SAINT

D2.7 Cyber-Security Standards, Benchmarking & Best Practices Overview

Work Package 2: Metrics of Cyber-security

Document Dissemination Level

P	Public	☒
CO	Confidential, only for members of the Consortium (including the Commission Services)	☐

Document Due Date: 30/04/2018
Document Submission Date: 15/05/2018

This work is performed within the SAINT Project – Systemic Analyser in Network Threats – with the support of the European Commission and the Horizon 2020 Program, under Grant Agreement No 740829

Document Information

Deliverable number:	**2.7**
Deliverable title:	Cyber-Security Standards, Benchmarking & Best Practices Overview
Deliverable version:	1.0
Work Package number:	2
Work Package title:	Metrics of Cyber-Security
Due Date of delivery:	30/04/2018
Actual date of delivery:	15/05/2018
Dissemination level:	Public
Editors:	Christopher Hemmens (MI), Sébastien Ziegler (MI)
Contributor(s):	Anna Brékine (MI) Adrian Quesada Rodriguez (MI) Sébastien Ziegler (MI) Christopher Hemmens (MI) Olivia Doell (AS) Pasquale Annicchino (AS) Gabriela Znamenackova (AS) Dimitris Kavallieros (KEMEA) George Kokkinis (KEMEA)
Reviewer(s):	Jart Armin (CYBE)
Ethical advisor(s):	Christina Chalanouli (KEMEA)
Project name:	Systemic Analyser in Network Threats
Project Acronym	SAINT
Project starting date:	01/05/2017
Project duration:	24 months
Rights:	SAINT Consortium

Version History

Version	Date	Beneficiary	Description
0.1	07/02/2018	Brékine, Hemmens (MI)	First round of content
0.2	06/04/2018	Brékine (MI), Quesada Rodriguez (MI), Hemmens (MI), Doell, Znamenackova (AS), Kavallieros, Kokkinis (KEMEA)	Contributions from other partners
0.3	13/04/2018	Hemmens (MI)	Addition of section introductions, section summaries, acronyms, and conclusion
0.4	20/04/2018	Ziegler (MI), Brékine (MI)	Revision structure and Addition of section 2
0.5	23/04/2018	Brékine (MI), Annicchino (MI)	Addition of section 6 and 8
0.6	27/04/2018	Brékine (MI)	Addition of section 9
0.7	28/04/2018	Ziegler (MI)	Text Section 8 and 9 + revised matrix
0.8	29/04/2018	Ziegler (MI), Quesada Rodriguez (MI), Brekine (MI)	Revision and structure modification

1.0	11.05.2018	Ziegler (MI), Quesada Rodriguez (MI), Brekine (MI)	Revision, methodology adaption and extension with new complements

Abbreviations and Acronyms

ACRONYM	EXPLANATION
BCMS	Business Continuity Management System
BIA	Business Impact Analysis
BITAG	Broadband Internet Technical Advisory Group
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
CPS	Cyber-Physical System
CTI	Cyber-Threat Intelligence
DCS	Distributed Control System
DHS	Department of Homeland Security
DoS	Denial of Service
DPA	Data Protection Act
ETSI	European Telecommunications Standards Institute
ICO	Information Commissioner's Office
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
LWC	Lightweight Cryptography
M2M	Machine-to-Machine
MAC	Media Access Control or Message Authentication Code
MILE	Managed Incident Lightweight Exchange
NIST	National Institute of Standards and Technology
NoT	Network of Things
PET	Privacy-Enhancing Technology
PII	Personally Identifiable Information
PIMS	Personal Information Management System
PKI	Public Key Infrastructure
POAS	Platform/Operating System/Application/Service
PP	Protection Profile
PPM	Privacy Policy Manager
RFID	Radio Frequency Identification
RMF	Risk Management Framework
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol

SDO	Standards-Developing Organisation
SN	Sensor Network
ST	Standard Target
TC	Technical Committee
TOE	Target of Evaluation
TLS	Transport Layer Security
TPM	Tamper-Proofing Mechanism
UEFI	Unified Extensible Firmware Interface
USN	Ubiquitous Sensor Network
WSN	Wireless Sensor Network

Table of Contents

Table of Figures

Table of Tables

1. Introduction

The deliverable D2.7 is directly related to the task T2.5 on Cyber-Security Standards, Benchmarking & Best Practices. The objectives of this task are:

1. **To investigate the various existing standards related to cybersecurity**. More specifically, it is in charge of reviewing and identifying relevant ISO standards, such as ISO 15408 on ICT Security, ISO 27000 related standards on information management systems (including of course ISO 27018 on cloud security), ISO 29100 related standards on privacy and ISO 31000 related standards on risk management. It is also reviewing existing privacy-related standards, such as EuroPriSe and EuroPrivacy.
2. **To extract the most relevant standards and norms** to be leveraged on in the context of fight against cyber-crime from a systemic perspective.
3. **To conclude with a set of recommendations** related to standards and benchmark use against cyber-crime.

In this deliverable, we set out a summary of existing standards and best practices in relation to cybersecurity as a whole. This includes not just standards of software and hardware, but also management, processes, and procedures among others. This list is not exhaustive; however, we have done our best to balance the number of standards and best practices that we cover against the amount of detail we provide about each one. In general, it should be possible to get a comprehensive sense of where the field stands in 2018.

We begin by looking at the large national and international standards organisations and then move on to more granular levels. Each section is dedicated to a particular type of best practice and broken down by organisation. In each section, we provide a general overview of the types of best practices detailed in the section, which are then followed by a short analysis of the section.

Ultimately, this document will stand as a reference guide for the methods and implementations that instituted elsewhere in the SAINT project and beyond.

In addition to the standards and best practices listed in this document, we would also like to direct the reader to publications by Working Group 1 of the European Cyber Security Organisation (ECS).[1] This organisation was established in June 2016 and is dedicated to the countering of cyber-threats in the European Digital Single Market and the support of the cybersecurity industry in Europe.

In a final note, we remark that the European Union Agency for Network and Information Security (ENISA) approved a new mandate on certification and standards in January 2018.[2] With the desire to create a "*single digital marketplace for Europe*", ENISA will be supporting a dedicated certification model for Europe following the success of standardised mobile phone technology throughout the EU member states.

[1] "ECSO - European Cyber Security Organisation," ECSO - European Cyber Security Organisation, accessed May 3, 2018, https://www.ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management.
[2] ENISA, "Towards a New Role and Mandate for ENISA and the European Cyber Security Month" (Brussels, January 2018).

1.1. Methodology

This deliverable does not aim to provide an exhaustive list of cybersecurity standards[3], but rather seeks to generate a comprehensive overview of those standards which are relevant to the fight against cybercrime on a systemic perspective. For this reason, the methodological approach to the compilation and selection of standards will be driven by the current cybersecurity landscape and the associated cybersecurity risks that are to be defined as part of section 2.

Upon the definition of such risks, the deliverable shall classify and briefly examine those standards which outline fundamental elements in the cybersecurity ecosystem (section 3); the standards that define methods for performing particular tasks in the cybersecurity context, such as managing data, infrastructure, and interchanging information (section 4); and finally, those which provide the fundamental methodologies for managing risk and evaluating systems and procedures (section 5). Additionally, section 6 will consider the effects of the GDPR to the field of cybersecurity and particularly introduce two of the main privacy certification mechanisms.

The contents of all these sections will be further enriched by introducing reference documents on privacy and security. On the privacy side, the document will focus the most relevant guidelines on privacy impact assessment and privacy risk management developed by some of the most influential personal data protection authorities worldwide. Security-wise, recommendations, publications and compilations of other cybersecurity standards generated by several industry associations will be introduced to ensure the reader can identify further resources.

The two final sections of this deliverable (8 and 9) shall be dedicated towards analysing the body of standards presented before and introducing some recommendations to help address the cybersecurity risks identified in section 2. The fundamental tool to perform this analysis, the cybersecurity management matrix, will be compiled in a way that enables to perform a simple but thorough examination of the standards with regards to the expected risks and to identify the smallest combinations of standards that, at the same time can offer the best risk coverage while also serving to identify standardisation gaps. Finally, recommendations will be generated with the aim to maximise risk coverage at the lowest cost to organisations and favouring systemic complementarity among the identified standard combinations, so as to ensure the outputs provided are reliable.

[3] Other bodies of work have attempted to achieve this task (see, for example ECSO - European Cyber Security Organisation, “ECSO State of the Art Syllabus V2,” December 2017, 210.).

2. Contextual Overview

The following section offers a contextual overview of the cybersecurity landscape. First, it addresses the evolution of cybercrime and cybersecurity risks. Next, it discusses the changes introduced with the entry into force of the GDPR. Finally, it presents a list of top cybersecurity risks, which are relevant in the context of this deliverable.

2.1 Evolution of Cybercrime and Cybersecurity Risks

According to Price Waterhouse Cooper's (PwC) Global Economic Crime Survey, cybercrime is the fastest growing economic crime.[4] New trends in cybercrime are surfacing all the time, with estimated costs to the world economy reaching billions of dollars. Criminals take advantage of the speed, accessibility, anonymity and global connectivity to the Internet to pursue a wide range of malicious activities, with either virtual or physical repercussions for the victims. The continuous evolution of cybercrime is fuelled by permanent technological advancements, which create new criminal opportunities, but also by the development of highly complex cybercriminal networks that involve individuals from all over the world and take the attacks to an unprecedented level.

Currently, traditional cybersecurity risks still dominate the cybercrime landscape. In the 2017 Internet Organised Crime Threat Assessment (IOCTA), Europol identifies the five following cybersecurity risk areas and subcategories. The cybersecurity risks are shown in Table 2-1:

Table 2-1: Cybersecurity risks identified by Europol (source: 2017 IOCTA)

Cybersecurity risk areas	Cybersecurity risk subcategories
Cyber-dependent crime	1. Malware 2. Attacks on critical infrastructure 3. Data breaches and network attacks
Child sexual exploitation online	4. Sexual coercion and extortion of minors 5. The availability of child sexual exploitation material 6. Commercial sexual exploitation of children 7. Behaviour of offenders
Payment fraud	8. Card-not-present fraud 9. Card-present fraud
Online criminal markets	10. Darknet markets
Cyber and terrorism	11. Cyberterrorism

A number of cybersecurity risk areas identified by Europol are shared by Interpol. Indeed, the main cybersecurity areas prioritised by Interpol are high-tech crime against computer hardware and software, and cyber-enabled crime, such as financial crime, internet crimes against children, fraud

[4] PwC, "Cyber Becomes the Fastest Growing Economic Crime - PwC's Global Economic Crime Survey 2016 - PwC in the North," accessed May 3, 2018, https://www.pwc.co.uk/who-we-are/regional-sites/yorkshire-north-east/insights/cyber-becomes-the-fastest-growing-economic-crime-pwcs-global-economic-crime-survey-2016.html.

and terrorism. In this matter, Interpol underlines the central role played both by the Darknet and malware, bots and botnets, as cybercrime enablers.[5]

Cybersecurity risks have also been addressed by ENISA. In its 2017 Threat Landscape Report, the European agency has put forward a list of 15 cyber-threats. It is interesting to note that the list includes cybersecurity risks such as identity theft, exploit kits, and cyberespionage, which have not been clearly prioritised by either Europol and Interpol. ENISA's list includes:

1. Malware
2. Web-based attacks
3. Web application attacks
4. Phishing
5. Spam
6. Denial of service
7. Ransomware
8. Botnets
9. Insider threat
10. Physical manipulation/damage/theft/loss
11. Data breaches
12. Identity theft
13. Information leakage
14. Exploit kits
15. Cyber-espionage

Interestingly, the topic of cybersecurity risk is addressed from a slightly differently angle when viewed from a corporate perspective. Cisco's 2018 Annual Cybersecurity Report highlights malware/ransomware, encrypted malicious web traffic, e-mail threats (spam and phishing), cloud service abuse and IoT and denial of service attacks as major concerns.[6] This position is shared by Symantec which, as stated in the 2018 Internet Security Threat Report (ISTR) adds mobile threats to the list of cybersecurity risk areas.[7] Based on these two reports, one can note that both companies approach cybersecurity from a purely business standpoint, and do not include global risks such as cyberterrorism and internet crimes against children in their daily priorities.

In addition to these traditional cybersecurity risks, it is important to note that new tendencies and policy developments risk overturning the cybercrime landscape and may create new challenges and opportunities in the field of cybersecurity:

- Artificial intelligence: artificial intelligence and machine learning will further aggravate current cybersecurity threats and create new challenges. Cybercriminals will use machine learning to carry out their attacks by learning from defensive responses and exploiting newly detected security gaps before they are addressed by the defenders. According to the McAfee

[5]Interpol, "The Threats / Cybercrime / Crime Areas / Internet / Home - INTERPOL," accessed May 3, 2018, https://www.interpol.int/Crime-areas/Cybercrime/The-threats.
[6]Cisco, "Cisco 2018 Annual Cybersecurity Report," February 2018, https://www.cisco.com/c/en/us/products/security/security-reports.html.Cisco, "Cisco 2018 Annual Cybersecurity Report," February 2018, https://www.cisco.com/c/en/us/products/security/security-reports.html.
[7] Symantec Corporation, "Internet Security Threat Report 2018" (Mountain View, California, March 2018).

Labs 2018 Threats Predictions Report, "the development of machine learning to protect organisations will fuel an arms race between defenders and attackers".[8]

- Increased connectivity between IoT devices: with the development of connected home devices, marketers and manufacturers will collect, with or without consent, more personal data in order to better understand consumer trends and behaviour, and to maximise their profit.[9]
- Ransomware: since improved cybersecurity safeguards have led to the decline in the profitability of ransomware, cybercriminals will change their strategies and switch to high-net worth individuals, cyber-sabotage and business disruption.[10]
- GDPR: with the entry into force of the General Data Protection Regulation (GDPR) in May 2018, organisations are likely to have enhanced data management and protection processes in place to guarantee the compliance with the European regulation. Nonetheless, the GDPR in itself is unlikely to deter cyber attackers from committing cybercrime and may even incentivise them to demand higher ransoms from the organisations they have successfully attacked, due to the expensive fines they may face in case of a security breach[11].

2.2 Selection of Top Cybersecurity Risks

Building on the various lists of cybersecurity risks identified by Europol, Interpol, ENISA, Symantec and Cisco in section 2.1, and on the aforementioned realities, it is foreseen that the current cybersecurity landscape will change significantly in the near future. For this reason, this research effort has aimed to compile and select those cybersecurity risks that will become relevant in the near future. It is important to note that the ranking order does not reflect the gravity of a given threat. Although the selection is not exhaustive, it attempts to represent the main cybersecurity challenges faced by the public and private sectors as well as by regular individuals. The list of prioritised cybersecurity threats below will be included in a matrix of risk management presented in chapter 9 of the deliverable. The top 19 cybersecurity risks are:

1. Malware: short for "malicious software" and refers to software programs intended to damage or corrupt an IT system. Common examples of malware include viruses, worms, Trojan horses and spyware. In the scope of this deliverable, malware also includes mobile malware, exploit kits and counter antivirus services.
2. Ransomware: another form of malware designed to limit users from accessing their system until a sum of money is paid.
3. Web-based attacks: attacks which make use of web-enabled systems and services such as browsers, websites and the IT-components of web services and web applications. Common examples of such attacks include web browser exploits, web servers and web services exploits, drive-by attacks water-holing attacks, redirection and man-in-the-browser attacks.[12]
4. Web application attacks: those attacks targeting web applications, web services and mobile applications. The characteristic of these attacks is that they occur within the scope of web application runtime environments and APIs.

[8] McAfee Labs, "McAfee Labs 2018 Threats Predictions," November 2017, 1.
[9] McAfee Labs.
[10] McAfee Labs.
[11] For more information on the GDPR, see supra section 6.1.
[12] ENISA, "ENISA Threat Landscape Report 2017" (Heraklion, Greece, January 2018).

5. Mobile threats: include mobile malware, mobile operation system vulnerabilities and other types of mobile-related threats.
6. Denial of service: security incidents that occur when an attacker attempts to prevent a legitimate user from accessing the service.
7. Botnets: collections of internet-connected devices, which are infected and administered by malware.
8. Identity theft: a type of data breach in which the attacker seeks to get access to private information that is used to identify a person or a computer system. Such information may be: names, addresses, financial data, contact data, health data, etc.
9. Data breaches: successful cyberattacks that have led to the loss of data.
10. Cloud service abuse: relates all kinds of cyberthreats occurring in a cloud environment. Examples of such threats include: data breaches, data loss, insufficient due diligence, abuse and reprehensible use of cloud services, account hijacking and malicious insiders.[13]
11. Information leakage: a type of data breach which occurs when diverse forms of information, ranging from personal data to business data is revealed.
12. Insider threat: a malicious threat to an organisation's security or data that comes from people within the organisation or close to the organisation, such as third parties.
13. Phishing: a cyberattack which consists in sending fraudulent e-mails claiming to be from authentic companies in order to lure individuals to divulge personal information, such as passwords and credit card numbers.
14. Spam: an irrelevant or unsolicited message, typically sent to a large number of users for the purposes of advertising, phishing, spreading malware, etc.
15. Darknet: networks that are not indexed by search engines and are only available to a select group of people. The Darknet may be used for illegal peer-to-peer file sharing.
16. Child sexual exploitation online: "*the sexual abuse of a person below the age of 18, as well as to the production of images of such abuse and the sharing of those images online."*[14]
17. Cyberespionage: the use of computer networks to gain illicit access to confidential information, usually detained by a government or an organisation.
18. Cyberterrorism: a *"premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents".*[15]
19. Personal Data Protection Breach: *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*[16]

[13] Matthew Wilson, "What Are the 12 Biggest Cloud Computing Security Threats? - Cloud Computing News," January 4, 2016, https://www.ibm.com/blogs/cloud-computing/2016/04/01/12-biggest-cloud-computing-security-threats/.
[14] Europol, "Child Sexual Exploitation," Europol, accessed May 3, 2018, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation.
[15] Peter W. Singer, "The Cyber Terror Bogeyman," *Brookings* (blog), January 11, 2012, https://www.brookings.edu/articles/the-cyber-terror-bogeyman/.
[16] European Council European Parliament, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)," Pub. L. No. 32016R0679, 119 OJ L (2016), http://data.europa.eu/eli/reg/2016/679/oj/eng.

