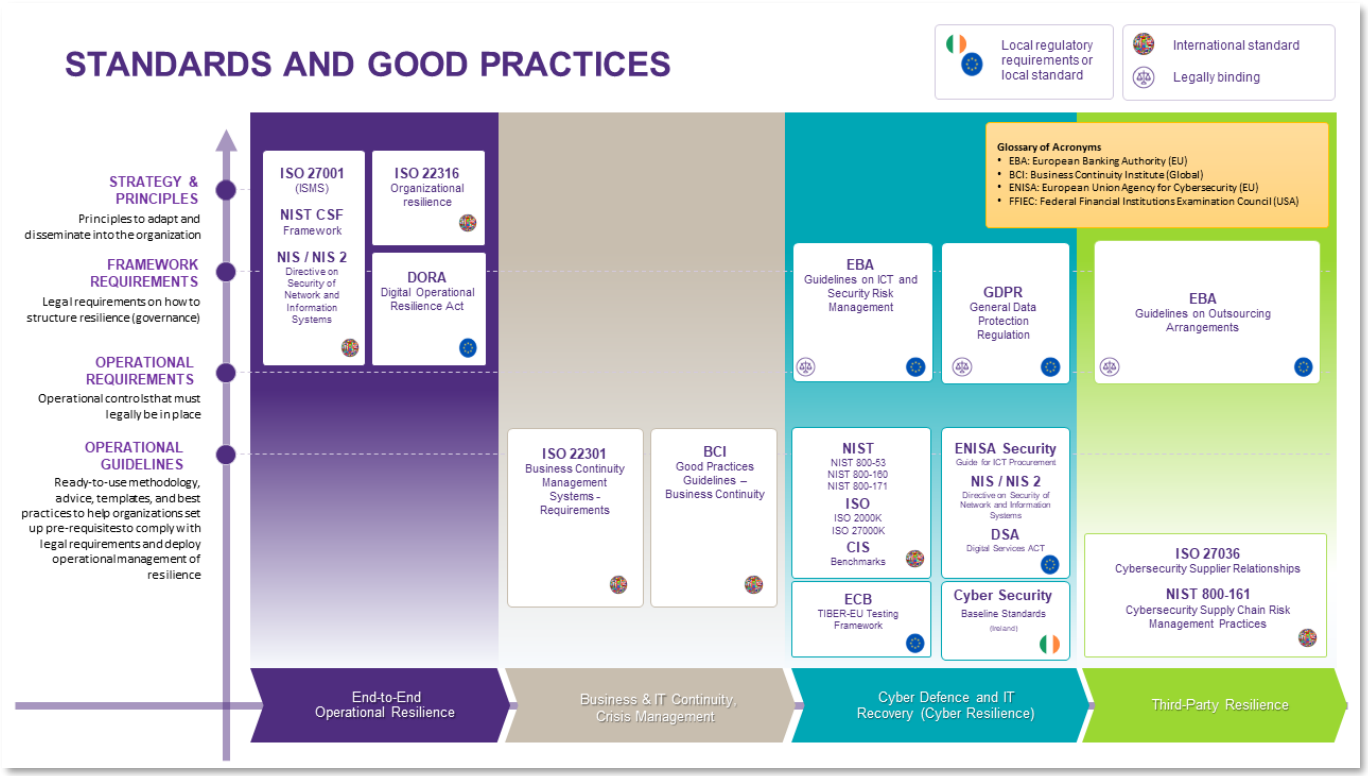


Illustration 1: Legislation, Standards and Good Practices for ICT goods and services

1.6 Acronyms and Abbreviations

The following are abbreviations and acronyms used across the document:

API	Application Programming Interface
AWS	Amazon Web Services
BISO	Business Information Security Officer
BOM	Bills of Materials
BYOD	Bring your Own Device
CCM	Cloud Controls Matrix
CIS	Center of Internet Security
CISO	Chief Information Security Officer
COTS	Commercial Off-the-Shelf software
CPU	Central Processing Unit
CSA	Cloud Security Alliance
CSF	Cyber Security Framework
CSIRT	Computer Security Incident Response Team
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
DECC	Department for the Environment, Climate, and Communication
DJEI	Department of Justice and Equality
DPIA	Data Protection Impact Assessment
ENISA	EU Agency for Cybersecurity
EULA	End User License Agreement
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
HSE	Health Service Executive
HTTP	Hyper Text Transfer Protocol
ICT	Information and Communications Technology
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
IaaS	Infrastructure as a Service
IoT	Internet of Things

KPI	Key Performance Indicators
LAN	Local Area Network
MITM	Man-in-the-Middle
MPS	Managed Print Services
NCSC	National Cyber Security Centre
NDA	Non-Disclosure Agreement
NISD	Network & Information Systems Directive
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturers
OES	Operators of Essential Services
OGCIO	Office of the Government Chief Information Officer
OGP	Office of the Government Procurement
OJEU	Official Journal of the EU
ORGCIO	Office of the Government Chief Information Officer
OS	Operating System
PSB	Public Service Body
PaaS	Platform as a Service
RAM	Random Access Memory
RAT	Remote Access Tool
ROM	Read Only Memory
SDL	Secure Development Lifecycle
SDLC	Software Development Life Cycle
SLA	Service Level Agreement
SMART	Specific, Measurable, Achievable, Realistic, Timely
SQL	Structured Query Language
SaaS	Software as a Service
TCP	Transmission Control Protocol
TED	Tenders Electronic Daily
WAN	Wide Area Network
XSS	Cross-Site Scripting

Section 2: Guidelines on Cyber Security Specifications for Public Service Bodies

This section outlines good practices[4] for maintaining and enhancing cyber security when acquiring ICT goods and services. These practices / guidelines are categorised per phase of the procurement lifecycle. In some cases, one practice may apply to two phases, in which case they are categorised under the phase where they should first be applied, or where they are most relevant.

The list of guidelines below is by no means exhaustive. However, it provides PSBs a foundation in ensuring cyber security is considered when procuring ICT goods and services. Annex 6 provides a security assessment list of all the relevant component guidelines.

2.1 Plan Stage Guidelines CG1

CG1. Establish Business, Technical, and Information Security Requirements

Description

When assessing the need for new ICT solutions, PSBs should involve IT, security, and data protection functions, and consult peers in procurement to ensure that various needs and regulatory implications are considered as part of the requirements definition.

Business Needs:

- Gather all business requirements including security requirements and obtain necessary approval / business sponsorship.
- Consider if there is an alternative and pre-existing solution that can provide the same level of benefit rather than acquiring a new or bespoke solution.
- As prerequisite to procurement, PSBs should conduct a business impact assessment (BIA) and data protection impact assessment (DPIA) to identify and assess the potential impact of the required solution or service. The result of the assessments may influence the requirements' definition, such that, PSBs may consider specifying enhanced features or specifications to ensure that risks are maintained at an acceptable level.
- Identify which threats are most relevant to your organisation. These threats should be considered when planning procurement of a new product or service. Annex 2 contains a comprehensive threat taxonomy which has been created to identify those threats in order to help PSBs choose defences most appropriate to defend such systems.
- Ensure that any vulnerabilities are considered before procuring new products or services.
- Establish a vulnerability management process to monitor and address vulnerabilities of ICT products and/or services. A breakdown of the ICT components and categories is listed in Annex 3.
- Where appropriate, the contract should include provisions for supplier responsibility in addressing vulnerabilities via software updates or timely patching.
- Identify the risk appetite of the business unit/purchaser, including any demands associated with compliance with regulatory requirements (GDPR, NIS or other).

ICT Procurement Stage

Applicable to:

- Managed service
- Professional services
- Direct / indirect hardware purchases
- Software development / customisation
- Commercial software / licenses
- Software escrow

4 NIST Special Publication NIST SP 800-161r1. Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations

- Identify any risks associated with sensitive data held by Government entities, including personal information, commercially sensitive data or national security sensitive data.
- Ensure the contract clearly defines who is responsible for managing each risk.

Technical Requirements:

- PSBs should establish how a required solution is expected to integrate within the existing network environment.
- Ensure that any risks to existing ICT networks infrastructure and environments arising from access to system by supplier is known and any risk is appropriately addressed.
- Ensure the new solution will not negatively impact the existing ICT infrastructure and services (e.g., storage space, bandwidth, licenses, network and communications security, as well as physical access).
- Ensure that the Public Service Body has appropriate resources available to support the new solution.

Information Security Requirements:

Establish Information Security policies that will be required of the supplier and their products and services. This should cover at a minimum:

- general security practices
- roles and responsibilities
- access management
- security awareness
- vulnerability management
- ICT device maintenance
- incident management and reporting obligations
- resilience requirements

Informative References

- **NIST CSF:** ID.BE (Business Environment), ID.GV-1, ID.GV-2, ID.GV-3, ID.RA-2, ID.RA-3, ID.RM (Risk Management Strategy), ID.SC-2
- **Irish Baseline Security Requirements:** 1.1 Corporate Responsibility,1.3 Identify/Manage ICT Security Risks

2.1 Plan Stage Guidelines CG2

CG2. Engage the market to determine current offering

Description

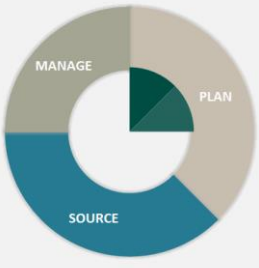
Preliminary market consultation may be necessary when acquiring new technology/potential solutions. This activity should be undertaken by the PSB as soon as needs have been established. Preliminary market consultation can provide insights about the capacity of the market to deliver on the specific cyber security requirements of the contracting authority and the risks involved.