3. Fundamental Sources

3.1. Introduction

This section features standards that outline the fundamentals of the cybersecurity ecosystem, in other words, the establishment of terminology and what we mean when we say "cybersecurity"[17] or "Internet of Things". This is important because we require a common basis on which to lay out the systems and frameworks that will comprise the core of the cybersecurity systems that we hope to implement.

It also includes reports from groups such as iiConsortium, Homeland Security, and the BITAG technical working group, who have identified and made recommendations on cybersecurity issues that are specific to the areas in which they work.

3.2. Summary

Table 3-2: Summary of standards in section 3

Section	Standard(s)	Framework for…
3.3.1	ISO/IEC 27000:2016	Identifying information
3.4.1	NIST SP 800-183	Networks of 'Things'
3.4.2	NIST IR 7628	Smartgrid cybersecurity
3.4.3	NIST SP 1500-201	Cyber-physical systems
3.5.1	ITU-T X.1205	Cybersecurity threats
3.5.2 3.6.1	ITU-T X.1275 ETSI TR 103 304 V1.1.1 (2016-07)	Protection of personally identifiable information
3.7.1	Publicly Available Standard (PAS) 555	Risk management

3.3. International Standards Organisation (ISO)

3.3.1. ISO/IEC 27000:2016 – Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary

This standard sets out a model for setting up and operating a management system and incorporates features that are expert-approved. ISO/IEC 27000 forms the basis for the Information Security Management System (ISMS) family of standards that details the correct storage of information assets including financial information, intellectual property, and employee details as well as other information entrusted to them by customers and third parties.

The ISMS family of standards

- *"defines requirements for an ISMS and those certifying such systems,*
- *provides direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS,*
- *addresses sector-specific guidelines for ISMS, and*

[17] For a thorough examination of the definition of Cybersecurity, see: Charles Brookson et al., *Definition of Cybersecurity: Gaps and Overlaps in Standardisation.* (Heraklion: ENISA, 2015), http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115934:EN:HTML.

- *addresses conformity assessment for ISMS."*[18]

Any organisation that collects and stores information is required by this international standard to maintain an ISMS and ensure they *"monitor and evaluate the effectiveness of [the] implemented controls and procedures; identify emerging risks to be treated; and select, implement, and improve appropriate controls as needed."*[19]

An ISMS consists of "*policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets*."[20] The fundamental principles for successfully implementing an ISMS are:

- *"awareness of the need for information security;*
- *assignment of responsibility for information security;*
- *incorporating management commitment and the interests of stakeholders;*
- *enhancing societal values;*
- *risk assessments determining appropriate controls to reach acceptable levels of risk;*
- *security incorporated as an essential element of information networks and systems;*
- *active prevention and detection of information security incidents;*
- *ensuring a comprehensive approach to information security management;*
- *continual reassessment of information security and making of modifications as appropriate."*[21]

The standard requires the organisation to undertake the following steps in establishing, monitoring, maintaining, and improving its ISMS:

- Identify information security requirements:
  - *"understand identified information assets and their value;*
  - *understand business needs for information processing, storage, and communication;*
  - *understand legal, regulatory, and contractual requirements."*[22]

- Assess information security risks:
  - See ISO/IEC 27005 for information security risk management guidance.

- Treat information security risks:
  - *"apply appropriate controls to reduce risks;*
  - *knowingly and objectively accept risks, providing they clearly satisfy the organisation's policy and criteria for risk acceptance;*
  - *avoid risks by not allowing actions that would cause risks to occur;*
  - *share the associated risks to other parties, for example insurers or suppliers."*[23]

[18] International Organisation for Standardisation, "ISO/IEC 27000:2016 Information Technology -- Security Techniques -- Information Security Management Systems -- Overview and Vocabulary," February 2016, https://www.iso.org/standard/66435.html.
[19] International Organisation for Standardisation.
[20] International Organisation for Standardisation.
[21] International Organisation for Standardisation.
[22] International Organisation for Standardisation.
[23] International Organisation for Standardisation.

- Select and implement controls:
  - See ISO/IEC 27002 for best practices on selecting and implementing the most appropriate controls for the ISMS.

- Monitor, maintain, and improve the effectiveness of the ISMS:
  - Ensure that all the above recommendations are put in place, report results to management, check suitable controls for treating risks within the scope of the ISMS are implemented, and keep records providing evidence and traceability of corrective, preventive, and improvement actions.

- Continual improvement:
  - "*analyse and evaluate the existing situation to identify areas for improvement;*
  - *establish the objectives for improvement;*
  - *search for possible solutions to achieve the objectives;*
  - *evaluate these solutions and make a selection;*
  - *implement the selected solution;*
  - *measure, verify, analyse, and evaluate results of the implementation to determine that the objectives have been met;*
  - *formalise changes."*[24]

Finally, where appropriate, ensure that there is:

- *"information security policy, objectives, and activities aligned with objectives;*
- *an approach and framework for designing, implementing, monitoring, maintaining, and improving information security [is] consistent with the organisational culture;*
- *visible support and commitment from all levels of management, especially top management;*
- *an understanding of information asset protection requirements achieved through the application of information security risk management (see ISO/IEC 27005);*
- *an effective information security awareness, training and education programme, informing all employees and other relevant parties of their information security obligations set forth in the information security policies, standards, etc., and motivating them to act accordingly;*
- *an effective information security incident management process;*
- *an effective business continuity management approach;*
- *a measurement system used to evaluate performance in information security management and feedback suggestions for improvement."*[25]

[24] International Organisation for Standardisation.
[25] International Organisation for Standardisation.

3.4. National Institute of Standards & Technology (NIST)

3.4.1. NIST SP 800-183 Networks of 'Things'

NIST SP 800-183[26] offers a scientific foundation for IoT technologies on the recognition that IoT involves sensing, computing, communication, and actuation. It introduces a shared terminology to improve the awareness of IoT and the communication between stakeholders on relevant matters.

The document argues that the relationship between the Internet of Things (IoT) and the Network of Things (NoT) is indirect. Indeed, IoT is a visual representation of a NoT, since IoT devices are tethered to the Internet. Local Area Networks are examples of NoT, which do not require any 'things' connected to the Internet.

Primitives are building blocks allowing reasoning and simulations. The document introduces five types of primitives which are building blocks for a NoT:

1. Sensor – an electronic tool which estimates physical properties such as temperature, sound, location, weight, acceleration, etc.
2. Aggregator – a software implementation which uses mathematical functions to transform unprocessed data into aggregated data. This process allows managing "big" data.
3. Communication Channel – a channel through which data is communicated.
4. eUtility – a software or hardware product.
5. Decision trigger – a mechanism that produces the final output required to meet the requirements, purpose or specification of a particular NoT.

The publication specifies the roles and specifications of each primitive and their relationships with each other. It is noted that a group of sensors is called a cluster. Clusters may be "weighted", which means that they may have a differentiated effect on an aggregator's computation.
The document establishes six elements that are essential in establishing trustworthiness in regard to what a NoT can offer:

1. Environment – the context in which all the primitives of a NoT operate in.
2. Cost – the financial expenses, as well as time consumed to create and run a NoT.
3. Geographic location – a physical place where a sensor or eUtility functions.
4. Owner – the holder of a sensor, aggregator, communication channel, eUtility or decision trigger.
5. Device_ID – a singular identifier for a specific sensor.
6. Snapshot – a moment in time when synchronisation fired by the other five primitives occurs

Additionally, NIST SP 800-183 discusses the security linked to a "closed" (not connected) NoT compared to an "open" NoT. The document also covers the challenges related to testability.

Finally, the publication focuses on the two core concepts relevant to the five primitives: security and reliability. Each primitive is illustrated with a hypothetical reliability and security scenario, with diverse applications from smart cities to the automobile sector.

[26] Jeffrey M Voas, "NIST SP 800-183 Networks of 'Things':" (Gaithersburg, MD: National Institute of Standards and Technology, July 2016), https://doi.org/10.6028/NIST.SP.800-183.

3.4.2. NIST IR 7628 Revision 1 – Guidelines for Smart Grid Cybersecurity, Volume 1

In the modern age, electric grids have become more complex, interconnected and dependent on IT infrastructures. The technological progress has brought considerable benefits but has also created cybersecurity concerns. NIST IR 7628[27] seeks to support organisations in establishing efficient cybersecurity strategies specifically adapted to smart grid-related characteristics, risks and threats. Organisations involved with smart grids, ranging from energy suppliers to electric car developers may benefit from the content of the report, particularly in regard to risk assessment and security implementation. However, the document serves purely as guidance and advises each organisation working with smart grids to establish its own cybersecurity plan. It is indispensable to address cybersecurity issues at all stages of the system development life cycle, from design through implementation, maintenance and disposition.

NIST IR 7628 Revision 1, Volume 1 is devoted to the smart grid cybersecurity strategy, architecture, and high-level requirements. The document underlines the role of cybersecurity in guaranteeing the grid's reliability and data confidentiality. Furthermore, it also addresses the cybersecurity strategy in the context of smart grids and outlines the tasks used to develop the smart grid cybersecurity document:

- *"Task 1: Selection of use cases with cybersecurity considerations*
- *Task 2: Performance of a risk assessment*
- *Task 3: Specification of high-level security requirements*
- *Task 4a: Development of a logical reference model*
- *Task 4b: Assessment of Smart Grid standards*
- *Task 5: Conformity Assessment*"[28]

This set of tasks allows NIST to establish a list of requirements, which in turn are developed using a high-level risk assessment process outlined in the cybersecurity strategy. The document covers both domain-specific and common requirements to guarantee interoperability. The high-level security requirements explain what smart grids need to provide to improve security. The document also explains at what architectural level security is required. Smart grids involve a large panel of actors, including organisations, buildings, individuals, systems and devices which share, store or process the data used by the smart grid. NIST also clarifies that the smart grid comprises seven areas: transmission, distribution, operations, generation, markets, customer and service provider. The publication introduces the concept of "logical interface", i.e. a "connection between two actors", which was assigned to a logical interface category. The section on "High-level security requirements" tackles the high-level security requirements for each type of logical interface category. The requirements are often performance and reliability oriented. NIST outlines the following requirements:

- *"Operation of the power system must continue 24×7 with high availability (e.g., 99.99% for SCADA and higher for protective relaying) regardless of any compromise in security or the implementation of security measures that hinder normal or emergency power system operations.*

[27] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee, "NIST IR 7628r1 - Guidelines for Smart Grid Cybersecurity" (National Institute of Standards and Technology, September 2014), https://doi.org/10.6028/NIST.IR.7628r1.
[28] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee.

- *Power system operations must be able to continue during any security attack or compromise (as much as possible).*
- *Power system operations must recover quickly after a security attack or the compromise of an information system.*
- *Testing of security measures cannot be allowed to impact power system operations.*
- *Power system management, monitoring, and control will increasingly extend away from the power entities' traditional physical and security environments into external environments that the power entity has little or no influence and control over."*[29]

Although the document offers support to organisations for identifying and adjusting security requirements of smart grids, NIST underlines that organisations are required to carry out their own risk evaluation in parallel.

3.4.3. NIST SP 1500-201 Framework for Cyber-Physical Systems: Volume 1, Overview

The special publication covers cyber-physical systems (CPS), i.e. "smart systems that include engineered interacting networks of physical and computational components"[30]. CPS are expected to have a wide range of applications in different sectors and contribute to an improved quality of life. The document seeks to introduce the terminology and the relationships between the key concepts to facilitate the communication between relevant stakeholders. The objective of the CPS Framework is to establish a unique language to discuss interoperable CPS architectures in a variety of domains. Additionally, it addresses the apprehensions faced by implementers and analysts on this matter;

The CPS Framework involves three facets, which are views on CPS responsibilities in the systems engineering process:

1. Conceptualisation: What are the necessary elements and what is their role in the framework?
2. Realisation: How are these elements supposed to be made and operate?
3. Assurance: How to reach the wanted level of confidence that the described elements will perform properly?

Furthermore, it introduces the following aspects (categories of concerns): functional, business, human, trustworthiness, timing, data, composition, boundaries, and lifecycle. Through the use of a shared vocabulary, NIST hopes to improve the cooperation and collaboration in cyber-physical systems. Figure 3-1 below illustrates the CPS framework.

[29] The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee.
[30] Edward R Griffor et al., "NIST SP 1500-201 - Framework for Cyber-Physical Systems: Volume 1, Overview" (Gaithersburg, MD: National Institute of Standards and Technology, June 26, 2017), https://doi.org/10.6028/NIST.SP.1500-201.

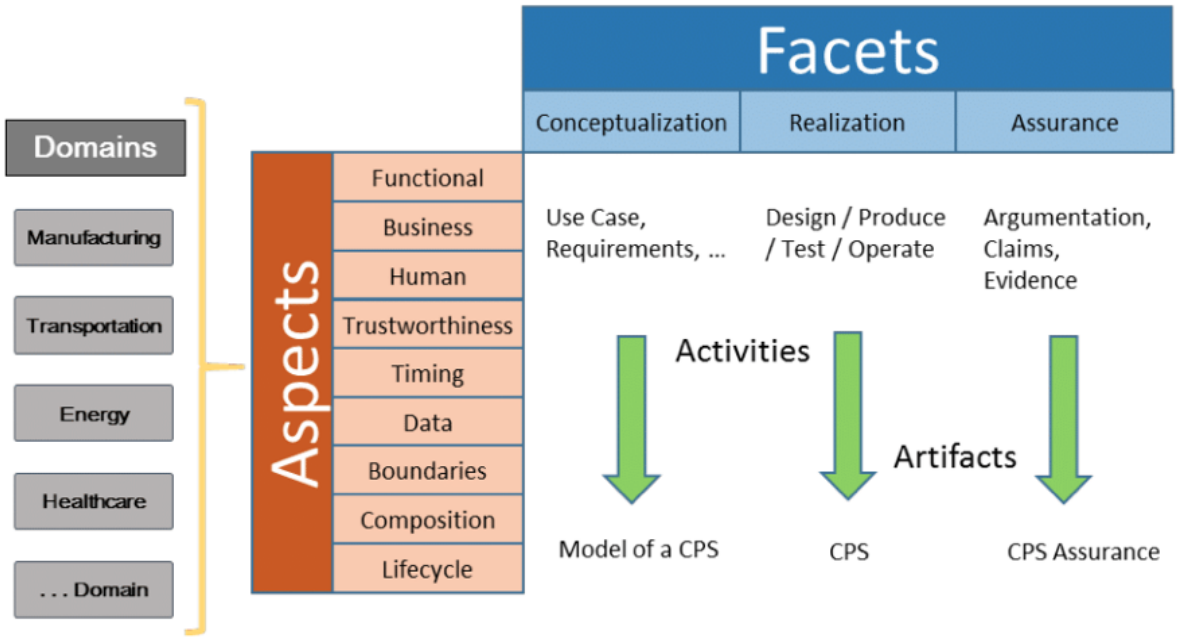

Figure 3-1 : CPS Framework[31]

3.5. International Telecommunication Union (ITU)

3.5.1. ITU-T X.1205 Overview of Cybersecurity

ITU-T X.1205[32] is a recommendation offering an overview of the security threats from an organisation perspective. It discusses the vulnerabilities and the methods used by hackers to conduct an illicit activity. Furthermore, the report discusses the various technologies, network protection principles and risk management strategies to remedy these threats.

The document specifies that threats can either be accidental (not premeditated) or intentional (an "attack"). The following threats to cybersecurity are listed:

- Destruction of information and/or other resources
- Corruption or modification of information
- Theft, removal or loss of information and/or other resources
- Disclosure of information

The document recommends a multiple step methodology to remedy against threats.

1) Identifying the vulnerabilities of the system
2) Analysing the likelihood of threats aimed at exploiting these vulnerabilities
3) Assessing the consequences if each threat were to be successfully carried out
4) Estimating the cost of each attack
5) Costing out potential countermeasures
6) Selecting the security mechanisms that are justified

[31] Griffor et al., 14.

[32] International Telecommunications Union, "Recommendation X.1205: Overview of Cybersecurity," April 18, 2008, https://www.itu.int/rec/T-REC-X.1251-200909-I.

Security strategies are intended for all the architectural layers of a network. This structure allows higher layers to define their own security requirements and allows using the security services at lower levels. The document recommends the following network protection strategies:

- Closed loop policy management: the security policy consists in a dynamic document. ITU-T X.1205 advises IT and network administrators to carry out vulnerability evaluations on their networks, and to guarantee that audits trails are re-examined. Furthermore, the document stresses the importance of implementing the security policy. Responsibility and accountability for policy implementation are necessary.
- Uniform access management: authentication consists in creating an identifier to a network. The process of authorisation establishes the extent of privileges based on access control. The document recommends the use of a centralised authentication mechanism, the use of an authentication system. Furthermore, it advises to use complex, securely stored passwords. The system should be simple and easy to use administratively.
- Secure communications: the document calls for the use of encryption tools for data, voice and mobile networks.
- Variable depth security: security layering allows adjustable depth security. Each consecutive security levels delivers more complex security. Layer 3 VPNs may be used as a third layer to improve security.
- Security management: security management is the basis for all components of the network's management, functioning and lastingness. Nine network management domains need to be examined in order to classify a network's management plane as secure: *"security activity logs, network operator authentication, access control for network operators, encryption of network management traffic, secure remote access for operators, firewalls, intrusion detection, OS hardening, virus free software."*

3.5.2. ITU-T X.1275 Guidelines on Protection of Personally Identifiable Information in The Application of RFID Technology

ITU-T X.1275[33] is a recommendation offering support to radio frequency identification (RFID) users, manufacturers, providers and marketers by securing personally identifiable information. The guidance seeks to protect the individuals' personally identifiable information and to foster a secure environment for RFID technology.
Amongst the most notable threats and violations of PII in RFID the ITU notes:

- Information may be collected without the user's knowledge;
- The RFID tag information can serve profiling purposes by divulging the user's preferences or private data;
- Users can be tracked through the RFID tag.

[33] International Telecommunication Union, "Recommendation X.1275: Guidelines on Protection of Personally Identifiable Information in the Application of RFID Technology," December 2010, https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1275.

The document outlines the following set of privacy principles in the context of RFID:

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security safeguards
- Openness
- Individual participation
- Accountability

The document specifies that given the diverse context in which RFID technologies are use, there is no universal solution to protect personally identifiable information. However, a number of managerial methods can be noted:

- Policies and procedures should be elaborated by data controllers, assigning tasks and responsibilities.
- In respect with the collection limitation principle, only the data that fits the purpose should be used and can only be stored for a limited period of time. The process of recoding PII on the RFID tag should only be used under unique circumstances stipulated by the law or upon the data owner's approval. Furthermore, the collected PII should be encrypted.
- In respect with the individual participation principle, individuals must be informed about any recorded PII, provide consent, right of access, rectification and hold right to oppose. Individuals should be informed of any third parties to whom the data has been divulged. Consent must be obtained before any data is retrieved.
- Shall the data controllers need to keep the PII for different purposes than initially intended or share the information with a third party, consent from the data subject is mandatory.
- The RFID tag should be deleted, destroyed or permanently deactivated when the individual obtains the tagged object, unless the law requires differently or the user consents to keeping the tag active.
- A precise and easily understandable information policy specific for each application should be provided by the data controllers.
- Organisational and technical measures should be taken in order to keep the PII of the RFID system safe from being stolen, leaked, modified or impaired.
- A privacy impact assessment process should be put into place to address privacy concerns and seek the best responses to resolve them. The document recommends a five-stage process (“Project initiation” – “data flow analysis” – “analysis of personally identifiable information infringement factors and risk” – “improvement plan and risk management planning” – “reporting the privacy impact assessment result”).

A data protection official should keep track of the operations carried by the data controller and be up to date on the impact assessments and security measures. Furthermore, they should be able to promptly attend users' requests or concerns.

3.6. European Telecommunications Standards Institute (ETSI)

3.6.1. ETSI TR 103 304 V1.1.1.1 (2016-07) CYBER; Personally Identifiable Information (PII) Protection in Mobile and Cloud Services

ETSI TR 103 304[34] focuses on modern-day ICT and offers an analysis of possible threats to Personally Identifiable Information (PII) in mobile and cloud-based services. It also discusses the technical challenges.

The document discusses the following threats to PII:

- Data fusion and re-identification: Indeed, the concentration of important quantities of data on a limited number of service providers may incite data fusion. Furthermore, tracking cookies may enable the re-identification process.
- Data breaches: service providers and partners of providers processing data may experience data breaches, particularly in the context of cloud computing. Data breaches may not be apparent to the PII principal, which may trust the service provider but not the partner.
- Service termination/inaccessibility: cloud computing storage at large data centres may increase the likelihood of momentary unavailability or even large losses of data.
- Lock-in mechanisms: since lock-in mechanisms do not allow portability of customer's data across various service providers, they may result in data unavailability or data loss.
- Ransomware and spyware: malicious software may threaten data availability and confidentiality.
- Over-collection: the process of over-collection may result in undesirable disclosure of PII.
- Mis-contextualisation: this process occurs when either the data from various customers or from the same user is mixed and used improperly.
- User impersonation: an attacker may steal user information and exploit it for malicious purposes.
- Alteration of ownership or access rights: ownership may be changed when data is shared with some services, which in turn may lead to data being made public, modified or index in search engines.
- Alteration of persistence: storing data on a remote location comes with the risk of alteration of natural data persistence.

Furthermore, the standard addresses technical aspects including the importance of principles from ISO/IEC 29100, the degree of link-ability, trust, awareness of data transaction, semantics, portability, access control, log and auditing, embedded sensors and devices and lawful interception.

[34] European Telecommunications Standards Institute, "ETSI TR 103 304 - CYBER; Personally Identifiable Information (PII) Protection in Mobile and Cloud Services," July 2016, http://www.etsi.org/deliver/etsi_tr/103300_103399/103304/01.01.01_60/tr_103304v010101p.pdf.

3.7. British Standards Institution (BSI)

3.7.1. Publicly Available Standard (PAS) 555

[This standard features in Fundamentals, Frameworks, Evaluation, and Systems.]

PAS 555[35] was released by the British Standards Institution (BSI) in 2013. While most guidance and standards identify problems and offer solutions, PAS 555 takes the approach of describing the appearance of effective cyber security. That is, rather than specifying how to approach a problem, it describes what the solution should look like.

PAS 555 specifically targets the organisation's top management and is deliberately broad in its scope. It is primarily intended as a framework for the governance of cyber security which allows executives and senior management to compare the organisation's cyber security measures against the established descriptions at a high level. When implemented, this provides an 'umbrella' under which other standards and guidance can fit to flesh out the results described.

As mentioned, PAS (Publicly Available Specification) 555:2013 – (Cyber security risk - Governance and management – Specification) provides a structured framework for managing the digital security of organisations. Whereas information security (ISO 27001) deals with information regardless of format, cybersecurity is concerned with protecting digital assets. That means any information processed, stored and transported by inter-networked information systems.

In contrast with the majority of many standards and sources of best practice that detail how to deliver effective cyber security (the how to), PAS 555 is different as it details what effective cyber security looks like (the what). The PAS 555 approach to cyber security allows organisations to choose how they achieve the specified outcomes, whether that be through the use of others standards such as ISO/IEC 27001, ISO/IEC 27031 or through the use of their own internal best practices.

The PAS 555 standard is dedicated to the issues of risk assessment, strategy formulation and compliance tracking; all of which are sub domains within the Governance domain. PAS 555 indicates high level business objectives within the main body of the text, supplemented by the identification of a relatively large number of indicative controls from other well-known cyber security standards.

PAS 555 applies to the whole organisation and its supply chain, avoiding the dangers that can arise when the security measures fail to cover the whole of the business. It is an adaptable approach which can apply to any organisation, whatever its size or type, whether commercial, not-for-profit or public sector.

In addition, PAS 555's flexibility allows an organisation to utilise its own defined processes or the adoption of other standards and management systems to achieve its intended cyber security ends. PAS 555 can be used alone, but is also compatible with many major security standards, such as ISO 20000-1, ISO 27001, ISO 22301 and ISO 31000.

[35] British Standards Institution, "PAS 555:2013:Cyber Security Risk. Governance and Management. Specification" (BSI, May 2013), https://shop.bsigroup.com/ProductDetail/?pid=000000000030261972.

4. Frameworks

4.1. Introduction

This section features standards that outline a method for doing a particular task relevant to cybersecurity. In many cases, this will refer to the management of various types of data (including personal data), but also protection of the infrastructure containing the data and methods for exchanging information with others hoping to prevent cyber-crime in their own organisations.

Each one lays out a procedure or process that teams, individuals, or management should follow or implement in order to optimally protect the data that they hold. Ensuring that this is done in a consistent and easily-completed way should ensure that the data remains safe.

4.2. Summary

Table 4-1 : Summary of standards in Section 4

Section	Standard(s)	Framework for…
4.3.1	ISO/IEC 24760	Identifying information
4.3.2	ISO/IEC 27001:2013	ISMSs (all aspects from establishing to reviewing)
4.3.3 4.7.4	ISO/IEC 27002:2013 ETSI TR 103 305-4 V1.1.1 (2016-08)	Security controls for ISMSs
4.3.4 4.5.6	ISO/IEC 27017 NIST SP 800-144	Security controls for Cloud services
4.5.2	NIST SP 800-53r4	Security controls for federal information systems
4.6.1 4.6.2	ITU-T X.810 and X.816	Security controls for open systems
4.7.2 4.7.3	ETSI TR 103 305 V1.1.1 (2015-05) and 305-3 V1.1.1 (2016-08)	Security controls (general)
4.3.9	ISO/IEC 29180	Security architecture for USNs
4.5.3	NIST SP 800-121	Bluetooth security
4.3.5 4.3.8 4.4.1 4.6.3	ISO/IEC 27018 and 29151 BS 10012:2009 ITU-T X.1171	Protection of PII
4.3.6 4.3.7 4.5.4 4.6.6	ISO/IEC 29100 and 29101 NIST SP 800-122 ITU-T X.1251	Privacy for PII
4.3.11 4.3.12	ISO 22301:2012 ISO 22313:2012	Business continuity following or in counter to a cyber-attack
4.3.10 4.5.1 4.5.8 4.8	ISO/IEC 31000:2018 NIST SP 800-37 and Framework for Improving Critical Infrastructure Cybersecurity PAS 555	Risk management

4.5.5	NIST SP 800-126	Management of SCAP content
4.5.7 4.6.4 4.6.5 4.7.1	NIST SP 800-150 ITU-T X.1206 and X.1209 ETSI TR 103 331 V1.1.1 (2016-08)	Exchange of cyber-threat information

4.3. International Standards Organisation (ISO)

4.3.1. ISO/IEC 24760-1:2011– Information Technology – Security Techniques – A Framework for Identity Management

This standard defines the key terminology for identity management and specifies the fundamental concepts and operational aspects of identity management. The document delivers a complete bibliography outlining various aspects of identity information management. Identity information management relates to governance, policies, processes, data, technology and standards which may include:

- *"Application(s) implementing an identity register;*
- *Authenticating the identity;*
- *Establishing provenance of identity information;*
- *Establishing the link between identity information and an entity;*
- *Maintaining the identity information;*
- *Ensuring integrity of the identity information;*
- *Providing credentials and services to facilitate authentication of an entity as a known identity;*
- *Mitigating the risk of identity information theft or misuse."*[36]

4.3.2. ISO/IEC 27001:2013 – Information Technology – Security Techniques – Information Security Management Systems – Requirements

ISO/IEC 27001:2013[37] outlines the requirements for establishing, implementing, operating, monitoring, reviewing an Information Security Management System (ISMS). Each organisation has a unique design and implementation plan for an ISMS, in line with the objectives, internal policy and security requirements.

The requirements are targeted at all kinds of organisations. ISO/IEC 27001:2013 promotes a risk assessment process for organisations to detect, study and address security risks. The document provides guidelines about:

- The context of the organisation
- Leadership
- Planning
- Support

[36] International Organisation for Standardisation, "ISO/IEC 24760-1:2011 Information Technology -- Security Techniques -- A Framework for Identity Management -- Part 1: Terminology and Concepts," December 2011, https://www.iso.org/standard/57914.html.
[37] International Organisation for Standardisation, "ISO/IEC 27001:2013 Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements," October 2013, https://www.iso.org/standard/54534.html.

- Operation
- Performance evaluation
- Improvement

The control categories in ISO/IEC 27001:2013 are directly derived from ISO/IEC 27002:2013 and include:

- *"Information security policies*
- *Organisation of information security*
- *Human resource security*
- *Asset management*
- *Access control*
- *Cryptography*
- *Physical and environmental security*
- *Operations security*
- *Communications security*
- *System acquisition, development and maintenance*
- *Supplier relationships*
- *Information security incident management*
- *Information security aspects of business continuity management*
- *Compliance"*[38]

The new controls introduced in ISO/IEC 27001:2013 are:

- *"Information security in project management*
- *Restrictions on software installation*
- *Secure development policy*
- *Secure system engineering principles*
- *Secure development environment*
- *System security testing*
- *Information security policy for supplier relationships*
- *Information and communication technology supply chain*
- *Assessment of and decision on information security events*
- *Response to information security incidents*
- *Availability of information processing facilities"*[39]

[38] International Organisation for Standardisation.
[39] International Organisation for Standardisation.

4.3.3. ISO/IEC 27002:2013 – Information Technology – Security Techniques – Code of Practice for Information Security Controls

ISO/IEC 27002:2013[40] provides guidelines for those responsible for choosing, implementing and managing information security. It is destined for organisations that plan to:

- choose controls within the process of implementing an ISMS;
- implement commonly approved information security controls;
- create their own information security management guidelines.

ISO/IEC 27000 is the only standard deemed necessary for the application of ISO 27002. ISO/IEC 27000 contains 35 security categories and lists 114 specific security controls in accordance to the industry's best practice, including these particular focus areas:

- Information Security Policies: provides management direction and support for information security.
- Organisation of Information Security: provides formal and detailed security mechanisms for the internal use in an organisation, for information processing and information sharing with third parties.
- Human Resource Security: offers security insights for the staff of the organisation.
- Asset Management: protects the assets of an organisations by identifying the valuable IT assets and granting them sufficient protection.
- Access Control: controls the access to information, mobile communications and network services and identifies illicit activities.
- Cryptography: Allow to protect data confidentiality, integrity and authenticity.
- Physical and environmental security: Stops unauthorised access, use, modification or destruction of data.
- Operations security: guarantees safe and successful data processing.
- Communications security: guarantees safe data exchange between parties.
- System acquisition, development and maintenance: enforces security controls into operations to protect the system's software and information.
- Supplier relationships: enforces security controls to protect internal organisational information and assets which are accessible by suppliers and ensures that the suppliers also deliver the adequate security.
- Information security incident management: implements mechanisms to identify and address information security incidents.
- Information security aspects of business continuity management: reduces the impact of on an incident on an organisation.
- Compliance: guarantees the respect of legal obligations and offers a complete audit process.

[40] International Organisation for Standardisation, "ISO/IEC 27002:2013 Information Technology -- Security Techniques -- Code of Practice for Information Security Controls," October 2013, https://www.iso.org/standard/54533.html.

4.3.4. ISO/IEC 27017:2015 – Information Technology – Security Techniques – Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services

ISO/IEC 27017:2015[41] is based on ISO/IEC 27002 and provides complementary support to address security threats and risks related to the use of cloud computing. The uniqueness of 27017 resides in its double approach, as it intended both for cloud service providers and cloud service users. The document delivers guidance to both parties and educates cloud service users on what they should expect from their cloud service providers.

ISO/IEC 27017:2015 provides cloud-related support on 37 of the controls in ISO/IEC 27002 but also introduces 7 additional control sets, summarised in the table 4-2 below.

Table 4-2 : Descriptions of control sets

Control set	Description
CLD.6.3.1	Defines the relationship between the cloud service customer and cloud service provider for information security management. Roles and responsibilities must be clearly defined, communicated and implemented by both parties.
CLD.8.1.5	Defines how the assets should be removed from the cloud if the cloud service customer terminates their contract with the cloud service provider.
CLD.9.5.1	Stipulates that the cloud service customer's virtual environment must be protected from other cloud service customers and third parties.
CLD.9.5.2	Stipulates that virtual machines found in a cloud computer environment are required to be hardened to respect the business needs.
CLD.12.1.5	States that the cloud service customer is required to document the administrative procedures and operations relevant to the cloud. In exchange, the cloud service provider is expected to provide documentation about critical operations and procedures upon the cloud service customer's request.
CLD.12.4.5	Defines the capabilities of a cloud service customer and of the cloud service provider relevant to the monitoring of cloud services.
CLD.13.1.4	Calls for thorough verification of the configuration of virtual networks in order to ensure its consistency with the cloud service provider's network security policy.

[41] International Organisation for Standardisation, "ISO/IEC 27017:2015 Information Technology -- Security Techniques -- Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services," December 2015, https://www.iso.org/standard/43757.html.

Additionally, ISO/IEC 27017 also discusses matters relevant to:

The roles and responsibilities

- Ambiguity regarding the roles and responsibilities of the cloud service customer and cloud service providers can lead to business or legal disputes, and severe loss in data. ISO/IEC 27017 indicates that for this reason, the roles and responsibilities of each party need to be clearly defined in order to avoid bad turns of events.

Security controls

- The standard provides the cloud service provider a way to communicate the level of security controls implemented. Independent evidence and certifications must be provided to the cloud service customer prior to signing a contract.

Cryptography

- The cloud service provider is expected to inform the cloud customer about how cryptography is being used and assist the customer with applying additional protection individually.

Customer relationship

- The standard highlights the importance of training for cloud service provider employees and partners in order to improve the quality of customer support.

Asset ownership

- ISO/IEC 27017 calls for the creation of an inventory of assets that are stored on the cloud and addresses the matter of secure disposal of customer assets.

4.3.5. ISO/IEC 27018:2014 – Information Technology – Security Techniques – Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors

ISO/IEC 27018:2014[42] establishes internationally-recognised objectives, control and guidelines for enforcing measures to protect personally identifiable information (PII) in accordance with ISO/IEC 29100. The publication allows certified cloud service providers to prove that they are complying to the best practices when processing PII under contract, protecting PII and only using it for the purposes which the cloud service customer has agreed to. The document offers support to organisations on how cloud providers can protect personally identifiable information. The standard seeks to:

- Support public cloud service providers to respect their obligations when handling PII;
- Contribute to the transparency of the public cloud personally identifiable information processors so that cloud service customers can choose well-managed cloud-based PII processing services.
- Support both the cloud service customer and the public cloud PII processor in achieving a contractual agreement.

[42] International Organisation for Standardisation, "ISO/IEC 27018:2014 Information Technology -- Security Techniques -- Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors," August 2014, https://www.iso.org/standard/61498.html.

- Offer tools to the cloud service customers to carry out audit and ensure that compliance rights are respected.

The standard provides a set of controls regarding:

1) Information security policies
2) Organisation of information security
3) Human resource security
4) Asset management
5) Asset control
6) Cryptography
7) Physical and environmental security
8) Operations and communications security
9) System acquisition, development and maintenance
10) Supplier relationships
11) Compliance
12) Information security aspects of business continuity management

As previously explained, the objective is that the cloud service provider, acting as PII processor, enables the cloud service client, acting as PII controller, to conform to its obligations. Additionally, these controls allow the PII processor to comply to their obligations. ISO/IEC 27018:2014 is applicable to all kinds of organisations, which deliver information processing services as PII processors through cloud computing to other organisations.

4.3.6. ISO/IEC 29100:2011 – Information Technology – Security Techniques – Privacy Framework

ISO/IEC 29100:2011[43] is a standard delivering a professional privacy framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems. Examples of PII include: First and last name, age, location, criminal record, banking information. The standard is destined to improve the existing security standards and to harmonise the requirements in the field of PII protection at the international level.