The Public Procurement Guidelines for Goods and Services sets out information on procurement procedures and is available at (https://www.gov.ie/en/publication/c23f5-public-procurement-guidelines-for-goods-and-services/).

The Public Procurement Guidelines and the EU/Irish legislation sets out the scope and important measures to take to ensure that no bidder in the subsequent tender procedure has an unfair advantage or disadvantage based on the preliminary market consultation.

Consider the following:

ICT Procurement Stage



Applicable to:

- Managed service
- Professional services
- Direct / indirect hardware purchases
- Software development / customisation
- Commercial software / licenses

- ICT goods and service providers may deliver different solutions to meet the same business needs.
- Consideration towards managed, bundled services and functionalities which may be commercially/technically advantageous but can lead to more functions/functionality in the product than needed and may provide an additional cyber security attack vector risk.
- The purpose of preliminary market consultation is to obtain a clear picture of which solutions (products, works and services) are available.
- A Nondisclosure Agreement (NDA) is a contracting tool to ensure an organisation's non-public information and any non-public vendors information is being protected. NDAs allows PSBs to have confidence that data shared between the PSB and prospective vendors is appropriately protected. External experts should sign confidentiality and non-disclosure agreements and comply with any other security or confidentiality requirements of the contracting authority as appropriate. Normally, NDAs are signed at the tender stage however, in scenarios where sensitive information is involved in the tender, NDAs must be signed off in advance of sharing sensitive or confidential information.
- The most economically advantageous tender (MEAT) criterion enables the contracting authority to take account of criteria that reflect qualitative, technical and sustainable aspects of the tender submission as well as price when reaching an award decision.

- Software escrow

Informative References

- **NIST CSF:** ID-RM-3, ID.SC-2
- **Directive 2014/24/EU:** Article 40 and 41
- **Irish Baseline Security Requirements:** 1.1 Corporate Responsibility,1.3 Identify/Manage ICT Security Risks

2.1 Plan Stage Guidelines CG3

CG3. Translate Requirements into Technical Specifications

Description

At this stage, PSBs should pay careful attention when translating business, technical, and security requirements into tender specifications requirements & contractual provisions. Any Cyber Security technical obligations including reporting obligations must be stipulated in the contract as they may not apply retrospectively except in certain specific circumstances e.g. Voluntary reporting or an additional charge.
In particular:

- The scope of work and service level requirements should be specified. Where appropriate, seek market intelligence support utilising publications, and rating bodies, as necessary.
- Roles and responsibilities of the PSB, the supplier and other third parties in the delivery of the contract must be clearly defined.
- Technical Specifications for inclusion in the tender documents.
- Requirements that will be qualitatively assessed.
- Requirements that will be a specific contractual provision.
- Post-contract performance evaluation including monitoring and measurement of service levels should be defined.
- Post contract information on the suppliers own organisational cyber security posture, including any event or incident that may compromise this posture, should be defined as well as any remediation procedures. Exit Management and effective termination / expiry terms must be included in all contracts.
- Any technical specifications should include an update policy to address vulnerabilities via software updates or timely patching.

ICT Procurement Stage

Applicable to:

- Managed service
- Professional services
- Direct / indirect hardware purchases
- Software development / customisation
- Commercial software / licenses
- Software escrow

- **Any update procedure or involvement of third-party providers should be documented.**

Cyber security requirements should consider:

1. Prospective Supplier's internal information security policies that are applicable to the ICT goods and services under offer. The objective of this Supplier Security Policy is to ensure the protection of the PSBs' assets that are accessible by suppliers and to identify & minimise the risk from suppliers and vendors.
2. Goods and services maintenance, and management plan including lifetime vulnerability management and notification of addressable weaknesses (this should include hardware and software patches and updates). Understand and challenge any inconsistencies in the security policies.
3. Reporting and notification obligations of the supplier when they become aware of a security vulnerability, incident and/or data breach. Vulnerability management encompassing Coordinated Vulnerability Disclosure (CVD) and mandatory reporting obligations should be set out.
4. Research relevant suppliers and products. Where procurement of ICT products or services includes devices with features such as Wi-Fi, Bluetooth, file sharing, remote access, etc., ensure that commissioning and provisioning of devices includes disablement of non-essential services and secure by design and secure by default cybersecurity models.
5. Acquisition of ICT devices and solutions intended to provide essential services must be thoroughly tested to ensure they deliver what is expected: verify functionality, ease of use, stress test to determine the correctness of results under certain loads, and check for common security flaws (misconfiguration, retention of default credentials, weak passwords, or other known vulnerabilities). Testing policies and acceptable criteria/thresholds should be communicated to suppliers and should be part of the tender documentation.
6. Resilience requirements (business continuity / disaster recovery) for the new ICT goods or services should be defined for inclusion in the contract. PSBs should also update their internal resilience plans as a result of the new ICT acquisition.
7. Require, where permissible, access to logs and define data retention requirements.
8. Include, where permissible, the 'right to audit' clause in contracts and establish requirements to access security audit reports and/or further 3rd party attestation from suppliers.
9. Specify encryption and other protection measures required for certain data types and regulated devices. Encrypt data at rest on mobile devices, laptops and removable media. Consult the Data Protection Officer, as necessary.
10. Specify the cyber security certification requirements (i.e., EU certification scheme, if applicable, or equivalent) within the details to be provided by suppliers in response to tender requests.
11. When procuring cloud-based solution / services, PSBs should refer to OGP Cloud Guidance and OCGIO Cloud Computing Advice Note. Attention is specifically required on the collection, processing, and storage of data by cloud service providers.

Informative References

- **OGP Cloud Guidance**
- **OCGIO Cloud Computing Advice Note**
- **CSA Cloud Controls Matrix (CCM):** Audit & Assurance, Business Continuity Management and Operational Resilience, Data Security & Privacy Lifecycle, Infrastructure and Virtualisation Security, Logging and Monitoring, Threat and Vulnerability Management.
- **NIST CSF:** ID.BE-1, ID.BE-2, ID.BE-5, ID.GV-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4, ID.SC-5, ID.RA-1, ID.RA-2, PR.AC (Access Control), PR.DS (Data Security) PR.IP-2, PR.DS-7, PR.IP-3, PR.IP-6, PR.IP-7, PR.IP-9, PR.IP-10, PR.PT-1, PR.PT-

2, PR.AT-5, DE.DP-2, DE.CM-3, DE.CM-7, DE.CM-8, RS.RP (Response Planning), RS.CO-1, RS.CO-3, RS.AN-5, RC.IM (Improvements), RC.RP (Recovery Planning), RC.CO-2, RC.CO-3

- **Irish Baseline Security Requirements:** 1.1 Corporate Responsibility,1.3 Identify/Manage ICT Security Risks

2.1 Source Stage

2.2 Source Stage Guidelines CG4

CG4. Prepare Request for Proposals / Tender Documentation

Description

Now that all business, technical, and security requirements noted in CG3 have been identified, PSBs must ensure that these are formally included in the tender documentation.

The Cyber Security Requirements in Annex 4 provides some guidance on what evidence or documentation should be submitted by the suppliers. It is important to note that the documentation provided by the supplier should be used as evidence as either 1) validating a mandatory requirement (e.g. certification) or 2) to support the qualitative assessment of a requirement.

Consider the following:

1. PSBs should set the minimum-security requirements for the proposed ICT solution as well as the security expectations of the supplier.
2. Refer to the Irish Baseline Standards for the minimum-security requirements required of the PSB.
3. The minimum or better level should be required of the supplier if public services / ICT solutions are out-sourced to a third party.
4. The tender documentation should clearly stipulate the mandatory and supporting evidence required from suppliers to demonstrate their compliance or adherence to the PSB's requirements.

ICT Procurement Stage

Applicable to:

- Managed service
- Professional services
- Direct / indirect hardware purchases
- Software development / customisation
- Commercial software / licenses
- Software escrow

Informative References

- **Directive 2014/24/EU:** Article 40 and 41
- **NIST CSF:** ID.AM-6, ID.BE-1, ID.GV-2, ID-GV-3
- **Irish Baseline Security Requirements:** 1.1 Corporate Responsibility,1.3 Identify/Manage ICT Security Risks, 1.6.2 (All Third-Parties must be made aware of the organisation's cyber security obligations)

2.2 Source Stage Guidelines CG5

CG5. Evaluate Proposals and Tender Responses

Description

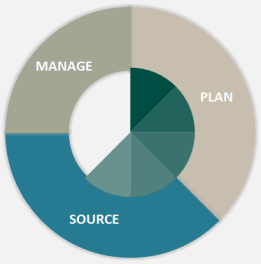
It is important at this stage to ensure the evaluation team has the required specialist knowledge to effectively evaluate the cyber security requirements in the supplier submission.

The cyber security requirements in Annex 4 provides guidance on the documentation expected from the suppliers for each cyber security requirements. It is important to note that the documentation provided by the supplier should be used as evidence as either 1) validating a mandatory requirement e.g. certification or 2) to support the qualitative assessment of a requirement.

Consider the following:

1. When evaluating certifications, it is important to understand the scope of the certification and the scope of the service to be contracted. A provider of cloud services might be ISO 27001 certified on some parts of the service (customer support service) but not in other services which may be of higher importance to the PSB.
2. It should also be noted that any supplier using a third-party service which has a certification in place does not confer any certification rights on the supplier providing the service. Each supplier has to have its own accredited certification in place.
3. Evaluate supplier responses against each requirement.
4. All cyber security regulatory requirements must be met.
5. Cyber security requirements must be set out clearly in the tender documentation and evaluation confined to the tenderer's response to each of the cyber security requirements.
6. Validate supplier claims for third party certification / assurance.