Despite the fact that there are already existing standards in the field of security (ISO 27001, ISO 27002 and ISO 27018, etc.), the purpose of ISO 29100:2011 is to focus particularly on the "processing" of PII. In this context, "processing" refers to the "operation or set of operations performed upon personally identifiable information (PII). Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymisation, pseudonymisation, dissemination or otherwise making available, deletion or destruction of PII."

The standard is particularly oriented towards organisations which seek to outline their privacy safeguarding requirements related to PII within an ICT by:

- "*specifying a common privacy terminology;*
- *defining the actors and their roles in processing PII;*

[43] International Organisation for Standardisation, "ISO/IEC 29100:2011 Information Technology -- Security Techniques -- Privacy Framework," December 2011, https://www.iso.org/standard/45123.html.

- describing privacy safeguarding requirements; and
- referencing known privacy principles."[44]

The aim of the standard

"Use of this International Standard will:
- aid in the design, implementation, operation, and maintenance of ICT systems that handle and protect PII;
- spur innovative solutions to enable the protection of PII within ICT systems; and
- improve organisations' privacy programs through the use of best practices."[45]

The privacy framework provided within this International Standard can serve as a basis for additional privacy standardisation initiatives, such as for:

- "a technical reference architecture;
- the implementation and use of specific privacy technologies and overall privacy management;
- privacy controls for outsourced data processes;
- privacy risk assessments; or
- specific engineering specifications."[46]

The actors of the privacy framework

The standard identifies four types of actors involved in the processing of the PII:

1) PII principals – defined as a "natural person to whom the personally identifiable information (PII) relates." This group of actors provides their PII for processing to PII controllers and PII processors
2) PII controllers – defined as a "privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes." This group of actors establishes the purpose and the means how PII processing takes place.
3) PII processors – defined as a "privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller." These actors execute the instructions obtained from the PII controllers, examine the privacy requirements and enforce the necessary privacy controls.
4) Third parties – defined as a "privacy stakeholder other than the personally identifiable information (PII) principal, the PII controller and the PII processor, and the natural persons who are authorised to process the data under the direct authority of the PII controller or the PII processor". A third party may act as a PII controller if it received the examined PII.

[44] International Organisation for Standardisation.
[45] International Organisation for Standardisation.
[46] International Organisation for Standardisation.

The 11 principles of ISO/IEC 29100

ISO/IEC 29100 establishes 11 privacy principles that the PII controller should adhere to. Indeed, these privacy principles seek to guarantee that "the privacy safeguarding requirements set for a specific PII principal, transaction, or scenario are addressed and consistently fulfilled."

1) *"Consent and choice*
2) *Purpose legitimacy and specification*
3) *Collection limitation*
4) *Data minimisation*
5) *Use, retention and disclosure limitation*
6) *Accuracy and quality*
7) *Openness, transparency and notice*
8) *Individual participation and access*
9) *Accountability*
10) *Information security*
11) *Privacy compliance"*[47]

It is important to note that not only can these principles be used as a tool to guide policy making in the field of privacy, but they can also serve as indicators in the monitoring and auditing process in an organisation.

4.3.7. ISO/IEC 29101:2013 – Information Technology – Security Techniques – Privacy Architecture Framework

ISO/IEC 29101:2013 uses the privacy framework foundations established in ISO/IEC 29100, targeted at organisations which seek to define their privacy safeguarding requirements, in relation to PII processed by any ICT system.

ISO/IEC 29101:2013 presents a complex architecture framework and related controls for the safeguarding of privacy in information and communication technology (ICT) systems that collect and process personally identifiable information (PII).

The architecture framework:

- "*provides a consistent, high-level approach to the implementation of privacy controls for the processing of PII in ICT systems;*

- *provides guidance for planning, designing and building ICT system architectures that safeguard the privacy of PII principals by controlling the processing, access and transfer of personally identifiable information; and*
- *shows how privacy enhancing technologies (PETs) can be used as privacy controls."* [48]

Furthermore, the architecture framework:

[47] International Organisation for Standardisation, 14.
[48] International Organisation for Standardisation, "ISO/IEC 29101:2013 Information Technology -- Security Techniques -- Privacy Architecture Framework," October 2013, https://www.iso.org/standard/45124.html.

- "*specifies concerns for ICT systems that process PII;*
- *lists components for the implementation of such systems; and*
- *provides architectural views contextualising these components."* [49]

The International Standard is intended as a technical reference and targeted at bodies and developers working with ICT systems that treat personally identifiable information.

ISO/IEC 29101 specifies that the actors involved in PII processing are the same as the ones described in ISO/IEC 29100, namely: the PII principal, the PII controller and the PII processor. The document analyses each of the three actors individually. It identifies the conditions for complying with the privacy principles of ISO/IEC 29100:

1) "Consent and choice
2) Purpose legitimacy and specification
3) Collection limitation
4) Data minimisation
5) Use, retention and disclosure limitation
6) Accuracy and quality
7) Openness, transparency and notice
8) Individual participation and access
9) Accountability
10) Information security
11) Privacy compliance"[50]

4.3.8. ISO/IEC 29151:2017 – Information Technology – Security Techniques – Code of Practice for Personally Identifiable Information Protection

This publication offers a set of controls for PII protection, in relation to the 11 privacy principles previously described in ISO/IEC 29100. The purpose of the standard is to allow organisations to establish a set of controls as part of their PII protection programme.

PII protection requires following a number of requirements. According to ISO/IEC 29151[51], the three principal sources of PII protection requirements should be:

- Legal, statutory, regulatory and contractual requirements related to protection of PII;
- Assessment of risks;
- Corporate policies.

Furthermore, organisations are required to identify principles, objectives and business requirements for processing PII. They should also identify and enforce controls to address the risks revealed by the risk impact process. Both the controls and treatments should be documented. Organisations may either select the controls provided by the document, or from other controls sets. The choice of controls varies from one organisation to another, and depends on the general risk

[49] International Organisation for Standardisation.
[50] International Organisation for Standardisation, 7.
[51] International Organisation for Standardisation, "ISO/IEC 29151:2017 Information Technology -- Security Techniques -- Code of Practice for Personally Identifiable Information Protection," August 2017, https://www.iso.org/standard/62726.html.

management approach, on the organisational decisions and on the organisation's role in the provision of infrastructure or services.

ISO/IEC 29151 contains an extended list of controls, divided into twelve categories, in accordance with the privacy principles established in ISO/IEC 29100. These controls categories are:

1) Consent and choice
2) Purpose legitimacy and specification
3) Collection limitation
4) Data minimisation
5) Use, retention and disclosure limitation
6) Accuracy and quality
7) Openness, transparency and notice
8) PII principal participation and access
9) Accountability
10) Information security
11) Privacy compliance

Additionally, ISO/IEC 29151 provides implementation guidance for the protection of PII on:

- Information security policies;
- Organisation of information security;
- Human resource security;
- Asset management;
- Access control;
- Cryptography;
- Physical and environmental security;
- Operations security;
- Communications security;
- System acquisition, development and maintenance;
- Supplier relationships;
- Information security incident management;
- Information security aspects of business continuity management;
- Compliance

4.3.9. ISO/IEC 29180:2012 – Information Technology – Telecommunications and Information Exchange Between Systems – Security Framework for Ubiquitous Sensor Networks

The main focus of ISO/IEC 29180:2012 are ubiquitous sensor networks (USN). A USN collects data from all types of sensors wirelessly and monitors the condition of the target objects in real time. It is made of three elements: a sensor network, a base station, and an application server. USN can be a valuable tool in the digital era and find applications in various fields, such as logistics, structural health monitoring, agricultural control, disaster management, and military. However, is also subject to possible security and privacy threats in transferring and storing data in the USN. ISO/IEC 29180 outlines the security threats and security requirements of the ubiquitous sensor network. It "categorises the security technologies according to the security functions that satisfy the said security requirements and where the security technologies are applied in the security model of

ubiquitous sensor networks." Furthermore, it introduces the security functional requirements and security technologies for the ubiquitous sensor networks.

ISO/IEC 29180:2012 lists the following threats in sensor networks:

- *"Destruction of information and/or other resources*
- *Corruption or modification of information*
- *Theft, removal, or loss of information and/or other resources*
- *Disclosure of information*
- *Interruption of services"*[52]

Furthermore, there are "many sensor node-specific threats such as sensor node vulnerability, eavesdropping, privacy of sensed data, denial of service attack, and malicious use of commodity network." [53]

General security requirements for USN

The following table 4-3 gives an overview of security measures listed in ISO/IEC 29180 destined to protect a sensor network or IP network from security threats.

Table 4-3 : General security requirements for USN

Type of measure	Description
Data confidentiality	A sensor network should not leak sensor readings to neighbouring networks. In many applications (e.g., key distribution), nodes communicate highly sensitive data. The standard approach for keeping sensitive data confidential is to encrypt the data with a secret key that only the intended receivers possess, thus ensuring confidentiality.
Data authentication/identification	Authentication mechanisms are mainly used to validate the legitimacy of the node so that its legitimacy and credibility are ensured.
Data integrity	In communication, *data integrity* assures the receiver that the received data is not altered in transit by an adversary.
Access control	Access control ensures that only the authorised user or entity is allowed to gain access to information, resource, or services.
Non-repudiation	Non-repudiation ensures that the entity or user cannot deny the activities in the network he/she has done.
Communication security	Communication security ensures that the information only flows from the source to the destination.
Availability	Availability ensures that information, service, and application are available to legitimate users anytime.
Privacy	Privacy ensures that the identifier of the user or entities and network usage is kept confidential.

[52] International Organisation for Standardisation, "ISO/IEC 29180:2012 Information Technology -- Telecommunications and Information Exchange between Systems -- Security Framework for Ubiquitous Sensor Networks," December 2012, https://www.iso.org/standard/45259.html.
[53] International Organisation for Standardisation.

Resilience of attacks	Resilience to attacks include resilience against compromised nodes, resilience against eavesdropping on routing information, etc.

Specific security functional requirements for USN

Additionally, the following table 4-4 presents the specific security function requirements for USN, as presented in ISO/IEC 29180.

Table 4-4 : Specific security functional requirements for USN[54]

Mandatory functional requirements
- *"The SN is required to support the data integrity and message authenticity of the sensed data.* - *The key management scheme in the SN is required to support the key pre-distribution scheme described in clause 10.1 of ISO/IEC 29180.* - *Key management is required to support both pair-wise key establishment and group-wise key establishment.* - *The SN is required to authenticate broadcast messages from a base station to all the sensor nodes and vice versa.* - *The SN is required to support secure routing protocols with message authentication, ID authentication, data freshness, and data integrity.* - *The SN is required to support the capability to be resilient against various attacks.* - *The base station in the SN is required to support the capability to mitigate the effects of DoS attacks from both wireless interface and wired interface.* - *The USN is required to support USN middleware security as described in clause 10.6 of ISO/IEC 29180.* - *The SN is required to support authentication/identification of the node by other nodes."*
Recommended functional specifications
- *"The SN is recommended to support a secure end-to-end encrypted data aggregation scheme.* - *The SN is recommended to support data freshness for sensed data.* - *The SN is recommended to support the confidentiality of sensed data.* - *Key management is recommended to support the pair-wise key establishment based on ID-based authentication.* - *The USN is recommended to support the mechanism for ensuring the privacy of the sensed data.* - *The base station is recommended to support tamper resistance to avoid a single point of failure."*
Optional functional specifications

[54] International Organisation for Standardisation.

- *"The sensor node or base station can optionally provide a secure hop-by-hop data aggregation scheme.*
- *The sensor node can optionally have a tamper resistant module for protecting credentials, sensed data, or other confidential data.*
- *The sensor node can optionally have tamper detection, tamper evidence, or tamper response.*
- *The SN can optionally have the capability to mitigate DoS attacks against the sensor node.*
- *The SN can optionally have the capability to access multiple or randomly selected base stations to mitigate large scale security threats due to single point of failure effects.*
- *The SN can optionally have the capability to mask asynchronous activity into synchronous messaging.*
- *The SN can optionally have the capability to provide multipath and/or randomised route selection to enhance resilience to attacks.*
- *The base station in the sensor network can optionally have the capability of intrusion detection.*
- *The SN can optionally have the capability to be configured to provide privacy protection."*

4.3.10. ISO/IEC 31000:2018 – Risk Management – Guidelines

This standard provides guidelines on managing risk in the context of an organisation. It introduces a common approach to addressing any type of risk, regardless of the industry or sector.

The use of ISO 31000:2018 can support the organisations to reach their objectives, detect opportunities and risks, and efficiently distribute and use resources for risk management. Although ISO 31000:2018[55] may not be used for certification purposes, it can be used to support audit programmes. Indeed, it may be used to compare management practices implemented by organisations with a globally approved benchmark.
The document provides guidelines about the risk management process, particularly regarding risk assessment, risk treatment, monitoring and review, and recording and reporting.

[55] International Organisation for Standardisation, "ISO 31000:2018, Risk Management – Guidelines," 2018, https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

4.3.11. ISO 22301:2012 – Business continuity management systems requirements

This standard specifies the requirements for setting up and managing an effective business continuity management system for any business, regardless of type or size. ISO 22301:2012[56] is associated with cybersecurity since the majority of Business continuity management plans document the prerequisites for any organisation that might suffer a cyberattack and experience service disruption.

Organisations should design a Business Continuity Management System (BCMS) which complies with legal, regulatory, organisational and industry requirements, the products and services, the processes employed, the size and structure of the organisation, and the requirements of its interested parties.

BCMS is a management system standard that specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. It is intended to be applicable to all organisations, or parts thereof, regardless of type, size and nature of the organisation.

The requirements specified in ISO 22301:2012 are generic and intended to be applicable to all organisations, or parts thereof, regardless of type, size and nature of the organisation. The extent of application of these requirements depends on the organisation's operating environment and complexity.

ISO 22313:2012 is the guidance document for ISO 22301.

4.3.12. ISO 22313:2012 – Business Continuity Management Systems Guidance

ISO 22313:2012[57] for business continuity management systems provides guidance based on good international practice for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a documented management system that enables organisations to prepare for, respond to and recover from disruptive incidents when they arise.

It is not the intent of ISO 22313:2012 to imply uniformity in the structure of a BCMS but for an organisation to design a BCMS that is appropriate to its needs and that meets the requirements of its interested parties. These needs are shaped by legal, regulatory, organisational and industry requirements, the products and services, the processes employed, the environment in which it operates, the size and structure of the organisation and the requirements of its interested parties.

ISO 22313 is generic and applicable to all sizes and types of organisations, including large, medium and small organisations operating in industrial, commercial, public and not-for-profit sectors that wish to:

[56] International Organisation for Standardisation, "ISO 22301:2012 Societal Security -- Business Continuity Management Systems -- Requirements," May 2012, https://www.iso.org/standard/50038.html.
[57] International Organisation for Standardisation, "ISO 22313:2012 Societal Security -- Business Continuity Management Systems -- Guidance," December 2012, https://www.iso.org/standard/50050.html.

- establish, implement, maintain and improve a BCMS;
- ensure conformance with the organisation's business continuity policy; or
- make a self-determination and self-declaration of compliance with this international standard.

4.4. British Standards Institution (BSI)

4.4.1. BS 10012:2009 – Specification for a Personal Information Management System

BS 10012:2009[58] provides a framework for maintaining and improving compliance with data protection legislation and good practice. It has been developed to help businesses to establish and maintain a best practice personal information management system that complies with the Data Protection Act 1998. The Data Protection Act, 1998 implements European Directive 95/46/EC, and sets out the rights individuals have over personal data, pertaining to themselves, which is held, processed or used by organisations.

Data needs to remain authentic, reliable and useable, while retaining its integrity. These characteristics of data can be preserved through the implementation of an effective information management systems. Without these characteristics data cannot be confidently reused, and there may be both short-term and long-term legal repercussions for mismanaging data. The policies, procedures, human and machine resources which constitute an information management system should ensure that the Confidentiality, Integrity and Availability — is maintained across an organisation's physical, personal and organisational layers.

1. Confidentiality ensures that data is only available to those authorised to access it
2. Integrity ensures that data can only be altered by authorised persons
3. Availability demands that authorised persons can access data when they require

It is important that UK curators of data, which includes any personal element, is familiar with the DPA, and engages in robust curation practices to ensure they remain within the law. The newly published standard BS 10012 recommends the implementation of a Personal Information Management System (PIMS) to ensure this, as part of an overall strategy for quality information management.

4.4.2. Publicly Available Standard (PAS) 555

[This standard features in Fundamentals, Frameworks, Evaluation, and Systems.]

PAS 555 maintains a strong emphasis on management buy-in and direction in order to deliver a cross-organisation security culture. It mentions that ownership of cybersecurity should be given at an 'appropriate' level of seniority but does not give an indication as to the likely role(s) involved. PAS 555 also mentions that a training strategy is required, but not what form this could take.

PAS 555 supplies a holistic framework for effective cybersecurity which not only considers the technical aspects, but also the related physical, cultural and behavioural aspects of an organisation’s approach to addressing cyber-threats, including effective leadership and governance.

[58] British Standards Institution, “BS 10012:2009 Data Protection. Specification for a Personal Information Management System,” May 2009, https://shop.bsigroup.com/ProductDetail/?pid=000000000030175849.

Through this approach, PAS 555 enables organisations to:

- focus investment in the most appropriate way, minimising potential losses and improving operational effectiveness and efficiency;
- develop organisational resilience by improving loss prevention and incident management;
- identify and mitigate cybersecurity risk throughout the organisation.

4.5. National Institute of Standards & Technology (NIST)

4.5.1. NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems

The NIST SP 800-37[59] guide outlines the main concepts to be implemented to the management of security risks to information systems. The document highlights planning and designing information security capabilities through the information systems' entire life cycle.

In the context of information systems, the publication promotes a risk-based management approach. The process counts on the active participation of staff members at all organisational levels. The document introduces a three-tiered approach to risk management:

- Tier 1: the organisation-level which consists in creating a coherent governance and risk management strategy.
- Tier 2: related to the mission and business process perspective of risk
- Tier 3: related to the information system perspective of risk

Information security requirements should be addressed throughout the system development life cycle. Early integration allows for cost-effective integration of improved information security systems.