ICT Procurement Stage



Applicable to:

- Managed service
- Professional services
- Direct / indirect hardware purchases
- Software development / customisation
- Commercial software / licenses
- Software escrow

Informative References

- **Directive 2014/24/EU:** Article 40 and 41
- **NIST CSF:** ID.RA (Risk Assessment), ID.SC-1, ID.SC-2
- **Irish Baseline Security Requirements:** 1.3 Identify/Manage ICT Security Risks

2.2 Source Stage Guidelines CG6

CG6. Award Contract

Description

The Public Procurement guidelines for Goods and Services provides guidance on the procedures to be followed in the award of contracts.

- Service level agreements (SLAs) and Key performance indicators are set out by the contracting authority in the SLA which is set out as a schedule in the contract.
- Any legally binding cyber security requirements at contract award stage must be upheld through the life of the contract and include provisions for any identified deviation, where not corrected within a defined timeframe, that may lead to contract termination and legal remedy.

ICT Procurement Stage

Applicable to:

- Managed service
- Professional services
- Direct / indirect hardware purchases
- Software development / customisation
- Commercial software / licenses
- Software escrow

Informative References

- **Directive 2014/24/EU:** Article 40 and 41
- **NIST CSF:** ID.SC-3
- **Irish Baseline Security Requirements:** 1.1 Corporate Responsibility,1.3 Identify/Manage ICT Security Risks, 1.6.2 (All Third-Parties must be made aware of the organisation's cyber security obligations), 1.6.3 (Dependencies on Third-Parties are recognised and recorded), 1.6.4 (There is a clear and documented shared responsibility model between the organisation and suppliers/service providers)

2.2 Manage Stage

2.3 Manage Stage Guidelines CG7

CG7. Assess supplier risk and performance regularly

Description

Management and performance management provisions must be stated within the contract provisions in order to allow for effective performance management. As provided for in the contract, PSBs should review supplier performance on a regular basis after awarding the contract. This includes direct hardware purchases with maintenance agreements and other contracts with defined service level agreements.

For as long as the supplier has direct or indirect access to the PSBs ICT systems, services, and information, the supplier should be required to provide regular reports on how they are performing against the SLA as well as the previously defined security metrics, including:

- Security incidents and near misses during the period (i.e., monthly/quarterly);
- Trend of security attacks detected over time (e.g., DDoS attacks, email attacks, virus/malware, phishing incidents, etc.).

The PSB may add more metrics, as appropriate, depending on the procurement type.

- The risk posed by outsourcing services or acquiring ICT products from a third-party in the delivery of the contract should be assessed by the PSB on a regular basis (i.e., at least annually) depending on the risk profile of the third party. Suppliers with access to the PSBs sensitive information, or those who provide critical services to the PSB should be assessed on a more frequent basis commensurate with the assessed risk.
- A periodic risk assessment should be carried out to ensure that the supplier is managing information security risks related to the services / products they provide to the PSB. There are various ways that this objective can be met, including:
- The PSB should assess the adherence of the supplier's control environment against the Public Sector Cyber Security Baseline Standards or equivalent standards or certification (e.g., ISO 27002, NIST CSF, etc.).
- Information systems should be thoroughly tested to guarantee they deliver what is promised in the contract.
- The supplier should include testing scenarios for the services/devices/ systems offered. In addition, they should explain how testing should take place and how it will be coordinated. Ideally, benchmarks should be defined for testing purposes.
- The supplier may, at their own expense, secure an independent 3rd party certification or services to attest their continuous adherence with the aforementioned standards.

ICT Procurement Stage

Applicable to:

- Managed service
- Professional services
- Direct / indirect hardware purchases
- Software development / customisation
- Commercial software / licenses
- Software escrow

Informative References

- **Directive 2014/24/EU:** Article 40 and 41

- **NIST CSF:** ID.GV-3, ID.GV-4, ID.SC-4, ID-SC-5
- **Irish Baseline Security Requirements:** 1.1 Corporate Responsibility,1.3 Identify/Manage ICT Security Risks

2.3 Manage Stage Guidelines CG8

CG8. Review contract compliance and conduct exit management procedures

Description

In addition to performance checks and security risk assessments in CG7, the PSB should also review their supplier's compliance to contractual requirements at regular intervals. These must be stated in the contract. Contractual provisions in relation to remedies should be clearly set out in the contract or as part of the service level agreements. Any access/information/reporting requirements on the supplier to undertake this review should be set out in the contract.

This review is aimed at understanding whether the supplier has delivered the products / services as expected by the PSB. This should also allow the PSB to identify opportunities for improvement if re-tendering for the same products / service in the future.

Similarly, suppliers that meet original qualifying / evaluation criteria for contract award are expected to maintain or improve throughout the contract duration which should be provided for in the contract. Any lowering of standards during contracted terms requires remediation by the supplier.

As the contract with supplier reaches its end of the contracted term, it is important that PSBs are aware of the security implications and data protection obligations in relation to the data held or accessed by the supplier. In both cases below, the PSB should ensure that all data and intellectual property owned by the PSB which may have been stored by the incumbent supplier is made available to the PSB and thereafter destroyed by the outgoing supplier. The contract must specify all requirements for exit and transition.

In case of termination and as stated in the contractual requirements:

- The PSB should ensure that access by the supplier and their staff members to PSB resources are revoked accordingly.
- For data retention purposes, personally identifiable information of the supplier's staff must be anonymised if required for data retention or legally permissible purposes.

In case of change in the supplier:

- The PSB should ensure that appropriate arrangements with the incumbent supplier are in place to ensure portability and interoperability of data when moving from one supplier to another, or from one system to another.

ICT Procurement Stage

Applicable to:

- Managed service
- Professional services
- Direct / indirect hardware purchases
- Software development / customisation
- Commercial software / licenses
- Software escrow

Informative References

- **Directive 2014/24/EU:** Article 40 and 41
- **NIST CSF:** ID.GV-3, ID.GV-4, ID.SC-4
- **Irish Baseline Security Requirements:** 1.1 Corporate Responsibility,1.3 Identify/Manage ICT Security Risks, 1.6.2 (All Third-Parties must be made aware of the organisation's cyber security obligations), 1.6.3 (Dependencies on Third-Parties are recognised and recorded), 1.6.4 (There is a clear and documented shared responsibility model between the organisation and suppliers/service providers)

Annex 1: Laws and Industry Standards per ICT Component

#	Standards/Regulations	Industry (Core)	Hardware (laptops, network devices, etc.)	Software (applications, software licences, etc.)	Data & Data Warehousing (hosting, supply and management of data)	Telecommunications (internet, telephone, etc.)	Cloud Computing (all types of cloud services)	ICT Services (professional services)	Type	Description
1	ISO 20000 Series	All	☑	☑	☑	☑	☑	☑	Standard	Information technology — Service management — Service management system requirements
2	ISO 27001:22 (ISMS)	All	☑	☑	☑	☑	☑	☑	Standard	Information technology — Security techniques — Information security management systems — Requirements
3	ISO 27002	All	☑	☑	☑	☑	☑	☑	Standard	Information security, cybersecurity and privacy protection — Information security controls
4	ISO 27017	All					☑		Standard	Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
5	ISO 27018	All			☑		☑		Standard	Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
6	ISO 27036	All					☑	☑	Standard	Information technology — Security techniques — Information security for supplier relationships (four parts)
7	ISO 27070	All					☑		Standard	Information technology — Security techniques — Requirements for establishing virtualized roots of trust
8	ISO 27071	All	☑			☑	☑	☑	Standard	Information technology — Security techniques — Security recommendations for establishing trusted connections between devices and services
9	ISO 27011	All				☑			Standard	Information technology -- Security techniques -- Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations
10	ISO 27701	All	☑	☑	☑	☑	☑	☑	Standard	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
11	ISO 22301	All	☑	☑	☑	☑	☑	☑	Standard	Security and resilience — Business continuity management systems — Requirements
12	ISO 15288	All		☑					Standard	Systems and software engineering — System life cycle processes
13	ISA 62443	All	☑	☑	☑	☑		☑	Standard	Cyber Security Standards - Security of Industrial Automation and Control Systems
14	NIST Cyber Security Framework (CSF)	All	☑	☑	☑	☑	☑	☑	Standard	Cybersecurity Framework Version 1.1
15	NIST SP 800-53	All	☑	☑	☑	☑		☑	Standard	Security and Privacy Controls for Information Systems and Organizations
16	NIST SP 800-122	All			☑				Standard	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
17	NIST SP 800-160	All		☑					Standard	Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
18	NIST SP 800-161	All						☑	Standard	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
19	NIST SP 800-171	All	☑	☑	☑	☑		☑	Standard	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
20	CIS Benchmarks	All	☑	☑	☑	☑	☑		Standard	Center of Internet Security (CIS) Benchmarks - Critical Security Controls (SANS TOP20)
21	GDPR	All	☑	☑	☑	☑	☑	☑	Regulation	General Data Protection Regulation
22	EU Cybersecurity Act	EU	☑	☑	☑	☑	☑		Regulation	EU Cybersecurity Act
23	Radio Equipment Directive	EU	☑	☑	☑	☑	☑		Regulation	Radio Equipment Directive Delegated Regulation on Cybersecurity
24	Regulation on electronic identification and Trust Services (eIDAS)	EU	☑	☑	☑	☑	☑		Regulation	Regulation on electronic identification and Trust Services (eIDAS) 910/2014
25	Law Enforcement Directive	Ireland			☑	☑			Regulation	Data Protection Act 2018
26	Data Protection Acts 1988 and 2003	Ireland			☑	☑			Regulation	Data Protection Act 1988
27	Digital Service Act (DSA)	EU	☑	☑	☑	☑	☑	☑	Regulation	
28	ePrivacy Regulations	Ireland			☑	☑			Regulation	S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011
29	NCSC UK Cyber Essentials	UK	☑	☑	☑	☑			Standard	National Cyber Security Centre (NCSC) UK Cyber Essentials
30	DORA	UE	☑	☑	☑	☑			Regulation	Digital Operational Resilience Act
31	NIS / NIS 2	UE	☑	☑	☑	☑	☑		Regulation	Directive on Security of Network and Information Systems
32	Irish Cyber Security Baseline Standards	Ireland	☑	☑	☑	☑	☑	☑	Standard	Irish Cyber Security Baseline Standards
33	ENISA Security Guide for ICT Procurement	UE	☑	☑	☑	☑	☑	☑	Standard	European Nework and Information Security Agency (ENISA)
34	NSAI	Ireland	☑	☑	☑	☑	☑	☑	Standard	National Standards Authority of Ireland
35	COBIT	All	☑	☑		☑		☑	Standard	Control Objectives for Information and Related Technologies
36	PCI DSS	All	☑	☑	☑	☑	☑		Standard	Payment Card Industry Data Security Standard
37	BCI Good Practices	All	☑	☑	☑	☑	☑	☑	Standard	Business Continuity Institute Good Practices

Annex 2: Threat Taxonomy

Natural Phenomena

Threat Type	Description
Natural phenomena	Natural phenomena threats are rare but can damage the infrastructure and overall equipment (devices, network components, data centres, etc.) when they happen. In Ireland, emergencies related to severe weather events (storm, snow, ice, and flooding) dominate the natural risk classification[5]. Ireland's geographic position means it is less vulnerable to large-scale natural disasters such as earthquakes, tsunamis and on-island volcanoes.

Supply Chain Failure

Threat Type	Description
Cloud Services provider failure	There are four main reasons why the public sector is moving to the cloud[6]: • Putting the citizen at the centre; • Using data as an asset; • Enabling the public sector workforce; • Providing better services for everyone. Nearly all personal ICT devices work in the cloud or access data from cloud bases sources. Certain applications used by PSBs and the related services are also best delivered using cloud platforms as they offer better reach than traditional on premise services. These services, if not adequately considered for resilience and off-line accessibility, may cause severe disruptions in the provision of day-to-day services to the public. The OGCIO's Cloud Computing Advice Note[7] was issued in line with the Public Service ICT Strategy in 2019 and can be used as reference by PSBs when deciding cloud migration.

[5] https://www.gov.ie/en/press-release/5e685-national-risk-assessment-for-ireland-2020/
[6] https://www.forbes.com/sites/sap/2021/09/17/4-reasons-public-sector-organizations-are-moving-rapidly-to-the-cloud/
[7] https://www.gov.ie/en/publication/078d54-cloud-computing-advice-note-october-2019/

Network and Telecoms provider failure	Both the network and telecoms provider failure can have devastating effects. Most of the main PSB's form a hub between the main building and its associated sites, redundancy and topology design are crucial when mitigating this type of threat. PSBs should consider network segmentation when designing their network.
Power supply failure	Loss of electricity can be of life-impacting importance depending of the equipment affected. Servers and operational technology, signal networks, and human life systems must be protected by uninterruptible power sources.
Legacy equipment (Devices at end-of-life / end of extended vendor support)	All ICT devices, software, firmware, and other components have a definitive lifecycle, and include levels of vendor support during the lifecycle. It is important for PSBs to understand the lifecycle of each system component when going through ICT procurement as these may incur significant cost, particularly if there are system dependencies. Outdated or legacy systems are prone to vulnerabilities that will not be fixed by their manufacturers/developers and thereby expose significant risk.

Human Error

Threat Type	Description
System configuration error	Configuration errors continues to be a dominant trend and is responsible for 13%[8] of breaches. The rise of the Misconfiguration error began in 2018[9]. Overlooked misconfigurations can open a door for attackers to drop malware or exfiltrate data leading to extortion risks. The following top five configuration mistakes should be avoided to reduce the threat exposure: • Default credentials. • Password re-use. • Exposed Remote Desktop Services. • Default Ports. • Delayed Software patching.
Absence of audit logs	Audit logs maintain a record of activity by system and application processes, and by user activity within or upon systems and applications. Audit logs can assist in detecting security violations, including attempts to exceed access authority, performance problems, and flaws.

[8] https://bankingjournal.aba.com/2022/05/verizon-report-cyber-incidents-breaches-driven-by-external-actors/
[9] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

	PSBs and their suppliers should have appropriate levels of logging information. These logs should be retained for an appropriate period to assist with the detection of a cyber security attack. Most, if not all, network connected devices contain critical logs that can be vital in detecting anomalies, attacks, and loss of information. Retaining detailed audit logs helps companies monitor data and keep track of potential security breaches or internal misuses of privileges with regard to access and use of sensitive or confidential information. Keeping audit logs secure, and within the data retention policies as established, is an important task. PSBs should also ensure that logs are reviewed periodically and regularly check for unusual activities.
Unauthorised access control / lack of processes	Unauthorized access continues to be a problem for organisations around the world. Lack of process and monitoring can lead to unauthorised individuals or processes gaining logical or physical access to a network, system, application, data, or other resource. Unauthorised access via default, shared, or stolen credentials constituted more than a third of the entire hacking category and over half of all compromised records[10]. Access control procedures should be in place due to the variety of roles in PSBs. Attempts to circumvent these controls are very common, as is human nature (including all types of access control from buildings to systems and accounts). This poses significant risks to the PSBs interconnected environment. PSBs should pay particular attention to remote access and accounts with privileged access. These should both be managed using multi-factor authentication.
Non-compliance (BYOD)	Employees want the freedom to work from any location using any device. Working hours have evolved and employees conduct business activities during non-traditional business hours. These individuals are increasingly using their personal devices to undertake work tasks. From a business perspective, enabling bring-your-own-device (BYOD) is an advantageous strategy. However, BYOD can also represent a significant risk for organisations. For IT departments, there is a challenge to securely enable BYOD. Failure to do so can lead to malware outbreaks, non-compliance with regulatory requirements, and corporate exposure in the wake of personal device theft.

Malicious actions

Threat Type	Description
Malware: • **Virus** • **Ransomware** • **Adware** • **Remote Access Tool (RAT)**	Ransomware is perhaps the most known threat for PSBs, due mainly to the service interruption caused to the Health Service Executive (HSE) in 2021. These highly targeted attacks against PSBs are due mainly to two factors: (i) software infrastructure used by PSBs may be difficult to keep up-to-date at a pace that matches the time it takes a threat actor to weaponise a weakness. Public facing services and high-availability solutions require downtime and maintenance windows suitable for update testing prior to deployment as each new update may affect the functionality of a service; (ii) machines running legacy software that only works on a specific legacy operating system or driver version can be an easy target for these attacks.

[10] https://www.routledge.com/Routledge-Handbook-of-International-Criminology/Smith-Zhang-Barberet/p/book/9781138380424

	Some PSB IT systems are interconnected (e.g., HSE and the Department of Health) and difficult to isolate without generating service disruption, creating a comfortable ecosystem for malware. PSBs should implement mitigating controls, including but not limited to, multi-factor authentication, logging and monitoring logs, IP white-listing, etc. Adware is one of the easiest ways to distribute malware and more often ignored by individual users. In addition, organisations with large number of devices may have difficulties updating their licenses because of the elevated costs. Remote access tools (RATs) are commonly delivered as a Trojan within a user-requested downloaded tool, or malware-laden document. RATs provide a mechanism for threat actors to connect to the device upon which the RAT has been inadvertently installed.
Cryptojacking	Crypto-jacking or hidden crypto-mining is a type of cybercrime where a criminal secretly uses victims' devices to use their central processing unit (CPU) and/or the victims' graphics processing unit (GPU) and available internet bandwidth to mine cryptocurrencies without their permission, often through legitimate websites. The Department of Justice and Equality (DJEI) has listed crypto-jacking as one of the emerging threats that will continue to grow due to the potential profitability and pervasiveness[11].
Social engineering: • **Phishing** • **Baiting** • **Vishing** • **Smishing** • **Whaling**	Three of the most common delivery modes of social engineering tactics[12] are through: • Online and mobile phone. • Human interaction. • Passive attacks. Compromised email (phishing, baiting, spam and spear-phishing) is still the most dominating attack vector for malware infections. PSBs allow access to the internet and may further allow access to private web mail accounts via PSB devices. Such access poses risks of allowing malware and mobile codes access to the local devices from which it is accessed if no sufficient security filters (web filters, firewall, and anti-virus) are in place. PSBs are particularly at risk as their email addresses are easy to collect through public directories and passive reconnaissance activity. Spear-phishing is a targeted attack against particular individuals, contrasted against phishing which is a general attack aimed at no particular target. Both differ from whaling which is a dedicated spear-phishing attack against a senior high-profile or board-level executive, commonly designed to cause a second action by interaction with the message such as transfer of funds, or used as a basis of extortion of that individual.