The document specifies that organisations are required to start their risk management activities at an early stage of the life cycle to guarantee cost-efficiency. With the exception of continuous monitoring, the remaining risk management activities should be carried out before the system is placed into operation. A continuous monitoring strategy should be put into place to tackle the security risks.

[59] Joint Task Force Transformation Initiative, "NIST SP 800-37r1 - Guide for Applying the Risk Management Framework to Federal Information Systems : A Security Life Cycle Approach" (National Institute of Standards and Technology, June 2014), https://doi.org/10.6028/NIST.SP.800-37r1.

The particularity of the document is the Risk Management Framework, which outlines a detailed process on implementing information security and risk management tasks into the system development life cycle. The six steps are:

1) "Categorise the information system": security categorisation; information system description; information system registration
2) "Select the security controls": common control identification; security control selection; monitoring strategy; security plan approval
3) "Implement the security controls": security control implementation; security control documentation
4) "Assess the security controls": assessment preparation; security control assessment; security assessment report; remediation actions
5) "Authorise the information system": plan of action and milestones; security authorisation package; risk determination; risk acceptance
6) "Monitor the security controls": information system and environment changes; ongoing security control assessments; ongoing remediation actions; key updates; security status reporting; ongoing risk determination and acceptance; information system removal and disposal

The risk management framework is principally applied to Tier 3. Additionally, each step includes information about the stakeholder responsible for each task, the supporting roles involved, the phase of the system development life cycle, complementary implementation support and references.

4.5.2. NIST SP 800-53r4 – Security and Privacy Controls for Federal Information Systems and Organisations

NIST SP 800-53r4[60] seeks the assist the executive agencies of the US federal government with identifying and detailing security controls for organisations and information systems. These controls seek to guarantee the integrity, confidentiality and security of information systems. Additionally, the document:

- *"provides a set of information security program management (PM) controls that are typically implemented at the organisation level and not directed at individual organisational information systems;*
- *provides a set of privacy controls based on international standards and best practices that help organisations enforce privacy requirements derived from federal legislation, directives, policies, regulations, and standards;*
- *establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation within federal information systems, programs, and organisations."*

[60] National Institute of Standards and Technology, "NIST SP 800-53, Revision 4 Security and Privacy Controls for Federal Information Systems and Organisations," April 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

The security controls identified in the publication have been classified into the following eighteen categories:

1. Access Control
2. Audit and Accountability
3. Awareness and Training
4. Configuration Management
5. Contingency Planning
6. Identification and Authentication
7. Incident Response
8. Maintenance
9. Media Protection
10. Personnel Security
11. Physical and Environmental Protection
12. Planning
13. Program Management
14. Risk Assessment
15. Security Assessment and Authorisation
16. System and Communications Protection
17. System and Information Integrity
18. System and Services Acquisition

The security control structure is made of the following elements:

1) A control section
2) A supplemental guidance section
3) A control enhancements section
4) A references section
5) A priority and baseline allocation section

Indeed, the publication introduces the concept of security controls baselines which are intended to support organisation in accurately choosing the security controls for information systems, depending on whether they are classified as low-impact, moderate-impact or high-impact. These baselines address fundamental topics such as operational and functional needs, and the most recurring threats towards information systems. NIST SP 800-53r4 offers a tailored approach to assist organisations with selecting only the security controls relevant to their information systems and to their organisational context.

The tailored process consists of the following steps:

- *"Identifying and designating common controls in initial security control baselines*
- *Applying scoping considerations to the remaining baseline security controls*
- *Selecting compensating security controls, if needed*
- *Assigning specific values to organisation-defined security control parameters via explicit assignment and selection statements*
- *Supplementing baselines with additional security controls and control enhancements, if needed*
- *Providing additional specification information for control implementation, if needed."*

Organisations are expected to provide thorough documentation regarding the decisions taken during the control selection process. Documentation is essential to help managers make well informed organisational decisions.

4.5.3. NIST SP 800-121 Revision 2 – Guide to Bluetooth Security

NIST SP 800-121 Revision 2[61] addresses the Bluetooth security capabilities, discusses its vulnerabilities and offers recommendations to Bluetooth implementers and organisations which use Bluetooth technologies. The Bluetooth versions tackled by the document are versions 1.1, 1.2, 2.0 + Enhanced Data Rate (EDR), 2.1 + ED, 3.0 + High Speed (HS), 4.0, 4.1, and 4.2.

The second chapter of the publication provides an overview of Bluetooth wireless technology. Bluetooth is an open standard used for short-range radio frequency communication essentially used to establish wireless personal area networks (WPANs). Currently, Bluetooth is widespread across all sorts of IoT devices, including mobile phones, laptops, cars, keyboards, headsets, smart watches, home monitoring devices, etc. The Bluetooth technology enables a connection between these devices and the Internet. NIST identifies the four following benefits of using Bluetooth:

- Cable replacement
- Ease of file sharing
- Wireless synchronisation
- Internet connectivity
- Low-cost
- Low-power

Bluetooth security features are addressed in chapter 3. The publication introduced five security services which are specified in the Bluetooth standard:

- *"Authentication: verifying the identity of communicating devices based on their Bluetooth address Bluetooth does not provide native user authentication.*
- *Confidentiality: preventing information compromise cause by eavesdropping by ensuring that only authorised devices can access and view transmitted data.*
- *Authorisation: allowing the control of resources by ensuring that a device is authorised to use a service before permitting it to do so.*
- *Message integrity: verifying that a message sent between two Bluetooth devices has not been altered in transit.*
- *Pairing/bonding: creating one or more shared secret keys and the storing of these keys for use in subsequent connections to form a trusted device pair."*[62]

NIST SP 800-121 Revision 2 explains the security services proposed by Bluetooth and provides specifics regarding its security modes.

In chapter 4, the document explains that Bluetooth wireless technologies are vulnerable to threats such as denial-of-service attacks, eavesdropping, man-in-the-middle attacks, message modification, resource misappropriation, but also more specific types of attacks including bluesnarfing,

[61] John Padgette et al., "NIST SP 800-121r2 Guide to Bluetooth Security" (Gaithersburg, MD: National Institute of Standards and Technology, May 2017), https://doi.org/10.6028/NIST.SP.800-121r2.
[62] Padgette et al., 121.

bluejacking, bluebugging, car whisperer, denial of service, fuzzing attacks, pairing eavesdropping and secure simple pairing attacks. Such attacks may allow cyber-criminals to gain unauthorised access to personal or critical information. The publication notes that the organisations intending to use Bluetooth 4.0, 4.1, or 4.2 should examine the related security repercussions. Additionally, they should monitor the development of new security threats and vulnerability and suggest complementary security guidelines.

Finally, NIST SP 800-121 Revision 2 delivers a 37 point "Bluetooth security checklist". The checklist addresses management, technical and operational recommendations. The three main ideas to remember from the recommendations are:

- Always use the strongest Bluetooth security mode available;
- Bluetooth technologies should be tackled in security policies and default settings of Bluetooth IoT devices should be updated accordingly;
- Communicate the security-related responsibilities to the Bluetooth users.

4.5.4. NIST SP 800-122 – Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

NIST SP 800-122 focuses on the protection of the confidentiality of personally identifiable information (PII) in information systems. The document defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." The publication states that PII should be protected from unauthorised access, use and disclosure. The document serves as a practical guide for recognising types of PII and establishing the appropriate protection level. Furthermore, recommendations on how to address incidents involving PII are provided.

NIST SP 800-122 offers the following recommendations about PII protection to organisations:

1. Identify all PII withheld by the organisation or by any third party. Such information may include (but is not limited to):

   - *"Name, such as full name, maiden name, mother's maiden name, or alias*
   - *Personal identification number, such as social security number, passport number, driver's, license number, taxpayer identification number, patient identification number,*

   and financial account or credit card number
   - *Address information, such as street address or email address*
   - *Asset information, such as Internet Protocol (IP) or Media Access Control (MAC)*

   address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
   - *Telephone numbers, including mobile, business, and personal numbers*
   - *Personal characteristics including photographic image, x-rays, fingerprints, or other biometric image or template data*
   - *Information identifying personally owned property, such as vehicle registration number or title number and related information*

- *Information about an individual that is linked or linkable to one of the above"*[63]

2. Limit the use, collection and storage of PII to what is indispensable for the organisation to achieve their goals. In this regard, the document refers to the OECD's list of Fair Information Practices.

3. *Classify all the PII according to the confidentiality impact level.* This evaluation allows the organisation to determine relevant safeguards for PII. The PII confidentiality impact level represents the extent of the potential damage which could result in case of a PII breach. The confidentiality impact level can be classified as low, moderate or high. Organisations are responsible for establishing the criteria used to assess the confidentiality impact level and for enforcing the necessary policies and safeguards.

4. *Implement the suitable safeguards for PII depending on the PII confidentiality impact level.* The document recommends a variety of measures to protect PII, including operational safeguards, privacy-specific safeguards and security controls such as:

    - Developing appropriate policies and procedures to protect the privacy PII
    - Educating all individuals on security awareness and on the protection of PII before granting them the access to PII systems.
    - De-identifying information. "*The term de-identified information is used to describe records that have had enough PII removed or obscured, also referred to as masked or obfuscated, such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual".*
    - Minimise or refuse the access to PII from portable devices which are at higher security risk than non-portable devices.
    - Protecting the privacy of the transmitted information by using technologies, such as encryption.
    - Monitoring incidents that may breach the security of PII.

5. *Build an incident response plan to address PII breaches.* The plan should tackle practical aspects such as how the victims should be informed, how an attack should be reported and what necessary steps to undertake after the incident.

4.5.5. NIST SP 800-126 Revision 2 – The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2

In this publication, NIST focuses on the Security Content Automation Protocol (SCAP). SCAP represents a *"suite of specification for standardising the format and nomenclature by which information about software laws and security configurations is communicated, both to machines and humans"*[64]. The publication seeks to deliver the definitive technical specification for the version 1.2 of the Security Automation Protocol (SCAP) and outlines the conditions for creating and managing SCAP content.

[63] David Waltermire et al., "NIST SP 800-126, Revision 2 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2," September 2011, 66.
[64] David Waltermire et al., "NIST SP 800-126, Revision 2 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2," September 2011, 66.

SCAP version 1.2 includes the following component specifications which can be classified into five categories. The following table gives an overview of the categories and related specifications.

Table 4-5 : SCAP version 1.2. component specifications

Component category	Specification
Languages	➢ *"Extensible Configuration Checklist Description Format (XCCDF) 1.2, a language for authoring security checklists/benchmarks and for reporting results of evaluating them;* ➢ *Open Vulnerability and Assessment Language (OVAL) 5.10, a language for representing system configuration information, assessing machine state, and reporting assessment results;* ➢ *Open Checklist Interactive Language (OCIL) 2.0, a language for representing checks that collect information from people or from existing data stores made by other data collection efforts."*
Reporting formats	➢ *"Asset Reporting Format (ARF) 1.1, a format for expressing the transport format of information about assets and the relationships between assets and reports;* ➢ *Asset Identification (AI) 1.1, a format for uniquely identifying assets based on known identifiers and/or known information about the assets."*
Enumerations	➢ *"Common Platform Enumeration (CPE) 2.3, a nomenclature and dictionary of hardware, operating systems, and applications names;* ➢ *Common Configuration Enumeration (CCE) 5, a nomenclature and dictionary of software security configuration identifiers;* ➢ *Common Vulnerabilities and Exposures (CVE), a nomenclature and dictionary of security-related software flaw identifiers."*
Measurement and scoring systems	➢ *"Common Vulnerability Scoring System (CVSS) 2.0, a system for measuring the relative severity of software flaw vulnerabilities;* ➢ *Common Configuration Scoring System (CCSS) 1.0, a system for measuring the relative severity of system security configuration issues."*
Integrity	➢ *"Trust Model for Security Automation Data (TMSAD)."*

NIST offers a series of recommendations to organisations which make use of SCAP version 1.2. These recommendations include:

- Ensuring that the enforcement and use of SCAP version 1.2 respect the requirements outlined in each component and technical specification

- When creating SCAP content, organisations are asked to respect the specifications and security configurations outlined in NIST SP 800-126.

4.5.6. NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing

The publication addresses the security and privacy challenges encountered in the field of public cloud computing. NIST has partnered with members of the public and private sector to stimulate the safe adoption of cloud computing. In this document, NIST seeks to assist organisations to benefit from cloud computing, while being aware of the security and privacy issues at stake. For this reason, the publication presents guidelines on how to protect security and privacy when using a cloud provider.

NIST defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[65] In regards to cloud computing, NIST recommends that the organisations follow the guidelines below:

1. *"Carefully plan the security and privacy aspects of cloud computing solutions before engaging them."*

   Before starting using public cloud computing, organisations should carefully assess the sensitivity of their data, which will be transferred from an internal hosting service to an external infrastructure which may be subject to vulnerabilities and attacks. Careful planning allows to address the most important concerns and to ensure that resources are wisely allocated.

   Organisations are required to use a risk-based methodology to examine existing security and privacy solutions and take the decision of shifting to a cloud computing system. Furthermore, security and privacy must be continuously considered throughout the system life cycle. Since it is more difficult and costly to make tackle security and privacy once a system has been deployed, it is advised to address all the possible concerns at an early stage.

2. *"Understand the public cloud computing environment offered by the cloud provider."*

   Organisations should be clearly informed of the roles and responsibilities regarding cloud computing, and how they are relevant to security and privacy. It is advised to have the cloud provider's guarantees double-checked by external and independent assessment centres. Furthermore, organisations should be well acquainted with the policies and procedures, as well as the digital tools used by the cloud provider. Consistent monitoring is essential to minimise potential risks.

3. *"Ensure that a cloud computing solution satisfies organisational security and privacy requirements."*

[65] W Jansen and T Grance, "NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing" (Gaithersburg, MD: National Institute of Standards and Technology, 2011), https://doi.org/10.6028/NIST.SP.800-144.

Organisations should demand from the cloud provider that any public cloud computing solution that they use was tailored to meet their specific organisational policies and security requirements. It is advised to use negotiated service agreements in order guarantee a customer-based approach. A negotiated service agreement (as opposed to non-negotiable service agreements) shall address all organisational concerns in regards to security and privacy and document the guarantees provided by the cloud provider to answer these preoccupations. Prior to making any decision about shifting to a cloud computing service, organisations should carefully consider the costs and benefits of such action, and also be aware of the related risks and liabilities.

4. *"Ensure that the client-side computing environment meets organisational security and privacy requirements for cloud computing."*

   Organisations should review their security and privacy measures and take extra steps to secure the client side. Indeed, services from different cloud providers, web browsers, social media, webmail, applications, plug-ins and browser add-ons may be a source of security problems as well.

5. *"Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments."*

   Organisations should use suitable security management practices and controls with regards to cloud computing. Furthermore, they should monitor their information system assets and ensure that the security policies, procedures and guidelines are continuously updated to ensure optimal protection. Organisations are required to gather and study the data regarding the state of the system in order to address security concerns for each organisational level: governance level, mission or business process level and information systems level. Organisations are asked to maintain continuous monitoring of security networks and information in order to minimise security risks.

   Given that a share of the computing environment is exclusively in the hands of the cloud provider, it is advised to use a combination of qualitative and quantitative tools to perform risk analysis. The organisations should also verify that the security and privacy controls are properly executed and that they operate in a way that respect the organisational requirements.

   Third party audits are suggested to maintain a level of confidence between the organisation and the cloud service provider. In the case that the level of confidence is insufficient, the organisation should make the decision of turning down the service or accepting a greater degree of risk.

4.5.7. NIST SP 800-150 Guide to Cyber-Threat Sharing

In this publication, NIST addresses the dangers of cyber-attacks and underlines the necessity for organisations to share cyber-threat information and to cooperate with the rest of the community to enhance the situation. Cyber-threat information is defined as "any information that can help an

organisation identify, assess, monitor, and respond to cyber-threats"[66]. NIST argues that cyber-threat information sharing will allow organisations to gain better understanding of the topic, as well as leverage the know-how and collective experience of the community. The document seeks to provide guidelines to organisations that improve their cyber security and support them with the cyber-threat information management and sharing.

The publication identifies the following categories of threat information:

- *Indicators*, defined as "technical artefacts or observables that suggest an attack is imminent or is currently underway or that a compromise may have already occurred".
- *Tactics, techniques, and procedures* are used to depict an actor's behaviour. Indeed, "tactics are high-level descriptions of behaviour, techniques are detailed descriptions of behaviour in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique."
- *Security alerts* are defined as "human-readable, technical notifications regarding current vulnerabilities, exploits, and other security issues."
- *Threat intelligence reports* are "prose documents that describe TTPs, actors, types of systems and information being targeted, and other threat-related information that provides greater situational awareness to an organisation".
- *Tool configurations* are described as "recommendations for setting up and using tools that support the automated collection, exchange, processing, analysis, and use of threat information."

The main objective of the document is to promote cyber-threat information sharing both at an internal and external organisational level. Indeed, by communicating this kind of information, organisations obtain data that would not have had access to under difference circumstances. Consequently, they can learn from each other's practices and mistakes and improve the state of their internal security. The key benefits of cyber-threat information sharing are:

- *"Shared situational awareness*
- *Improved security posture*
- *Knowledge maturation*
- *Greater defensive agility"*[67]

In return, organisations also face the following challenges in regards to cyber-threat information sharing:

- *"Establishing trust*
- *Achieving interoperability and automation*
- *Safeguarding sensitive information*
- *Protecting classified information*
- *Enabling information consumption and publication*
- *Accessing external information*
- *Evaluation the quality of received information*
- *Complying with legal and organisational requirements*

[66] Christopher S. Johnson et al., "NIST SP 800-150 Guide to Cyber Threat Information Sharing" (National Institute of Standards and Technology, October 2016), https://doi.org/10.6028/NIST.SP.800-150.
[67] Johnson et al.