[11] https://assets.gov.ie/122884/90fde3ae-6161-4d64-8064-4bf33fea0135.pdf
[12] https://www.proofpoint.com/us/corporate-blog/post/three-types-social-engineering-attacks-know

	There has also been increased SMS and phone-based scams during the COVID pandemic. Perpetrators pretending to be calling from various PSBs (HSE, Revenue, etc.) in an attempt to persuade individuals to either transfer money or collect sensitive information. An Garda Síochána issued a number of public warnings[13] to inform of the increasing activities in this area. The fight against phishing/smishing/whaling is not easy. Raising an adequate user awareness is a challenge. Many personnel have limited technical knowledge if any at all, making them easy targets for phishing attacks. Carefully crafted communications may seem realistic and cause even trained persons to be tricked into clicking links, opening attachments, or otherwise interacting with the message. Given the difficulty in protecting users from these attacks it is important for PSBs to have strong compensating controls, such as, but not limited to: • An up-to-date advanced malware and antivirus solution. • Regular patching of vulnerabilities. • Log recording and monitoring. • Enabling multi-factor authentication. • Regular access restriction/rights review. • Only give access to what is needed to perform the role. • Only install applications and services that are needed to carry out the function.
Theft: • **Device** • **Data**	Theft of ICT equipment and devices is a common crime. Devices are usually sold in the second-hand market for a fraction of their purchase price. Small to medium-sized portable devices such as laptops and mobile devices make easy targets. These devices must not expose sensitive data when lost. Encryption of data upon such devices is essential. Remote wiping of data and ensuring that factory default credentials are not in use is additionally important to prevent information leaks.
ICT device tampering	Unprotected communications between ICT devices and servers can result in tampering of the information. Sophisticated man-in-the-middle (MITM) attacks can harvest the data in transit.
Distributed Denial of service (DDoS)	Distributed Denial of Service (DDoS) is a common cyber-attack that overwhelms the processing capability and prevents the normal functioning and service delivery of web based services. Irish government websites such as Ireland's Central Statistics Office, the Department of Defense, and the Department of Justice, the National Lottery and many other Irish websites have fallen victim to DDoS attacks.[14] The impact can be high, depending on the type of systems affected. A threat actor performing DDoS attacks may be

[13] https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2021/august/gnecb-warn-public-about-recent-hse-covid-19-test-and-vaccine-scam.html
[14] https://www.ciab.com/resources/ddos-attack-in-ireland/

	motivated by social or political beliefs, part of an organised threat actor group, or state backed criminal organisation. Normally DDoS attacks seek to disrupt normal service over a sustained period of time to impact the target organisation.
Web-based attacks	Extended use of undocumented web services for interoperability purposes, re-used code-bases in developed applications and factors such as non-compliant systems coupled with the desire to maintain up-time and availability of critical services makes exploitation of known or discovered weaknesses trivial. The primary mitigation against vulnerabilities in Web applications is robust development and testing in line with commercial best practices, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities[15].
Web application attacks	Structured Query Language (SQL) Injection, Cross-site scripting (XSS) and DDoS represent a majority share of the occurring web application attacks. Of all applications with vulnerabilities, 65% of them experienced an SQL injection attack. Of this, Government institutions represent 26% or 2.7% globally.[16]
Insider threat	PSB staff, including 3rd party contractors assigned to PSBs, can act as insider threats at any position; however, guests can also act as insiders from within the site if insufficient physical security controls are in place. Commonly motivated by disgruntlement or disagreement with policies and practices, such individuals may collude with threat actors for cyber-attacks at a larger scale, or, by nature of the individuals access to information, they may remove sensitive information for later re-use.

System Failures

Threat Type	Description
Software failure	Most software has undiscovered weaknesses that may manifest as a failure in certain situations. Server-based software commonly includes the operating system, middleware (such as a database), and/or webserver software. A failure in any component of the integrated tools may lead to service disruption or other consequences. An update of any individual component may have knock-on impact to others resulting in a software failure.
Outdated software / firmware	Lack of procedures and good practice in relation to firmware or software updates is a threat for organisations, not just PSBs. Legacy systems and software used beyond their supported lifecycle have potential to expose unfixable weaknesses or inadvertent back doors to malicious actors. However, there may be circumstances where legacy software/systems can't be retired. In this case, PSBs must put in place additional controls to protect the wider network, including: • Isolating such systems from main network; • Enhanced monitoring for unusual network activity; • Restricted access to only those who needed it.

[15] https://owasp.org/www-project-top-ten/
[16] https://www.contrastsecurity.com/glossary/application-attacks

Network components failure	The interconnected network ecosystem within PSB environments has to be resilient, as the requirement for real time data availability is high. If a network component fails this can cause unavailability of a service or system, which can have cascading effects to other critical systems.

Annex 3: ICT Components and Categories

Description of ICT Components

ICT Component	Description
Hardware[17]	Hardware refers to a discrete physical component of an information technology system or infrastructure. A hardware device may or may not be a computing device (e.g., a network hub, a webcam, a keyboard, a mouse).
Software[18]	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
Data & Data Warehousing[19]	Data is facts, figures or information stored in or used by a computer. A database is an organised collection of data stored and accessed electronically and is usually controlled by a database management system (DBMS). Data is collected in a database and can be retrieved by querying it using one or more specific criteria. Databases offer security, remove redundancy and allow multiple views of data. MySQL, Microsoft SQL Server, Oracle database are all examples of databases. A data warehouse, also known as an enterprise data warehouse, is a system used for reporting and data analysis and is considered a core component of business intelligence. They are central repositories of integrated data from one or more disparate sources. A data warehouse allows users to access data from multiple sources all in one place. For example, a data warehouse may combine customer information, mailing list and website. Databases and data warehouses have assumed even greater importance in information systems with the emergence of "big data," a term for the truly massive amounts of data that can be collected and analysed.
Telecommunications	This component connects the hardware to / from a network. Connections can be through wires, such as Ethernet cables, or fiber optics, or wireless, such as Wi-Fi. A network is commonly designed to tie together computers in a specific area, such as an office or a school, through a local area network (LAN). If computers are dispersed over multiple areas, the network is called a wide area network (WAN). The internet itself may be considered as a network of networks.

[17] https://csrc.nist.gov/glossary/term/hardware_device
[18] https://csrc.nist.gov/glossary/term/software
[19] https://www.guru99.com/database-vs-data-warehouse.html

Cloud Computing[20]	Cloud computing is the on-demand availability of computer system resources such as computing power and data storage without the need for active user management. The term is generally used to describe data centre hosted resources made available to many users using the internet. Cloud computing may be limited to a single organisation (private cloud), be available to many organisations (public cloud), or a combination of both (hybrid cloud). There are three main types of cloud computing service models: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS). Customer responsibilities are determined by the service model selected, and the customer is assigned responsibility and ownership for functions such as data classification, network controls, identity and access management, and physical security, correlated to the chosen service model. **IaaS:** The cloud service provider manages the infrastructure - power, network, virtualisation, and data storage. The user has access through an API or dashboard, and essentially rents the infrastructure. The cloud customer manages elements such as the operating system and applications. **PaaS:** The hardware and an application-software platform are provided and managed by the cloud service provider. This gives developers a shared platform for development. **SaaS:** This provides a software application such as a web application that can be accessed through a browser (e.g. Microsoft Office 365). Maintenance is the responsibility of the service provider.
ICT Services	The final and possibly most important component of information systems is the human element: the people that are needed to run the system and the procedures they follow so that the knowledge in the huge databases and data warehouses can be turned into competitive advantage by learning what has happened in the past to guide future action. This component includes all human services support such as maintenance, advisory and professional services, technical support, etc.

ICT Categories

Outlined below are the various types of ICT categories based on their nature / mode of delivery and level of access / liabilities granted to the supplier, regardless of size / contract value.

Procurement Type	Description
Managed Service	A managed service is the outsourcing via contracted terms, of the responsibility to manage operations, maintenance, integration, or development practices of the service normally managed by the host organisation. Contracted terms include measurable elements such

[20] https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

	as service level agreements (SLAs) and key performance indicators (KPIs) that may result in financial sanctions against the Managed Service Provider subject to agreed baselines, for failure to maintain. Managed services enable organisations to avail of specific skills, technologies, or practices from a specialist provider that may be cost advantageous and reduce the risk for the organisation.
Professional Services	Professional services are delivered by human resources based on duration, knowledge, experience, and expertise to deliver required functions. Services may be provided by individual freelance/sole-traders, firms, or companies. Professional services are provided to customers to assist with improving maturity of functions in specific areas of the customer's business. An example of professional services is an independent assessment of organisation's cyber security risk management practices against industry standards or regulations. Another example is resource augmentation where a 3rd party may provide services on behalf of the contracting organisation.
Direct / Indirect Hardware Purchases	Direct procurement seeks to acquire devices, or components thereof, that may be required for the delivery of the main product or service. Direct hardware purchases may offer benefits such as economies of scale / discount by volume of purchase, expertise in function, maintenance, and support. Examples include WiFi network adapters, Graphics Processing Units (GPUs), and storage expansion modules. By contrast, indirect purchases is the practice of acquiring an integrated product or service. Examples of indirect hardware purchases include lease agreements to acquire laptops, physical servers, routers, switches, and even software.
Software Development / Customisation	Software development or customisation is the process of bespoke, tailored, processes used within the Software Development Lifecycle (SDLC). Secure Development Lifecycle (SDL), on the other hand, is the process of including security artefacts in the SDLC. Implementing secure SDL helps follow security best practices, integrating security activities and check-ups across the development cycle. SDL integrates activities such as penetration testing, code review, and architecture analysis into all steps of the development process. Development and customisation aims to fulfil the explicit requirements of an organisation by trained software developers and programmers. SDLC includes multiple phases to align with customer needs.
Commercial Software / Licenses	Commercial Software, often referred to as Commercial Off-the-Shelf software (COTS) comprises of the software package (i.e. Office 365) and a license for its use. Licences are commonly provided and renewed on an annual basis allowing organisations to scale-up and scale-down as required. Commercial software license agreements typically prohibit any modification and are subject to copyright.
Software Escrow	Software escrow exists to limit risk associated to a software developer abandoning or otherwise being unable or unwilling to support custom software. There are three parties to a Software Escrow agreement: the developer, the end-user, and the Software Escrow company. The developer hosts software source code with the software escrow company and agrees to a set of conditions by which the end-user may request the software escrow company to release source code of the software. Should the developer cease function, or become otherwise unable to maintain the codebase, the software escrow company will release the code to the purchaser.

Annex 4: Cyber Security Requirements Overview

For more specific information please see the Cyber Security Baseline Standard and the Cyber Security Baseline Standards Self-Assessment form

Cyber Security Requirements	Expected Evidence / Documentation	Additional Guidance
1. PSB should set out the minimum requirements that a Supplier must meet to ensure that the ICT solution/service being procured adheres to the PSB's internal information security policies. The supplier must demonstrate how they will meet the PSBs' requirements.	- Evidence of compliance / adherence to the PSBs' Information Security requirements may include - audits or verifications from an accredited third party. - Supplier's Information Security Policies which are a set of rules, policies and procedures designed to ensure goods, services, users and networks meet an industry recognised minimum IT security standard may also be provided as supporting evidence.	PSBs can refer to the Section 1.2 'Management of ICT Security Policies and Processes' of the 'Cyber Security Baseline Standards'. In addition, please see the Irish Cyber Security Baseline Standards Requirements for information regarding minimum requirements
2. PSB should set out the minimum requirements that a Supplier must meet to ensure that there are effective maintenance and vulnerability management plans in place for the ICT solution/services being procured which, for example, must include at a minimum notification of addressable weaknesses. The supplier must demonstrate how they will meet the PSBs' requirement including by providing supporting evidence.	- Supplier's vulnerability management policy (this is the ongoing, risk-informed process of addressing weaknesses on Information Technology (IT) infrastructure, operating systems and applications) could be submitted to support the supplier's response to the PSB's requirements. - Security hardening policy (which aims to reduce security risk by eliminating potential attack vectors and condensing any PSBs' attack surface) could be submitted to support the supplier's response to the PSBs' requirements. For example, a Patch Management Plan could be submitted to support the supplier's response to the PSB's requirements.	Other considerations include: Identification and remediation of technical vulnerabilities across IT infrastructure, including hardware, firmware, middleware, and network devices including operation systems and applications. - Enterprise patch management, which is the process of identifying, prioritizing, acquiring, installing, and verifying the installation of patches, updates, and upgrades throughout an organization. For an example of a Patch management plan see NISTSP 800-40 Rev. 4

3. PSB should set out the minimum requirements that a Supplier must meet to ensure that there is an effective reporting and notification policy in place when the supplier becomes aware of a security incident and resulting data breach. The supplier must demonstrate how they can support the claims that will meet the PSB's requirement including by providing supporting evidence.	A cyber security incident is considered to be any adverse event that threatens the confidentiality, integrity, authenticity or availability of a network or information system. The Supplier's breach notification policy (the General Data Protection Regulation (GDPR) introduces a requirement for organisations to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals. Organisations must do this within 72 hours of becoming aware of the breach) could be submitted to support the supplier's response to the PSB's requirement	Please see for further information: https://www.ncsc.gov.ie/incidentreporting/ https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification
4. PSB should set out the minimum requirements that a Supplier must meet to ensure that there are effective resilience plans (business continuity / disaster recovery) in place for the proposed ICT goods or services. The supplier must demonstrate how they will meet the PSBs' requirements including by providing supporting evidence.	Suppliers must provide evidence of their resilience capability which must satisfy the resiliency requirements of the PSB. Note that PSBs must also update their internal resilience plans as a result of the new ICT acquisition. In addition, evidence of regular business continuity and disaster recovery tests being conducted including restoring services to normal operation should be provided.	Disaster Recovery Plan (DRP) provides procedures for relocating information systems operations to an alternate location. Activated after the event of a major hardware or software failure or destruction of facilities**.** For further information please refer to NIST SP 800-34 (Contingency Planning Guide).

5. PSB should set out its minimum data protection requirements that a supplier must meet to ensure that the PSB's data is effectively protected. For example, access to audit and event logs (where permissible) and data retention requirements.	Suppliers should be requested to provide evidence of the following: - In the event of any possible cyber security incident, Supplier's shall have security event monitoring and logging in place in order to capture adequate log information to assist with the investigation of the incident. - Logs must be retained for an appropriate period in order to assist with the detection of malicious activity such as an advanced persistent threat (APT). In addition, the following could be requested as supporting evidence: - Supplier's audit logging and monitoring policy; - Supplier's data retention policy.	This must satisfy the logging and statutory retention requirements of the PSB. PSBs should include the 'right to audit' clause in contracts (where appropriate) and set out requirements to access data protection security audit reports and/or further third-party attestation from suppliers.
6. PSB should set out its minimum encryption and other data protection requirements for certain data types and regulated devices that a Supplier must meet to ensure that the PSBs' data is effectively protected.	Suppliers should be requested to provide evidence of the following: - Supplier's cryptography / encryption policy; - Evidence or details of encryption technology in use for the proposed solution and its communication channels.	PSBs should consider the following: - PSBs should consult IT and security teams as well as the Data Protection Officer, as necessary, for specific encryption requirements. - Encrypt data at rest on mobile devices, laptops and removable media. - Is confidential data at rest secured (e.g., strong encryption as defined by industry best practices)? - Implement cryptographic mechanisms to prevent unauthorised disclosure and modification.

7. PSB should specify any applicable cyber security standard or certification which it requires the Supplier to meet. This should be set out as a mandatory requirement in the tender document. To demonstrate this, Tenderers must provide evidence of their certification to the relevant standard (or equivalent) for example ISO 27001, NIST CSF.	Copy of the supplier's current valid standard or certificate outlining scope of standard and/or certification and validity.	For further information See Cyber Security Baseline Standards.
8. PSB should set out its minimum-security assessment or attestation reporting that a Supplier must meet supplier relevant to the proposed ICT solution or services for example approach to vulnerability assessment.	In addition, the following could be requested as supporting evidence: - Red Teaming. - Vulnerability Assessment. - Penetration Testing Reports.	Include the 'right to audit' clause in contracts, and establish requirements to access security audit reports and/or further third-party attestation from suppliers. For example, a security penetration test report should include the security issues identified, risks, and recommendations that demonstrate appropriate security controls.
9. PSB should set out its minimum-testing requirements that a Supplier must meet for ICT devices and solutions intended to provide essential services. Requirements for testing policies including criteria/ thresholds must be specified in the tender the tender documentation.	The following could be requested as supporting evidence: - Evidence of testing if carried out by a Third party. - Other Supporting evidence as appropriate.	Please see for further information: - NIST Special Publication 800-53B contains security and privacy control baselines for federal information systems and organizations. It provides guidance for tailoring control baselines and for developing overlays to support the security and privacy requirements of stakeholders and their organizations Security and Privacy Controls for Information Systems and Organisation. - NIST SP 800-171: Protecting Controlled Unclassified Information in Non-federal Systems and Organizations

Annex 5: Worked Example of ICT Risk Management Methodology based on ISO/IEC 27005 (Should be Organisation Specific)

The **worked example table below** includes a high-level risk matrix based on Likelihood/Impact to determine the Risk Rating in each stage of the cyber security specification process of the ICT components. It must be noted that these risks are not all inclusive and specific risks will apply depending on the category/ types of ICT components and the relative PSB requirements. As a pre-requisite to procurement, ***PSBs must complete their own organisation-specific risk assessment*** to identify potential risks and solutions in order to manage those risks as part of the ICT acquisition. ISO 27005 provides annexes as reference and guidance to organisations for conducting any information security risk assessment. It is up to the PSB to assess and measure risks in a way that is relevant to their respective functions.

Stage	CG	Risk ID #	Risk of…	Likelihood	Impact	Risk Rating	Risk Level
Plan	CG1	R1	Inaccurate or insufficient needs/requirements analysis for new ICT solution due to lack of clarity by the requestor regarding the needs.	4	4	16	High
		R2	Not meeting legal cyber security and data protection requirements.	4	5	20	Very High
	CG2	R3	Misunderstanding the market capability due to insufficient market analysis.	3	4	12	High
		R4	Not getting the best market offer for the required solution due to unclear requirements or suppliers' inability to meet the required level of cyber security controls.	4	4	16	High
	CG3	R5	Not identifying all requirements resulting to the solution not meeting the business needs.	3	4	12	High
		R6	Not accurately translating all requirements into tender specifications resulting to inaccurate response of suppliers.	4	4	16	High
Source	CG4	R7	Not including all technical, legal, and business requirements into tender documentation.	3	4	12	High
		R8	Not outlining all cyber security contractual requirements for the supplier to adhere to which may result in contract management/supervision and/or cost implications.	4	5	20	Very High
	CG5	R9	Inability to effectively evaluate supplier responses and claims on cyber security maturity.	4	5	20	Very High
	CG6	R10	Inability to agree a mutually beneficial service level agreements with suppliers resulting to sub-standard after-sales services (e.g., monitoring and reporting of cyber security incidents).	3	4	12	High
Manage	CG7	R11	Suppliers' cyber security controls falling below acceptable level during the contract term.	3	4	12	High
		R12	Supplier's inability to maintain the service level agreement and the PSB's lack of oversight.	3	3	9	Medium
	CG8	R13	Supplier's inability to meet contractual requirements, therefore not continuously meeting PSB's requirements and expected value for investment.	4	5	20	Very High
		R14	Vendor lock-in and other technical interoperability issues with data held by suppliers on behalf of the PSB.	4	5	20	Very High

The following **Likelihood** and **Impact** description were used to assign scores for objective calculation purposes.