- *Limiting attribution"*[68]

NIST SP 800-150 offers the following list of advice regarding establishing cyber-threat sharing relationships:

- *"Define the goals and objectives of information sharing*
- *Identify internal sources of threat information*
- *Define the scope of information sharing activities*
- *Establish information sharing rules*
- *Join a sharing community*
- *Plan to provide ongoing support for information sharing activities"*[69]

Furthermore, the organisations are advised to include the following stakeholders in the process:

- *"Experienced cybersecurity personnel*
- *Members and operators of established threat information sharing organisations*
- *Trusted business associates, supply chain partners, and industry peers*
- *Personnel knowledgeable about legal issues, internal business processes, procedures, and systems"* [70]

The document argues that organisations should actively participate in an information sharing community and identifies the following activities that may be undertaken:

- *"Engage in ongoing communication*
- *Consume and respond to security alerts*
- *Consume and use indicators*
- *Organise and store indicators*
- *Produce and publish indicators"* [71]

Additionally, organisations are strongly encouraged to establish a plan which discusses information sharing infrastructure maintenance and user support. The plan should outline the human, physical and financial resources necessary to:

- Gather and study the information obtained from internal and external sources
- Obtain and implement security measures
- Obtain and implement a monitoring and threat detection mechanism

[68] Johnson et al.
[69] Johnson et al.
[70] Johnson et al.
[71] Johnson et al.

4.5.8. NIST – Framework for Improving Critical Infrastructure Cybersecurity

The purpose of NIST 2014 Cybersecurity Framework is to establish a set of industry standards and executable goals to assist organisations with cybersecurity risk management. The framework comprises three sections: the framework core, the framework implementation tiers and the framework profile. The document thoroughly details each section.

The Framework Core "*is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors*." [72] It is further broken down into:

- Functions: the five functions used to secure systems and respond to threats are "Identify, Protect, Detect, Respond, Recover".
- Categories: functions use classifications to identify specific tasks or challenges within them.
- Subcategories: further subgroups of these specific tasks or challenges.
- Informative references: documents such as existing standards, guidelines and practices relevant for each subcategory.

The Framework Implementation Tiers "provide context on how an organisation views cybersecurity risk and the processes in place to manage that risk." NIST identifies four tiers of implementation. Organisations are encouraged to take the necessary steps to move toward Tier 4. However, it is important to note that tiers should not be understood as maturity levels.

- Tier 1: Partial – organisations at tier 1 have not formalised their cybersecurity risk management practices and have limited awareness of cybersecurity risk at the organisational level.
- Tier 2: Risk informed – organisations at tier 2 have their risk management practices approved by the management but are not included into a comprehensive organisational policy. Organisations are aware of cybersecurity risks but require a broader cybersecurity approach.
- Tier 3: Repeatable. – organisations at tier 3 have their risk management practices formally approved and incorporated into policy. Organisations can repeatedly respond to crisis situations.
- Tier 4: Adaptive – organisations at tier 4 have fully adopted the Cybersecurity Framework. They can not only respond to threats but also predict them in advance and take the necessary preventive steps.

The Framework Profile "*represents the outcomes based on business needs than an organisation has selected from the Framework Categories and Subcategories. The profile can be characterised as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario."*[73] The use of multiple profiles can help an organisation identify vulnerabilities in cybersecurity.

Additionally, NIST identifies seven steps which could be used by an organisation in order to develop a new cybersecurity program or to build on the existing one.

[72] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity" (National Institute of Standards and Technology, February 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[73] National Institute of Standards and Technology.

- *"Step 1: Prioritise and scope*
- *Step 2: Orient*
- *Step 3: Create a Current Profile*
- *Step 4: Conduct a Risk Assessment*
- *Step 5: Create a Target Profile*
- *Step 6: Determine, Analyse, and Prioritise Gaps*
- *Step 7: Implement Action Plan"*[74]

4.6. International Telecommunication Union (ITU)

4.6.1. ITU-T X.810 Information Technology – Open Systems Interconnection – Security Framework for Open Systems: Overview

This international standard presents a framework within which security services for Open System are specified. Security frameworks tackle the use of security services in an Open Systems environment. They seek to define the ways of protecting systems and objects within systems, as well as interactions between systems. Furthermore, they provide foundations for standardisation, and a coherent vocabulary relevant to specific security requirements. Finally, they also classify the mechanisms which can be used to meet those security requirements.

The document is structured around the three following sections:

- The organisation of security frameworks
- The necessary security concepts in more than one part of the security frameworks
- The interactions between services and the mechanisms detected in the frameworks

Security frameworks are organised in seven parts. The document provides a definition of each of them and describes how the framework tackles each of them.

1) Overview
2) Authentication
3) Access control
4) Non-repudiation
5) Confidentiality
6) Integrity
7) Security audit and alarms

Furthermore, the document tackles the following concepts:

- Security information defined as "information needed to implement security services"
- Security domain defined as "a set of elements under a given security policy administered by a single security authority for some specific security-relevant activities"
- Security policy considerations for specific security services
- Trusted entities: "An entity is said to be a trusted entity for some classes of activity, in the context of a security policy, if the entity can violate the security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do."

[74] National Institute of Standards and Technology.

- Trust: "An entity X is said to trust an entity Y (for a set of activities) if and only if X relies upon Y behaving in a particular way with respect to the activities"
- Trusted third-parties defined as "a security authority or its agent that is trusted (in the context of a security policy) with respect to some security-relevant activities".

As far as the interactions between security mechanisms are concerned, the document specifies that in certain cases multiple security services are necessary for a single communication. In that case, either one security mechanism delivering several security services or multiple different security mechanisms can be applied. Vulnerabilities may arise in the situation when multiple security mechanisms are used at the same time, which then can be exploited by an attacker. Oftentimes, two security mechanisms can be mingled in many different ways. The vulnerabilities depend on the way that the mechanisms were combined. The publication further specifies that "when asymmetric cryptographic algorithms are used, an integrity or non-repudiation transformation should be applied to plaintext, and the resulting signed or sealed data should then be enciphered". Furthermore, the "use of confidentiality and integrity services in reverse order carries a risk that the integrity service will not be able to support non-repudiation. If all three services are desired, and the reverse order of integrity and confidentiality is necessary, then it is possible to apply two integrity mechanisms, one before the confidentiality mechanism and one after"[75].

4.6.2. ITU-T X.816 Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Security Audit and Alarms Framework

This international standard offers a model for managing security alarms and for carrying out security audit for open systems. The objective of security audit and alarms covered in the document is to guarantee that open system security related events are managed in respect of the security policy of the applicable security authority. ITU-T X.816:

1) *"defines the basic concepts of security audit and alarms;*
2) *provides a general model for security audit and alarms;*
3) *identifies the relationship of the Security Audit and Alarms service with other security services."*[76]

In order to support a security audit and alarm service, the following functions are required:

- *"the event discriminator*
- *the auditor recorder*
- *the alarm processor*
- *the audit analyser*
- *the audit trail examiner*
- *the audit provider*
- *the audit archiver*
- *the audit trail collector*

[75] International Telecommunications Union, "Recommendation X.810: Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Overview," November 21, 1995, http://www.itu.int/rec/T-REC-X.810-199511-I.
[76] International Telecommunications Union, "Recommendation X.816: Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Security Audit and Alarms Framework," November 21, 1995, https://www.itu.int/rec/T-REC-X.816-199511-I/en.

- *the audit dispatcher"*[77]

Security audit and alarm procedures may occur in the following phases;

- *"detection phase, in which a security-related event is detected*
- *discrimination phase, in which an initial determination is made as to whether it is necessary to record the event in the security audit trail to raise an alarm event in the security audit trail or to raise an alarm*
- *alarm processing phase in which a security alarm or security audit message may be issued*
- *analysis phase, in which a security-related event is evaluated together with, and in the context of previously detected events as logged in the audit trail, and a course of action determined*
- *aggregation phase, in which distributed security audit trail records are collected into a single security audit trail*
- *report generation phase, in which audit reports are built from security audit trail records*
- *archiving phase, in which records from the security audit trail are transferred to the security audit trail archive."*[78]

As far as the interaction with other security services, the following points can be noted:

- Entity authentication: Mutual authentication is necessary in the case of transfer of a security audit trail between an audit dispatcher and an audit collector.
- Data origin authentication is used in order to divulge the origin of security audit messages and security alarms.
- Access control tools need to be used during the storage and sharing of security audit trail records.
- Confidentiality services may be used during the transmission of the security audit trails and in order to protect stored audit records.
- Integrity may be used in order to detect any unauthorised modification of a security trail or any change to a security audit record.
- A non-repudiation service will usually not be used, given that the transmission of audit trails is usually carried out within the same security domain.

4.6.3. ITU-T X.1171 Threats and Requirements for Protection of Personally Identifiable Information in Applications Using Tag-Based Identification

This recommendation covers a number of important personally identifiable information (PII) breaches in the context of applications using tag-based identification. Furthermore, the document offers a structure of PII protection based on PII policy profile. The objectives of the publication are:

- *"To describe PII threats in a business-to-customer-based environment of applications using tag-based identification;*

[77] International Telecommunications Union.
[78] International Telecommunications Union.

- *To identify requirements for PII protection in a business-to-customer-based environment of applications using tag-based identification."*[79]

The ITU the following PII threats in a business-to-customer-based environment:

- "Leakage of information associated with the identifier": the attacker is able to retrieve data from the ID tag without the knowledge of the ID tag user of the tagged product. This type of infringement can be avoided by removing the ID tag or deactivating the ID tag functionality.
- "Leakage of the historical context data": the attacker may access the user's data such as preferences, habits, areas of interest, based on the historical background information linked with the ID tag. Furthermore, the attacker may use the PII for illicit purposes without the user's accord.

The ITU recommends the following requirements to protect PII for business-to-consumer applications using tag-based identification:

- *"control of PII by ID tag user and/or ID terminal user;*
- *authentication for ID tag user and/or ID terminal user;*
- *access control to the PII of an ID tag user in an application server;*
- *data confidentiality of information associated to an ID tag;*
- *consent for collection of PII;*
- *technical safeguards for the application servers."* [80]

4.6.4. ITU-T X. 1206 A Vendor-Neutral Framework for Automatic Notification of Security Related Information and Dissemination of Updates

The following recommendation offers a framework for automatic notification of security related information and dissemination of updates. Its particularity of this framework is its vendor-neutral nature. Indeed, after a product is registered, updates regarding the vulnerabilities information may be directly shared with the users or the relevant applications.

The document tackles the shortcomings of the existing update mechanisms in applications and operating systems:

- Updates need to be turned on by the users,
- Updates need to be authorised by the users
- System administrators are often unaware of the state of security within the networks and systems they are responsible for unless they set up monitoring tools
- Updates often fail to inform the users on how to use the products securely
- Distribution of updates also has flaws and may reduce the bandwidth
- Users do not have anyone to report any usage problems to
- It is often difficult to understand who is targeted by a newly released update

[79] International Telecommunications Union, "Recommendation X.1171: Threats and Requirements for Protection of Personally Identifiable Information in Applications Using Tag-Based Identification," February 20, 2009, https://www.itu.int/rec/T-REC-X.1171-200902-I/en.
[80] International Telecommunications Union.

Numerous vendors and organisations such as the Information Security Incident Response Team share vulnerability materials with concerned users. Nonetheless, the information is often unused or misunderstood. X.1206 points to the following uncertainties:

- *"Ambiguity of version notation*
- *The version of a given product cannot always be used as a criterion for determining what may actually be vulnerable*
- *Products that embed another vendor's products as components*
- *System administrators are unaware of the condition of assets under their responsibility"*[81]

The publication introduces a framework for the distribution of vulnerability, update and patch information. Its architecture is depicted in the Figure 4-1 below.

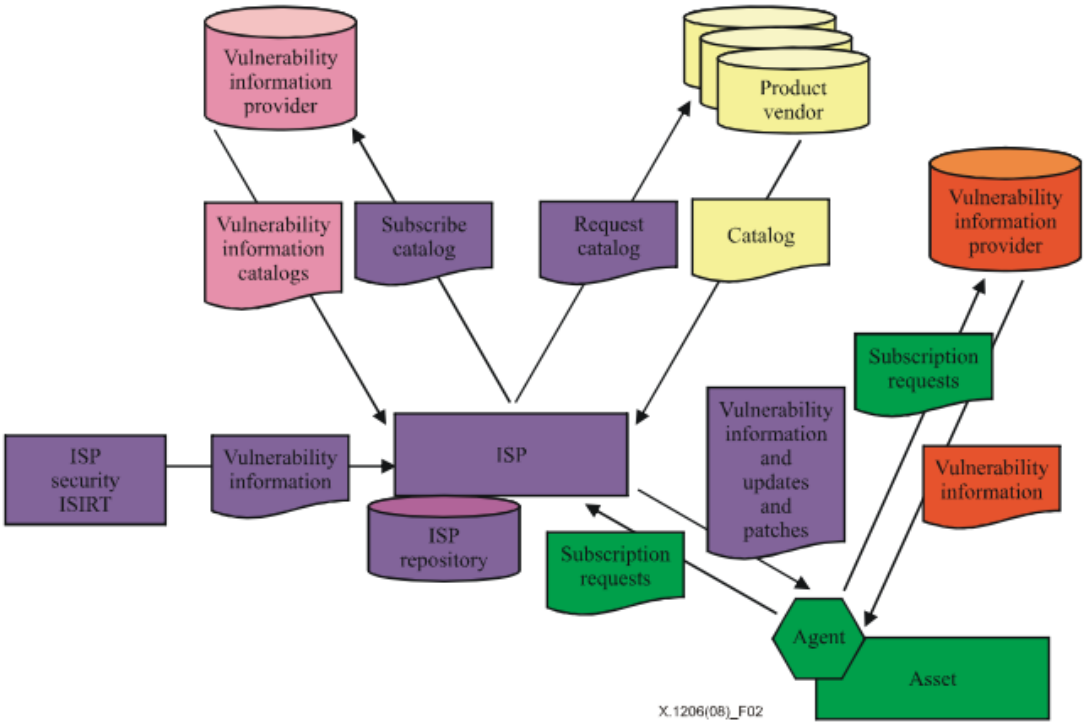

Figure 4-1 : Framework for the distribution of vulnerability, update and patch information[82]

Under this framework, any agent can ask or offer vulnerability information, updates and/or patches to another entity. Furthermore, users may subscribe to independent third-party sources for information updates and analyses.

It is advised to consider the following elements at the level of the architecture:

- Message core layer, which "provides platform/operating system/application/service (POAS) independent communication between compliant server and client applications built to platform/operating system/application/service independent dependent requirements".

[81] International Telecommunications Union, "Recommendation X.1206: A Vendor-Neutral Framework for Automatic Notification of Security Related Information and Dissemination of Updates," April 18, 2008, http://www.itu.int/rec/T-REC-X.1206-200804-I/en.
[82] International Telecommunications Union.

- Message/Application layer, which consists in "POAS independent processes or functions normally carried out during asset or device operations."
- Scalability, which "is supported via the topographical server/client identification architecture which supports a client of one server being a server to other clients below."
- Extensibility, according to which "new platforms, application, functions and services can be added simply by creating a scheme deriving from and extending this Recommendation's message core schema".
- Platform independence, according to which "any participating device can issue any specified message or request to any other participating device independent of the platform either device is implemented on."
- Client/Server communication (public protocol, server-client communication modes).

4.6.5. ITU-T X.1209 Capabilities and Their Context Scenarios for Cybersecurity Information Sharing and Exchange

The exchange of cybersecurity information about vulnerabilities within an organisation can be carried out fast. However, information exchange between organisations is still flawed and often lacks efficient communication. Efficient cybersecurity information exchange is important for cyber-threat prevention. For cybersecurity information to be efficiently exchange trusted and safe methods are required, as well as ways to guarantee privacy protection.

ITU-T X.1209[83] discusses the capabilities relevant for guaranteeing successful cybersecurity information sharing.

- Format/encoding capabilities
  - All parties involved need to comprehend the format and structure of the cybersecurity information.
  - Different types of security related information need to be shared.
  - Parties should provide different levels of security information.
  - All parties should understand the subject of the security information, which must also be recognisable.

- Transfer/exchange capabilities
  - All parties should have the possibility to share, provide and obtain security information globally.
  - Application are advised to sustain synchronous and asynchronous exchanges between the parties involved.
  - Applications should allow various forms of information delivery including push, pull and subscription.
  - Applications should guarantee steady operation throughout the exchange process.
  - Exchange protocols should be based on the ones commonly in use.

[83] International Telecommunications Union, "Recommendation X.1209: Capabilities and Their Context Scenarios for Cybersecurity Information Sharing and Exchange," December 17, 2010, https://www.itu.int/rec/T-REC-X.1209-201012-I/en.

- Security capabilities
    - Shared cybersecurity information should undergo authentication and verification.
    - All relevant parties should be recognisable through an authentication and verification process.
    - Applications must stop attacks stemming from forging and falsifying information or its source.
    - The concerned parties should make sure that the important information is only made available to the authorised parties. This task is particularly important for the source parties.
    - All parties should protect security information from unapproved intrusions.

- Policy capabilities
    - All the parties should outline their policy in use.
    - Parties should be able to deliver and access security information in respect with their security policy in use.
    - Parties should be able to specify the relevant jurisdiction for their policy.
    - Parties need to outline the restraints and extra requirements in regards to their policies.

- Vendor neutrality capabilities
    - Applications should deliver services in the most autonomous and neutral way possible.

4.6.6. ITU-T X.1251 A Framework for User Control of Digital Identity

This recommendation tackles the problem of privacy protection, which may be overlooked in the context of user information sharing between entities. Indeed, the parties involved are required to be in the possession of a prior business and privacy policy agreement. In order to address this issue, X.1251[84] offers a framework to improve user control when the user's digital related information is exchanged.

Identity management systems are highly vulnerable to cyber-threats. The biggest threat in this environment involve identity fraud and phishing.

The publication presents three layers for identity exchange:
- The application layer – an application operating on the Internet or a similar environment.
- The identity interchange layer: an interchange link to smoothen identity exchange between parties and grant the user complete control in implementing their privacy and security policies.
- The communication layer – an individual layer transmitting information across devices.

The framework design shares the following characteristics:
- Independent
- Pluggable
- Flexible
- Scalable

[84] International Telecommunication Union, "Recommendation X.1251 A Framework for User Control of Digital Identity," September 2009, https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9619.

The Figure 4-2 below represents the final product of the document, the digital identity interchange framework. The publication concludes with an accurate description of each component of the framework.

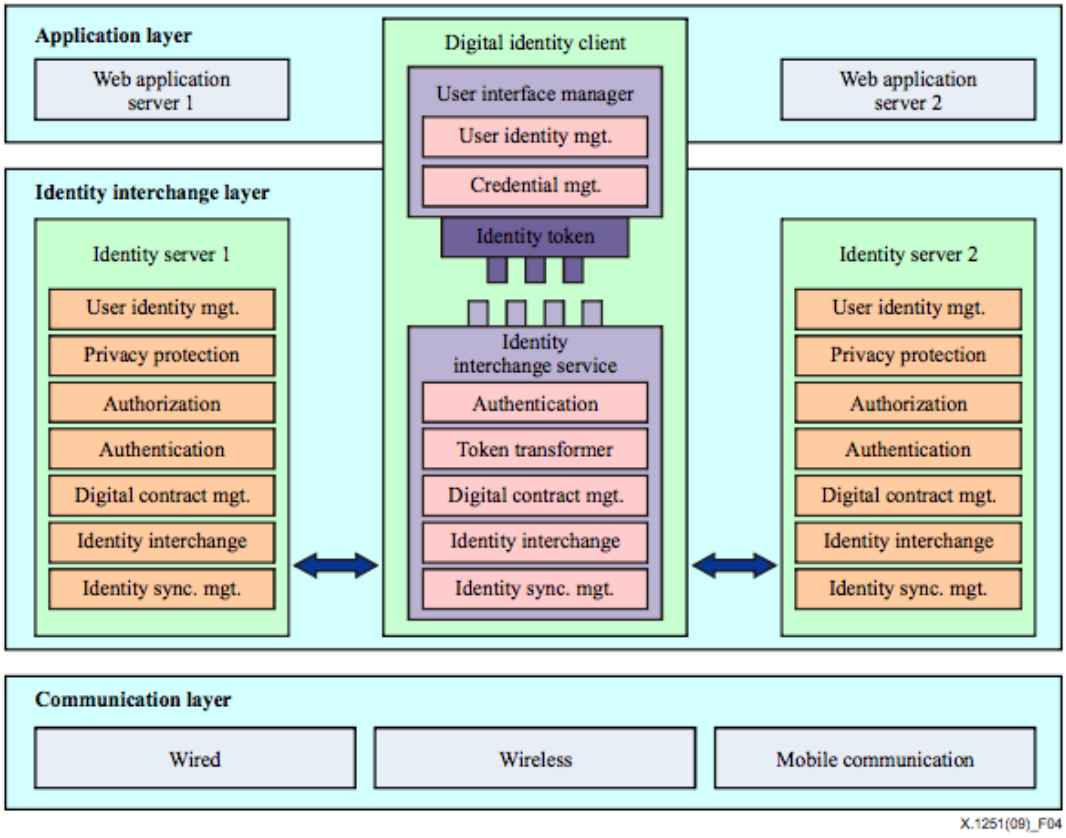

Figure 4-2 : Digital identity interchange framework[85]

[85] International Telecommunication Union.

4.7. European Telecommunications Standards Institute (ETSI)

4.7.1. ETSI TR 103 331 V1.1.1 (2016-08) CYBER; Structured Threat Information Sharing

The technical report covers the methods for describing and sharing cyber-threat information including adversary activity, contextual information, exploitation targets and courses of action, in a structured manner.

Currently, principle communities responsible for exchanging structured cyber-threat intelligence are the Financial Service Information Sharing and Analysis Centre (FS-ISAC) and The Depository Trust & Clearing Corporation (DTCC). The OASIS Technical Committee on Cyber-Threat Intelligence (TC CTI) is the largest standards activity and delivers information and protocols to address the need to analyse and share cyber-threat intelligence. OASIS has four active subcommittees:

- CTI STIX Subcommittee which seeks to "specify, characterise, and capture cyber-threat information";
- CTI TAXII Subcommittee which "defines a set of services and message exchanges that, when implemented, sharing of actionable cyber-threat information across organisation and product/service boundaries";
- CTI CybOX Subcommittee which "provides a common structure for representing cyber observables across and among the operational areas of enterprise cyber security that improves the consistency, efficiency, and interoperability of deployed tools and processes, as well as increases overall situational awareness by enabling the potential for detailed automatable sharing, mapping, detection, and analysis heuristics."
- CTI Interoperability Subcommittee which "helps guide adherence to CTI TC-promulgated standards and interoperability between CTI TC standards-based implementations, while encouraging standards maturity throughout the industry."

The IETF Managed Incident Lightweight Exchange Working Group (MILE) is another means for exchanging structured cyber-threat intelligence. MILE describes its function as:

> *"The Managed Incident Lightweight Exchange (MILE) working group develops standards to support computer and network security incident management; an incident is an unplanned event that occurs in an information technology (IT) infrastructure. An incident could be a benign configuration issue, IT incident, a system compromise, socially engineered phishing attack, or a denial-of-service (DoS) attack, etc. When an incident is detected, or suspected, there may be a need for organisations to collaborate. This collaboration effort may take several forms including joint analysis, information dissemination, and/or a coordinated operational response. Examples of the response may include filing a report, notifying the source of the incident, requesting that a third-party resolve/mitigate the incident, sharing select indicators of compromise, or requesting that the source be located. By sharing indicators of compromise associated with an incident or*

possible threat, the information becomes a proactive defence for others that may include mitigation options."[86]

The document also discusses the role of the CSIRT Gadgets Collective Intelligence Foundation (CIF), the EU Advanced Cyber Defence Centre (ACDC), AbuseHelper, OMG Threat Modelling Working Group, ITU-T SG17, Open Threat Exchange, OpenIOC Framework, VERIS Framework and ETSI ISI (Information Security Indicators) ISG in the structured threat information sharing.

4.7.2. ETSI TR 103 305 V1.1.1 (2015-05) CYBER; Critical Security Controls for Effective Cyber Defence

ETSI TR 103 305[87] presents 20 Critical Security Controls for effective cyber defence. For each Critical Security Control, the document provides:

- Evidence that the control is important blocks known attacks and an explanation how attackers exploit the absence of this control.
- A list of the actions taken by organisations to enforce, automate and assess the effectiveness of this control.

The 20 Critical Security Controls are:

1. Inventory of authorised and unauthorised devices
   This control is relevant because attackers are permanently scanning the address space of organisations, on the lookout for unprotected systems. This control is highly important for organisations allowing their members to bring their own devices and could be easily compromised.
2. Inventory of authorised and unauthorised software
   This control is relevant because attackers search for flawed or vulnerable software which can be exploited. Since attackers may disseminate hostile content, it is imperative to be aware of what software has been implemented in the organisation.
3. Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
   This control is essential because manufacturers and resellers configure the operating systems by prioritising the ease of deployment over security. For this reason, vulnerabilities may arise in the systems.
4. Continuous vulnerability assessment and remediation
   This control is essential because attackers exploit the security gaps newly identified by research teams.
5. Malware defences
   This control is critical because malware is constantly changing and at fast speed. Malware defences need to be effective in a dynamic environment.
6. Application software security

[86] European Telecommunications Standards Institute, "ETSI TR 103 331 CYBER; Structured Threat Information Sharing," August 2016, http://www.etsi.org/deliver/etsi_tr/103300_103399/103331/01.01.01_60/tr_103331v010101p.pdf.
[87] European Telecommunications Standards Institute, "ETSI TR 103 305 CYBER; Critical Security Controls for Effective Cyber Defence," May 2015, http://www.etsi.org/deliver/etsi_tr/103300_103399/103305/01.01.01_60/tr_103305v010101p.pdf.

This control is critical because attackers often exploit the vulnerabilities in web-based applications and software.

7. Wireless access control
   This control is critical because wireless devices are particularly vulnerable to cyber-attacks, since they do not require direct physical connection.
8. Data recovery capability
   This control is critical because attackers frequently modify data, configurations and software. Smooth data recovery is essential to mitigate an attack.
9. Security skills assessment and appropriate training to fill gaps
   This control is critical because the human factor and employee actions are often exploited by cyber attackers.
10. Secure configurations for network devices such as firewalls, routers and switches
    This control is critical the default configurations for network devices prioritise the ease of deployment rather than security. For this reason, network devices are exploited by attackers.
11. Limitation and control of network ports, protocols and services
    This control is important because attackers are on the lookout for remotely accessible network services which are easily exploitable, such as network ports, protocols and services.
12. Controlled use of administrative privileges
    This control is important because attackers primarily gain access to an organisation because of the incorrect use of administrative privileges.
13. Boundary defence
    This control is critical because attackers exploit the architectural and configuration vulnerabilities on perimeter systems, network devices and internet-accessing client machines to penetrate the organisation's system.
14. Maintenance, monitoring & analysis of audit logs
    This control is important because the absence of audit logs allows attackers to conceal their location and activities in the network.
15. Controlled access based on the need to know
    This control is critical because a number of organisations grant access to their users (and potentially malicious insiders) to more sensitive data than necessary.
16. Account monitoring and control
    This control is critical because attackers often exploit inactive user accounts to penetrate the organisation's system.
17. Data protection
    This control is critical because as organisations are shifting towards cloud computing and mobile access, it is essential to limit the risk of data loss and to guarantee encryption and integrity protection.
18. Incident response and management
    This control is critical because an efficient incident response is key to get through a cyber-attack.
19. Secure Network Engineering
    This control is critical because system or security designers seldom implement all the security features they might want. Furthermore, attackers continuously develop new methods to penetrate an organisation's system.
20. Penetration tests and red team exercises
    This control is critical because attackers can take advantage of the time gap between a vulnerability is identified and a defence plan is implemented. Defences should be regularly tested to identify and address security gaps in time.

4.7.3. ETSI TR 103 305-3 V1.1.1 (2016-08) CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations

The technical report offers guidelines on service sector Critical Security Control implementations, with a special focus on mobile device security and internet of things security.

With the increased use of mobile devices, including in the workplace, organisations are more exposed to cybersecurity risks. In order to address them, ETSI provides a series of recommendations to mitigate the risk including "not rooting or jailbreaking a device; only obtain apps from the device vendor or the organisation's app stores, not 3rd party stores; being wary of any app wanting to install a Profile on a mobile device, as well as if there is "Untrusted App Developer" popup for the app; and not leaving a device unlocked for longer periods of time." The standard also discusses the risks relevant to the IoT sector. Indeed, with the expansion of the internet of things and its application domains, Critical Security Controls also become applicable to the IoT networks. The standard delivers a total of 20 critical security controls for mobile device security, and then for IoT security, and discusses their applicability to mobile device security and IoT security respectively, as well as their relevant security challenges and considerations. The list of Critical Security Controls includes:

1. *"Inventory of authorised and unauthorised devices;*
2. *Inventory of authorised and unauthorised software;*
3. *Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers;*
4. *Continuous vulnerability assessment and remediation;*
5. *Controlled use of administrative privileges;*
6. *Maintenance, monitoring & analysis of audit logs;*
7. *E-mail and web browser protections;*
8. *Malware defences;*
9. *Limitations and control of network ports, protocols and services;*
10. *Data recovery capability;*
11. *Secure configurations for network devices such as firewalls, routers and switches;*
12. *Boundary defence;*
13. *Data protection;*
14. *Controlled access based on the need to know;*
15. *Wireless access control;*
16. *Account monitoring and control;*
17. *Security skills assessment and appropriate training to fill gaps;*
18. *Application software security;*
19. *Incident response and management;*
20. *Penetration tests and red team exercises."*[88]

4.7.4. ETSI TR 103 305-4 V1.1.1 (2016-08) CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms

[88] European Telecommunications Standards Institute, "ETSI TR 103 305-3 CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations," August 2016, http://www.etsi.org/deliver/etsi_tr/103300_103399/10330503/01.01.01_60/tr_10330503v010101p.pdf.

This technical report offers multiple facilitation mechanism guidelines for Critical Security Control implementations, including privacy impact assessment, mapping to cyber security frameworks, Cyber Hygiene programmes and management governance.

In the field of Privacy Impact Assessment, the standard recommends to:

- Define the objective of each Critical Security Control and motivate any occurring or possible intersection with privacy-sensitive information;
- Identify the legal bodies or policies which would allow, constrain or prevent the collection or usage of information by the Control;
- Identify the kind of information collected, used, shared or retained by the Control;
- Define the purpose for which the Control is using PII or protected data, and outline the manner in which the data is used;
- Create a security plan for the information system(s) supporting the Control;
- Determine if individuals should be informed about the implementation of the Control, the PII collected, the right to consent to the use of their information, and the right to decline to deliver information;
- Determine whether a data retention policy will be put in place;
- Outline the extent of the information sharing, internally but also with external parties, which support the Control;
- Create a mechanism which would allow individuals to notify and complain about any improper use of their information;
- Explain which technical and policy-based safeguards and security mechanisms may be required to support the Control.

As far as mapping to cyber security frameworks is concerned, the NIST Framework for Improving Critical Infrastructure Cybersecurity plays a central role. Indeed, the NIST Framework contains critical security controls, viewed as "Informative References", which can be used to drive implementation. In parallel, the standard suggests using a community-based approach to leverage the Framework.

The standard also addresses the topic of cyber hygiene programmes. Indeed, such campaigns support the implementation of the Critical Security Controls and contain a number of questions following the "Count, Configure, Control Patch, Repeat" logic, addressed to public and private sector officials. Such questions include:

- *"What is connected to their systems and networks?*
- *What software is running (or trying to run) on their systems and networks?*
- *Are their systems continuously managed using "known good" configurations?*
- *Is someone continuously looking for and managing "known bad" software?*
- *Do limits and tracking exist for the people who have the administrative privileges to change, bypass, or override security settings?"*[89]

[89] European Telecommunications Standards Institute, "ETSI TR 103 305-4 CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms," August 2016, http://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/01.01.01_60/tr_10330504v010101p.pdf.

5. Risk Management and Evaluation

5.1. Introduction

This section features standards that determine how well the cybersecurity systems and procedures have been put in place. These range from simple checks and stress tests to full audits of both physical systems and the processes that prevent cyber-crime through human error. It goes further and outlines standards and best practices for the organisations who are themselves conducting the checks and audits.

With the implementation of the procedures in place, a review of the adequacy of those procedures is a necessary part of ensuring that the relevant cybersecurity measures are in place.

5.2. Summary

Table 5-1 : Summary of standards in Section 5

Section	Standard(s)	Evaluation of…
5.3.1 5.3.2 5.3.3 5.4.3 5.8 5.7.1	ISO/IEC 15408 ISO/IEC 18043 SO/IEC 18045 NIST SP 800-115 IEC 62443-2-1:2010 COBIT 5	Security of IT products
5.4.2	NIST 800-53Ar4	Security of IT systems
5.3.4 5.4.1 5.5.1 5.9.1 5.10.3 5.11.1	ISO/IEC 27005 NIST SP/800-30r1 ITU-T X.1208 PAS 555 BSI-Standard 100-3 MAGERIT	Risk management (general)
5.3.7	ISO/IEC 27007:2011	ISMSs by means of an audit
5.6.1	ETSI TR 103 305_2 V1.1.1 (2016-08)	Security controls by means of an audit
5.3.7	ISO/IEC 29134	Impact on privacy
5.3.8	ISO/IEC 29190	Privacy systems
5.4.4	NIST SP 800-161	Risk management in supply chains
5.4.5	NIST IR 8062	Privacy risk management in federal systems
5.12.1	UPRAAM	User privacy online

5.3. International Standards Organisation (ISO)

5.3.1. ISO/IEC 15408:2009 - Information technology – Security techniques – Evaluation criteria for IT Security

ISO/IEC 15408:2009[90] enables comparing the findings of independent security evaluations. This is achieved through the use of a shared set of requirements regarding the security functionality of IT products implemented in hardware, firmware or software, and for assurance measures relative to these IT products in the context of a security evaluation.

This unique evaluation process allows to guarantee that both these IT products and the assurance measures relative to these IT products respect the specifications agreed upon in the standard. It is a useful tool for the consumers, in helping them to assess whether or not these IT products satisfy their security expectations.

Target of Evaluation

ISO/IEC 15408 uses the term "TOE" (Target of Evaluation) to describe the panel of IT products that are concerned by the evaluation. A TOE refers to software, hardware and/or firmware, possibly accompanied by guidance.

Examples of TOEs include:

- *"Software application;*
- *An operating system;*
- *A software application in combination with an operating system;*
- *A software application in combination with an operating system and a workstation;*
- *An operating system in combination with a workstation;*
- *A smart card integrated circuit;*
- *The cryptographic co-processor of a smart card integrated circuit;*
- *A Local Area Network including all terminals, servers, network equipment and software;*
- *A database application excluding the remote client software normally associated with that database application."*[91]

Target audience

The target audience of ISO/IEC 15408 comprises consumers, developers and evaluators. Consumers may find the findings of the security evaluations useful in assessing whether a TOE satisfies their security expectations. The standard is a useful tool for developers, which can use it to evaluate whether their own TOEs have met the relevant security requirements. Finally, evaluators can use ISO/IEC 15408 as an instrument defining how to undertake an evaluation, and as a foundation to make an opinion about the compliance of TOEs to their security requirements.

"Some of the additional interest groups that can benefit from information contained in ISO/IEC 15408 are:

[90] International Organisation for Standardisation, "ISO/IEC 15408-1:2009 Information Technology -- Security Techniques -- Evaluation Criteria for IT Security -- Part 1: Introduction and General Model," January 2014, https://www.iso.org/standard/50341.html.
[91] International Organisation for Standardisation.

a) *system custodians and system security officers responsible for determining and meeting organisational IT security policies and requirements;*
b) *auditors, both internal and external, responsible for assessing the adequacy of the security of an IT solution (which may consist of or contain a TOE);*
c) *security architects and designers responsible for the specification of security properties of IT products;*
d) *accreditors responsible for accepting an IT solution for use within a particular environment;*
e) *sponsors of evaluation responsible for requesting and supporting an evaluation; and*
f) *evaluation authorities responsible for the management and oversight of IT security evaluation programmes"*[92]

Evaluation

In order to verify whether a TOE meets the security requirements, it needs to undergo evaluation. Evaluation techniques can include, but are not limited to:

"a) analysis and checking of process(es) and procedure(s);
b) checking that process(es) and procedure(s) are being applied;
c) analysis of the correspondence between TOE design representations;
d) analysis of the TOE design representation against the requirements;
e) verification of proofs;
f) analysis of guidance documents;
g) analysis of functional tests developed and the results provided;
h) independent functional testing;
i) analysis for vulnerabilities (including flaw hypothesis);
j) penetration testing."[93]

"In ISO/IEC 15408, a Standard Target (ST)/Target of Evaluation (TOE) evaluation proceeds in two steps:

a) An ST evaluation: where the sufficiency of the TOE and the operational environment are determined;
b) A TOE evaluation: where the correctness of the TOE is determined. The TOE evaluation does not assess correctness of the operational environment.