Likelihood:

Level	Value	Description
Insignificant	1	Economic loss that does not jeopardize the interests of the company and does not affect the normal flow of processes.
Low	2	Economic loss acceptable to the company. It affects to the financial situation of the organization, but it does not affect considerably the normal execution of the processes of the institution.
Serious	3	Medium economic loss that may affect the normal flow of some processes of the company.
Disastrous	4	Significant economic loss which implies additional (not planned) effort. It may generate a partial interruption of processes of the company.
Catastrophic	5	Economic loss that seriously compromises company's equity and stability. It interrupts indefinitely the normal operation of different processes of the company.

Level	Value	Description
Highly improbable	1	This occurs only in exceptional circumstan The existing security controls are good anc they offer adequate level of protection.
Improbable	2	This could happen at some time. Existing security controls are moderate and they generally offer an adequate level of protect
Eventual	3	It is possible the occurrence of new incide but not very likely.
Probable	4	It happens normally. There is a high probability that there will be such incident the future.
Highly probable	5	It is expected to happen in most circumstar Existing security controls are low or ineffective.

Annex 6: Security Assessment Sheet

	PLAN Stage Guidelines
☐	Identify minimum security requirements for any solution.
☐	Engage the Market. Research relevant suppliers and products. Consider prospective suppliers' internal information security policies that are applicable to the ICT goods and services under offer. Understand and challenge any inconsistencies in the security policies which should not negatively affect existing resources.
☐	Consider goods and services maintenance and management plan including lifetime vulnerability management and notification of addressable weaknesses (this should include hardware and software patches and updates).
☐	Define SLAs and KPIs that the supplier must meet and any remedies that the supplier may incur in failing these performance objectives.
☐	Ensure reporting and notification obligations of the supplier are in place if they become aware of a security vulnerability, incident and/or data breach. Vulnerability management encompassing Coordinated Vulnerability Disclosure (CVD) and mandatory reporting obligations should be clearly set out.
☐	Where procurement of ICT products or services includes devices with features such as Wi-Fi, Bluetooth, file-sharing, Remote access, etc., ensure that commissioning and provisioning of devices includes disablement of non-essential services and secure by design and secure by default cybersecurity models.
☐	Research relevant suppliers and products. ICT devices and solutions intended to provide essential services should have been certified or independently verified and tested prior to use to ensure that they can perform and deliver as expected. Testing policies and acceptable criteria/thresholds should be communicated to suppliers and should be part of the tender documentation.
☐	Resilience requirements (business continuity / disaster recovery) for the new ICT goods or services should be defined for inclusion in the contract. PSBs should also update their internal resilience plans as a result of the new ICT acquisition.
☐	Require, where permissible, access to logs and define data retention requirements. Logs must be retained for an appropriate period in order to assist with the detection of malicious activity such as an advanced persistent threat (APT).
☐	Include, where permissible, the 'right to audit' clause in contracts and establish requirements to access security audit reports and/or further 3rd party attestation from suppliers.
☐	Specify encryption and other protection measures required for certain data types and regulated devices. Encrypt data at rest on mobile devices, laptops, and removable media. Consult the Data Protection Officer as necessary.
☐	Specify the cyber security certification requirements (i.e., EU certification scheme, if applicable, or equivalent) within the details to be provided by suppliers in response to tender requests.
☐	When procuring cloud-based solution / services, PSBs should refer to OGP Cloud Guidance and OCGIO Cloud Computing Advice Note. Attention is specifically required on the collection, processing, and storage of data by Cloud Service Providers. https://assets.gov.ie/135678/dfc88c52-108e-4d10-aaee-408d15f92c03.pdf
☐	PSBs should set the minimum security requirements for the proposed ICT solution as well as the security expectations of the supplier.
☐	Design the Tender. Translate Requirements into Procurement Specifications. The tender documentation should clearly stipulate the mandatory and supporting evidence required from suppliers to demonstrate their compliance and adherence to these requirements.
☐	When evaluating certifications, it is important to understand the scope of the certification and the scope of the service to be contracted. A provider of cloud services might be ISO 27001 certified on some parts of the service (customer support service) but not in other services which may be of higher importance to the PSB.
☐	Each organisation (Contract and supplier) has to have its own accredited certification in place. using a third party service which has a certification in place does not confer any certification rights on the organisation using the service.
☐	A periodic risk assessment should be carried out to ensure that the supplier is managing information security risks related to the services / products they provide to the PSB.
☐	Product specifications, scope of work, service level requirements, Terms and Conditions, roles and responsibilities must be included in the tender documentation. Cyber security requirements must be clearly outlined, and the supplier should be required to demonstrate how they will meet the requirements supported by evidence of compliance / adherence as appropriate.
☐	Any technical specifications should include an update policy to address vulnerabilities via software updates or timely patching.
☐	Any access procedures particularly remote access to administrative functions /update procedures or involvement of third-party providers should be risk assessed, and any risk mitigation measures should be clearly set out.
☐	The PSB should assess the adherence of the supplier's control environment against the 'Public Sector Cyber Security Baseline Standards' or equivalent standards or certification (e.g., ISO 27002, NIST CSF, etc.). Seek further evidence of compliance if needed.
	SOURCE Stage Guidelines
☐	Select Bidders Seek further evidence of selection criteria and specification/requirements as set out in the tender document, and then incorporated in the contract.

☐	Evaluate Bids. If appropriate, apply cyber security selection criteria based on technical and professional ability.
☐	Evaluate compliance with tender cyber security specifications. It is also important that the members of the contracting authority's evaluation team have appropriate subject matter expertise to assess the tender response.
☐	The tender proposals should clearly allow a tenderer to demonstrate how the goods/ services will be delivered as per the contractual specifications.
☐	All criteria used to assess supplier responses must be capable of being verified.
☐	Verify bidder claims relating to cyber security.
☐	Apply ICT and cyber security life cycle costing if included in tender.
☐	Notify bidders of outcome of evaluation.
☐	Apply stand-still period if applicable.
☐	Finalise contract terms with successful bidder.
	MANAGE Stage Guidelines
☐	Any third-party vendor access must be tightly controlled as this is a proven vector for penetrating highly protected networks.
☐	Logs must be kept securely, with defined access criteria.
☐	Logs must be retained for an appropriate period as defined in order to assist with the detection of malicious activity such as an advanced persistent threat (APT).
☐	For as long as the supplier has direct or indirect access to the PSBs ICT systems, services, and information, the supplier should be required to provide regular reports on how they are performing against the SLA as well as the certain security monitoring metrics and necessary software updates and patches.
☐	All cyber security requirements including any legally binding cyber security requirements must be included in the contract and must be upheld throughout the life of the contract. The contract should include provisions for any identified deviation, where not corrected within a defined timeframe,may lead to legal remedy, e.g. contract termination.
☐	Monitor Performance. Any changes to Information security policies that will be required of the supplier and their products and services should be monitored. This should cover, at a minimum, Information Security Requirements: Please see NIST Special Publication 800-53B Security and Privacy Controls for Information Systems and Organization and NIST SP 800-171https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
☐	In addition to performance checks and security risk assessments, the PSB should also review their supplier's compliance with cyber security contractual requirements at regular intervals (usually stated in the contracts) and prior to contract term / full delivery.
☐	For any clarification please see the Public Procurement Guidelines for Goods and Services which sets out information on procurement procedures and is available at (https://www.gov.ie/en/publication/c23f5-public-procurement-guidelines-for-goods-and-services/).

Annex 7: References

Category	References
Articles	Database vs Data Warehouse: Key differences *https://www.guru99.com/database-vs-data-warehouse.html*
	Three Types of Social Engineering Attacks to Know *https://www.proofpoint.com/us/corporate-blog/post/three-types-social-engineering-attacks-know*
	Types of Cloud Computing *https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud*
	Software Definition https://www.techtarget.com/searchapparchitecture/definition/software
	The Four Categories of Computer Hardware *https://turbofuture.com/computers/The-Four-Main-Categories-Of-Computer-Hardware-Parts*
Government Guidelines / Publications	Procurement Guidelines for Cybersecurity in Hospitals *https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.*
	ENISA Threat Landscape 2021 *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021*
	GNECB Warn Public About Recent HSE COVID-19 Test and Vaccine Scam *https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2021/august/gnecb-warn-public-about-recent-hse-covid-19-test-and-vaccine-scam.html*
	Cloud Computing Advice Note October 2019 *https://www.gov.ie/en/publication/078d54-cloud-computing-advice-note-october-2019/*
	NIST Special Publication NIST SP 800-161r1. Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations
	National Cyber Security Strategy (2019-2024) *https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf*
Industry Standards / Regulations	BCI Good Practices - Business Continuity Institute Good Practices
	CIS Benchmarks - Center of Internet Security (CIS) Benchmarks - Critical Security Controls (SANS TOP20)
	COBIT - Control Objectives for Information and Related Technologies
	Data Protection Acts 1988 and 2003 - Data Protection Act 1988
	Digital Service Act (DSA) - Proposed Digital Service Act
	DORA - Digital Operational Resilience Act
	ENISA Security Guide for ICT Procurement - European Network and Information Security Agency (ENISA)
	ePrivacy Regulations - S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011
	EU Cybersecurity Act - EU Cybersecurity Act
	GDPR - General Data Protection Regulation
	Irish Cyber Security Baseline Standards - Irish Cyber Security Baseline Standards
	ISA 62443 - Cyber Security Standards - Security of Industrial Automation and Control Systems
	ISO 15288 - Systems and software engineering — System life cycle processes
	ISO 20000 Series - Information technology — Service management — Service management system requirements
	ISO 22301 - Security and resilience — Business continuity management systems — Requirements
	ISO 27001:22 (ISMS) - Information technology — Security techniques — Information security management systems — Requirements
	ISO 27002 - Information security, cybersecurity and privacy protection — Information security controls
	ISO 27011 - Information technology -- Security techniques -- Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations
	ISO 27017 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Industry Standards / Regulations	ISO 27018 - Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
	ISO 27036 - Information technology — Security techniques — Information security for supplier relationships (four parts)
	ISO 27070 - Information technology — Security techniques — Requirements for establishing virtualized roots of trust
	ISO 27071 - Information technology — Security techniques — Security recommendations for establishing trusted connections between devices and services
	ISO 27701 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
	Law Enforcement Directive - Data Protection Act 2018
	NCSC UK Cyber Essentials - National Cyber Security Centre (NCSC) UK Cyber Essentials
	NIS / NIS 2 - Directive on Security of Network and Information Systems
	NIST Cyber Security Framework (CSF) - Cybersecurity Framework Version 1.1
	NIST SP 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
	NIST SP 800-160 - Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
	NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations
	NIST SP 800-171 - Protecting Controlled Unclassified Information in Non-federal Systems and Organisations
	NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organisations
	NSAI - National Standards Authority of Ireland
	PCI DSS - Payment Card Industry Data Security Standard
Journals/Books	Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on Public Procurement and Repealing Directive 2004/18/EC *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0024*
	Verizon report: cyber incidents, breaches driven by external actors *https://bankingjournal.aba.com/2022/05/verizon-report-cyber-incidents-breaches-driven-by-external-actors/*
	Routledge Handbook of International Criminology *https://www.routledge.com/Routledge-Handbook-of-International-Criminology/Smith-Zhang-Barberet/p/book/9781138380424*
	Life-long Learning Competence Perceptions of the Teachers and Abilities in Using Information-Communication Technologies *https://www.sciencedirect.com/science/article/pii/S1877042815030943?via%3Dihub*
Press Releases	DDoS Attack in Ireland https://www.ciab.com/resources/ddos-attack-in-ireland/
	Reasons Public Sector Organisations Are Moving Rapidly To The Cloud *https://www.forbes.com/sites/sap/2021/09/17/4-reasons-public-sector-organizations-are-moving-rapidly-to-the-cloud/?sh=523a8d2575eb*
	National Risk Assessment for Ireland 2020 *https://www.gov.ie/en/press-release/5e685-national-risk-assessment-for-ireland-2020/*
Reports	Cybercrime: Current Threats and Responses *https://www.justice.ie/en/JELR/Cybercrime_-_Current_Threats_and_Responses.pdf*
	CSIRT-IE Reports on Internet Accessible Servers & Services - DoS Attacks *https://www.ncsc.gov.ie/emailsfrom/Shadowserver/CVE/*
	Data Breach Investigations Report (2008-2022) *https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf*
	The Economic Cost of Cybercrime in Ireland *https://www.grantthornton.ie/insights/publications/cost-of-cyber/*

Annex 8: National/EU Public Procurement, Data Protection & Cyber Legislation

Title	Short Description
EU Directive 2014/24: EU Procurement Directive- These have been implemented into Irish law by S.I. No. 284/2016,	The EU Procurement Directives were transposed into Irish Law in 2016 and 2017 by way of national Regulations contained in various Statutory Instruments. This legislation applies to all PSBs, and includes procurement of ICT goods and services. The legislation specifies that national authorities must treat all applicants equally and not discriminate between them when using public procurement to invite tenders to provide works, supplies or services.
EU Directives 2014/25 Utilities **These have been implemented into Irish law by S.I. No. 286/2016.**	Directive 2014/25/EU on procurement by entities operating in the water, energy, transport and postal services sectors adopted an approach that Contracts are awarded based on the economically most advantageous tender (price, cost, quality-price ratio).
EU Directives 2014/23 Concessions These have been implemented into Irish law by S.I. No. 203 of 2017.	An adequate, balanced, and flexible legal framework for the award of concessions would ensure (i) effective and non-discriminatory access to the market to all Union economic operators; and, (ii) legal certainty, favouring public investments in infrastructures and strategic services to the citizen.
EU Directive 2009/81 Security and Defence	This directive sets EU rules for the procurement of arms, ammunitions and war material (plus related works and services) for defence purposes, but also for the procurement of sensitive supplies, works and services for security purposes. It is tailored to the specificities of defence and security equipment and markets.
EU Resilience Act CRA (DRAFT)	The Cyber Resilience Act (CRA) aims to safeguard consumers and businesses buying or using products or software with a digital component. The Act would see inadequate security features become outdated with the introduction of mandatory cybersecurity requirements for manufacturers and retailers of such products, with this protection extending throughout the product lifecycle.
The Network and Information Security Directive (NISD) [21]	The European Parliament adopted the NIS directive to establish a standard for implementing cyber security regulations for EU organisations. The NIS was adopted in 2016 and was incorporated into Irish law as Statutory Instrument No. 360 of 2018 on 18th September 2018.The expected introduction of enhancements via NIS2 directive include strengthening the security requirements, addressing the security of supply chains, improving reporting obligations, and introducing increasingly stringent supervisory measures with higher enforcement expectations backed by sanctions throughout the EU.
General Data Protection Regulation (GDPR)	GDPR came into force on 25th May 2018. It sets the rules for the processing and free movement of personal data and applies to all domains of the public and private sector. PSBs and their suppliers / service providers may gain access directly or indirectly to personal data during the course of service delivery. As such, both the PSBs and their suppliers processing personal data have the following obligations (among others):

[21] A revised and updated Directive, the so called NIS2 is to be published in the Official Journal of the EU shortly.

	• implement appropriate technical and organisational measures to ensure security of the processing systems, services, and personal data; • perform data protection impact assessment, and; • report data breaches that are likely to result in a risk to the rights and freedoms of individuals within 72 hours after having become aware of them.
EU Cybersecurity Act	The EU Cybersecurity Act has been operational since 27th June 2019, establishing ENISA as the focal point for cyber security issues across the EU and establishes the European cyber security certification framework. This act strengthens the powers of ENISA taking on additional responsibilities and resources, and the framework brings with it rules for EU wide certification of ICT goods, services and processes. Companies conducting business in the EU will benefit from having to certify their ICT goods, processes and services only once and see their certificates recognised across the European Union. The European cyber security certification framework effectively supersedes all national frameworks. Under this framework, multiple schemes were created for different categories of ICT goods and services, including the security standards that should be achieved and the evaluation methods to attest them.

Annex 9: Relevant Industry Standards and Guidelines

Title	Short Description
Cyber Security Baseline Standards	The National Cyber Security Centre (NCSC), in conjunction with the Office of the Government Chief Information Officer (OGCIO), have developed these guidelines, which are intended to create an acceptable security baseline, and form a broad framework for a set of measures which can be revised over time. The 'Cyber Security Baseline Standard Framework' can be used to assess and improve the management of cyber security risks and is aimed at Public Service Bodies to increase maturity by identifying, protecting, detecting, responding, and recover from/to realised cyber security risks by minimising damage and impact.
ENISA Security Guide for ICT Procurement	This 'Security Guide for ICT Procurement' aims to support primarily electronic communications service providers but also ICT vendors with practical guidelines to better manage potential security risks in procured goods or outsourced services, which could lead to disruptions, or outages in electronic communications services. This guide maps a set of security risks with security requirements and can be applied to vendors to prevent or mitigate those risks.
NIST Cyber Security Framework (CSF)	The NIST CSF provides guidance on how to manage and reduce IT infrastructure security risk. The CSF is made up of standards, guidelines and practices that can be used to prevent, detect, and respond to cyber-attacks.
ISO:IEC 27001:2022 Information Security Management System (ISMS)	ISO 27001 is the international standard that describes best practices for an ISMS. The Standard takes a risk-based approach to information security. This requires organisations to identify information security risks and select appropriate controls to tackle them.
Center of Internet Security (CIS) Benchmarks	CIS Benchmarks are a set of globally recognized and consensus-driven best practices to help security practitioners implement and manage their cyber security defenses.
United Kingdom's Cyber Security Essentials and Supply Chain Security Guidance	The UK's government, in an effort to improve cyber security practices and reduce associated risk through the supply chain, introduced the 'Cyber Essentials Scheme'. The scheme defines a set of expected controls and two certification levels: Cyber Essentials – a self-assessment of standard attainment and, Cyber Essentials Plus – an independent third-party certification of a suppliers attainment of standards. The supply chain security guidance is composed of 12 principles, designed to help UK-based organisations to establish effective control and oversight of the supply chain.

Annex 10: Acknowledgements

This document has been prepared by Grant Thornton Ireland under contract with the National Cyber Security Centre (NCSC). This document is the first cyber security guidance issued to Irish Public Service Bodies (PSB) in relation to specific best-practice cyber security requirements as part of an ICT procurement process. These guidelines are dynamic in nature and will be subject to amendment and review in line with best practice and technical advances within the ICT ecosystem. The authors would like to thank the following organisations for their valuable contributions (in alphabetical order):

Brian Honan Ltd

Central Statistics Office

Cork City Council

Defence Forces

Department of Agriculture, Food and the Marine

Department of Defence

Department of Education

Department of Employment Affairs and Social Protection

Department of Finance

Department of Foreign Affairs and Trade

Department of Further and Higher Education, Research, Innovation and Science

Department of Health

Department of Public Expenditure and Reform

Department of the Environment, Climate and Communications

Department of the Taoiseach

Dublin City Council

Dublin Port

EirGrid Group

European Union Agency for Cybersecurity

Health Service Executive

Local Government Management Agency

Mandiant EMEA Government Team

Microsoft

National Cyber Security Centre

Office of Government Procurement

Office of Public Works

Palo Alto Networks

Public Appointments Service

Revenue Commissioners

The National Shared Services Office

University College Cork