The ST evaluation is carried out by applying the Security Target evaluation criteria (which are defined in SO/IEC 15408-3) to the Security Target. The precise method to apply the ASE criteria is determined by the evaluation methodology that is used.

The TOE evaluation is more complex. The principal inputs to a TOE evaluation are: the evaluation evidence, which includes the TOE and ST, but will usually also include input from the development environment, such as design documents or developer test results".

5.3.2. ISO/IEC 18043:2006 – Selection, Deployment and Operation of Intrusion Detection Systems

[92] International Organisation for Standardisation.
[93] International Organisation for Standardisation.

ISO/IEC 18043:2006[94] standard provides guidelines to assist organisations in selecting, deploying and operating intrusion detection systems (IDS). The National Institute of Standards and Technology (NIST), granted non-exclusive license to ISO/IEC to use the NIST Special Publication on Intrusion Detection Systems (SP800-31) in the development of the ISO/IEC 18043 International Standard. However, the NIST retains the right to use, copy, distribute, or modify the SP800-31 as they see fit.

Organisations should not only know when, if, and how an intrusion of their network, system or application occurs, they also should know what vulnerability was exploited and what safeguards or appropriate risk treatment options (i.e. risk transfer, risk acceptance, risk avoidance) should be implemented to prevent similar intrusions in the future.

Organisations should also recognise and deflect cyber-based intrusions. This requires an analysis of host and network traffic and/or audit trails for attack signatures or specific patterns that usually indicate malicious or suspicious intent. In order for an organisation to derive the maximum benefits from IDS, the process of IDS selection, deployment, and operations should be carefully planned and implemented by properly trained and experienced personnel. In the case where this process is achieved, then IDS products can assist an organisation in obtaining intrusion information and can serve as an important security device within the overall information and communications technology (ICT) infrastructure.

5.3.3. ISO/IEC 18045:2008 – Information Technology – Security Techniques – Methodology for IT Security Evaluation

ISO/IEC 18045:2008 outlines the minimum required steps to be undertaken by an evaluator in order to conduct an ISO/IEC 15048 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15048. Each evaluation, whether of protection profiles (PP) or standard targets (ST), follows the same model and involves four following steps:

- *"The input task: its purpose is to make sure that the evaluator is in possession of the right version of the evaluation evidence necessary for the evaluation process.*
- *The output task: its purpose is to deliver a description of the Observation Report and the Evaluation Technical Report.*
- *The evaluation sub-activities: the sub-activities vary depending on the type of evaluation.*
- *The demonstration of the technical competence to the evaluation authority task."*[95]

[94] International Organisation for Standardisation, "ISO/IEC 18043:2006 Information Technology -- Security Techniques -- Selection, Deployment and Operations of Intrusion Detection System," June 2006, https://www.iso.org/standard/35394.html.

[95] International Organisation for Standardisation, "ISO/IEC 18045:2008 Information Technology -- Security Techniques -- Methodology for IT Security Evaluation," August 2008, https://www.iso.org/standard/46412.html.

The standard develops the general evaluation model below:

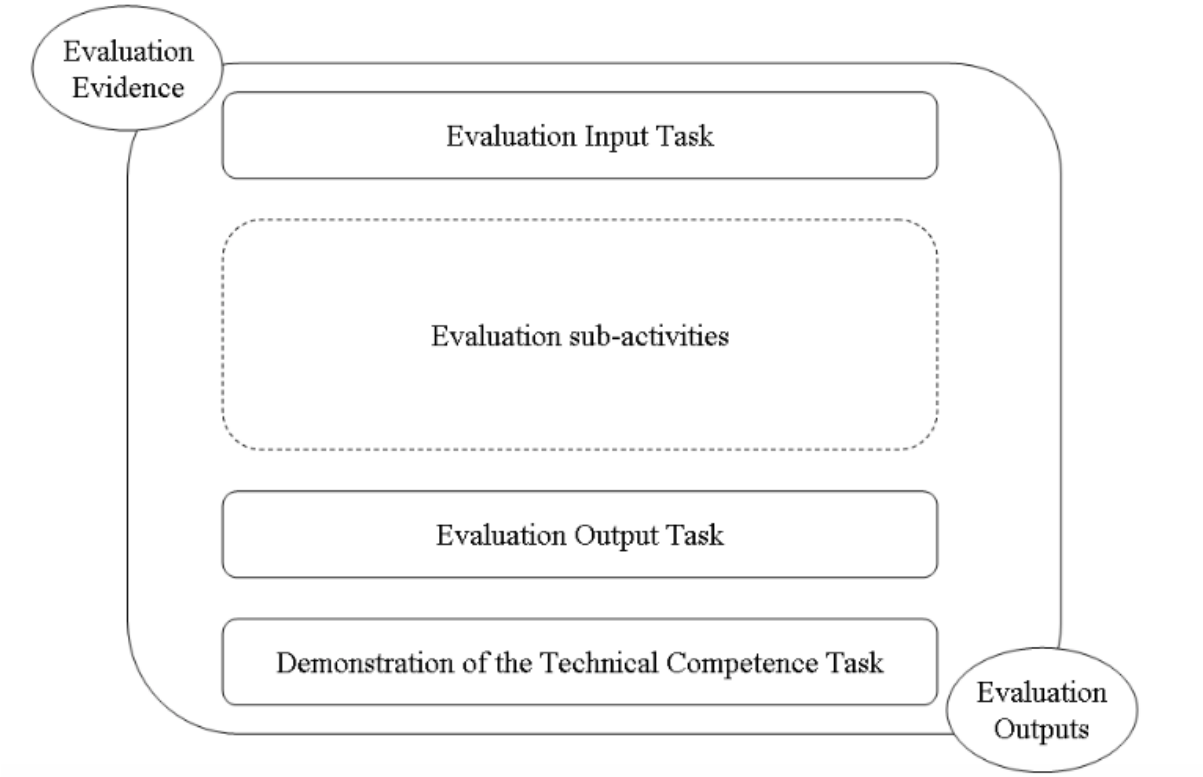

Figure 5-1 : ISO 18045 - General Evaluation Model (p.6)

Furthermore, ISO/IEC 18045 describes the roles of the four stakeholders involved in the evaluation process. The description of their responsibilities is found in the table below.

Table 5-2 : Stakeholders and Roles

Stakeholder	Role
Sponsor	*"Responsible for requesting and supporting an evaluation"*
Developer	*"Produces the TOE and is responsible for providing the evidence required for the evaluation on behalf of the sponsor"*
Evaluator	*"Performs the evaluation tasks required in the context of an evaluation: the evaluator receives the evaluation evidence from the developer on behalf of the sponsor or directly from the sponsor, performs the evaluation sub-activities and provides the results of the evaluation assessment to the evaluation authority."*
Evaluation authority	*"Establishes and maintains the scheme, monitors the evaluation conduct by the evaluator, and issues certification/validation reports as well as certificates based on the evaluation results provided by the evaluator."*

ISO/IEC 18045 delivers three possible verdicts to the evaluation:

- Conditions for a *pass* verdict are defined as "(1) *the constituent work units of the related evaluation methodology action, and; (2) all the evaluation evidence required for performing these work units is coherent, that is it can be fully and completely understood by the evaluator, and (3) all evaluation evidence required for performing these work units does not have any obvious internal inconsistencies or inconsistencies with other evaluation evidence."*
- Conditions for a *fail* verdict are defined as "*an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, ST, or TOE under evaluation are not met, or that the evidence is incoherent, or an obvious inconsistency in the evaluation evidence has been found"*;
- "*Verdicts are inconclusive and remain so until either a pass or fail is assigned*."[96]

5.3.4. ISO/IEC 27005 Information Technology – Security Techniques – Information Security Risk Management

This international standard offers guidelines for information security risk management through the creation of an information security management system (ISMS). This standard is based on an iterative perspective should be incorporated into an organisation's broader risk management policy. The standard describes the overall risk management process, including context establishment risk assessment, risk treatment, risk acceptance, risk communication and consultation, as well as risk monitoring and review. It is supplemented by six annex documents necessary for the set-up of a risk management method.

The risk management approach starts with context establishment. This approach requires to address the following:

- Establishing basic criteria such as the risk management approach, risk evaluation criteria, impact criteria and risk acceptance criteria;
- Outlining the perimeter and the limits of the risk management process;
- Outlining the stakeholders and their roles for information security risk management.

Risk assessment involves:

- *Risk identification* which seeks to identify and analyse sources of potential loss: the assets, the threats, the existing controls, the vulnerabilities, the consequences that a loss may have on the assets
- *Risk analysis/estimation* which comprises the choice of a risk methodology (qualitative, quantitative or both), the assessment of the business impact that may result from information security occurrences, the assessment of the likelihood of such event, the assessment of the risk level for each relevant case scenario.
- *Risk evaluation* which seeks to compare levels of risk against risk evaluation criteria and risk acceptance criteria.

[96] International Organisation for Standardisation.

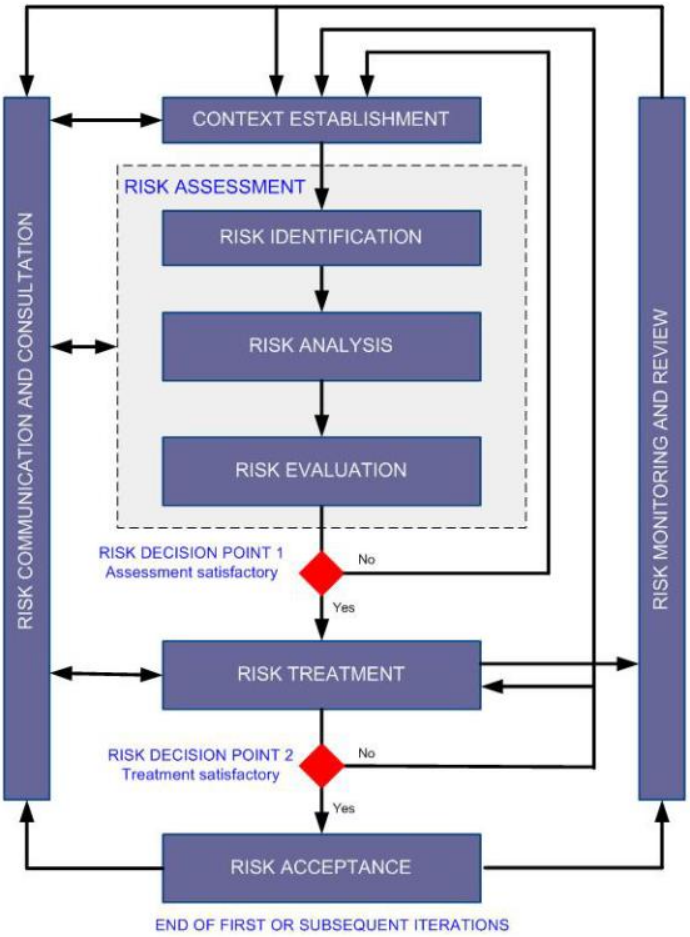

Figure 5-2 : Information security risk management process[97]

The standard summarises the information risk management process as shown in the Figure 5-2 above. Based on the outcome of the risk assessment process, risk treatment will be carried out. ISO/IEC 27005:2011 identified four options for risk treatment:

- Risk modification: Reducing the level of risk by introducing, removing or altering controls so that the residual risk becomes acceptable;
- Risk retention: Accepting the risk without further action;
- Risk avoidance: Withdraw from an activity that is at the core of the risk;
- Risk sharing: Share the risk with another stakeholder who can manage the risk.

After a satisfactory accomplishment of the risk treatment, the residual risks should be accepted by responsible managers. In the case where the accepted residual risk is higher than the previously establish risk acceptance criteria, a documented explanation should be provided. The document also stresses that risk communication should be continuously carried out between the decision-makers and parties involved. Risk monitoring and review is also a crucial step in order to identify potential threats and vulnerabilities.

[97] International Organisation for Standardisation, "ISO/IEC 27005:2011 Information Technology -- Security Techniques -- Information Security Risk Management," June 2011, https://www.iso.org/standard/56742.html.

5.3.5. ISO/IEC 27006:2015 – Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems

ISO/IEC 27006:2015[98] describes the requirements and provides support for accreditation bodies in charge of auditing and certification of an information security management system (ISMS) of type ISO 27001. The requirements outlined in this standard, as well as in ISO/IEC 17021-1 and ISO 19011 need to be demonstrated in terms of capability and reliability by any organisation delivering ISMS certification. The guidance offered in this standard provided further interpretation of these requirements. The certification process includes auditing the management system for respecting ISO/IEC 27001.

The key elements addressed by ISO/IEC 27006:2015 offers clarifications for the ISO 27001 audits including:

- A classification of security measures (organisational and technical);
- The types of checks on technical security measures to be conducted;
- The duration (in days) of an audit

The requirements in the context of ISMSs, covered by the publication take the following forms:

- General requirements: these requirements cover legal matters, impartiality management and liability and financing.
- Structural requirements: are identical to ISO/IEC 17021-1, 6.
- Resource requirements: requirements regarding the competence of personnel, the personnel involved in the certification activities, conditions for the use of external personnel, personnel records and outsourcing.
- Information requirements: includes requirements regarding public information, certification documents, referencing, confidentiality and information exchange.
- Process requirements: these requirements address the pre-certification activities, planning audits, initial certification audit, conducting audits, certification process details, complaints and client records.
- Management system requirements for certification bodies.

5.3.6. ISO/IEC 27007:2011 – Information Technology – Security Techniques – Guidelines for Information Security Management Systems Auditing

ISO/IEC 27007:2011 delivers guidance on managing an information security management system (ISMS) audit programme, on carrying out the audit process and on the competency of ISMS auditors, in complementation to ISO 19011.

The document recommends the use of ISO 19011 to the ISMS context and makes a number of new contributions about managing an audit process, performing an audit and offers additional comments about the competence and evaluation of auditors.

Regarding the managing of an audit process, ISO/IEC 27007:2011 provides guidelines about the manner in which audit programme objectives should be established, as well as about how the scope

[98] International Organisation for Standardisation, "ISO/IEC 27006:2015 Information Technology -- Security Techniques -- Requirements for Bodies Providing Audit and Certification of Information Security Management Systems," October 2015, https://www.iso.org/standard/62313.html.

of the audit programme should be determined. Indeed, factors which may have an impact on the scope of the audit programme include:

- *"The size of the ISMS;*
- *The complexity of the ISMS;*
- *The gravity of the information security risks identified for the ISMS;*
- *The importance of information and related assets within the scope of the ISMS;*
- *The complexity of the information systems to be audited on site;*
- *Whether there are many similar sites;*
- *The variations in ISMS complexity across the sites in scope."*[99]

The standard also covers the manner in which audit objectives should be defined and illustrates the recommendation with examples of audit criteria.

Additionally, ISO 27007 provides guidelines on how an audit should be performed. The contribution to this section discusses how the feasibility of the audit should be determined. Before the audit commences, the auditor needs to evaluate whether the audit may be carried in the absence of any ISMS records deemed unavailable or confidential by the auditee. In case that the task is unfeasible without these ISMS records, alternative arrangements need to be agreed upon to carry out the audit.

Finally, on the topic of the competence and evaluation of auditors, the document states that when determining auditor competence to meet the requirements of the audit programme, the following points should be examined:

- *"complexity of the ISMS (e.g. criticality of information systems, risk situation of the ISMS);*
- *the type(s) of business performed within the scope of the ISMS;*
- *extent and diversity of technology utilised in the implementation of the various components of the ISMS (such as the implemented controls, documentation and/or process control, corrective/preventive action, etc.);*
- *number of sites;*
- *previously demonstrated performance of the ISMS;*
- *extent of outsourcing and third-party arrangements used within the scope of the ISMS;*
- *the standards, legal requirements and other requirements relevant to the audit programme."*[100]

The standard also mentions that the auditors are required to be competent in the fields of:

- information security management methods;
- information technology and information security techniques;
- current information security threats, vulnerabilities and controls, as well as the larger context for the ISMS.

[99] International Organisation for Standardisation, "ISO/IEC 27007:2011 Information Technology -- Security Techniques -- Guidelines for Information Security Management Systems Auditing," November 2011, https://www.iso.org/standard/42506.html.
[100] International Organisation for Standardisation, "ISO/IEC 27006:2015 Information Technology -- Security Techniques -- Requirements for Bodies Providing Audit and Certification of Information Security Management Systems."

5.3.7. ISO/IEC 29134:2017 – Security Techniques – Guidelines for Privacy Impact Assessment

ISO/IEC 29134:2017[101] is an international standard which delivers guidelines for carrying out a Privacy Impact Assessment (PIA) and for establishing the structure and content of the Privacy Impact Assessment report. It is applicable in various situations involving PII processing, including:

- Identifying the causes, risks and responsibilities related to privacy;
- Providing guidelines to protect PII in the project design phase (also called privacy by design);
- Limiting the risk related to PII processing.

The document covers in detail the process for conducting a privacy impact assessment. The process requires:

- Determining whether a PIA is indispensable;
- Preparing the PIA:
    - building the PIA team and formulating the scope of the PIA;
    - preparing a plan and allocating resources for the PIA;
    - describing the object of the assessment;
    - engaging with stakeholders.
- Performing the PIA:
    - identifying information flows of PII;
    - studying the consequences of the use case;
    - identifying privacy safeguarding requirements;
    - assessing privacy risk;
- Following up the PIA:
    - preparing the report;
    - publishing the report;
    - enforcing privacy risk treatment plans;
    - reviewing and/or auditing the PIA.

ISO/IEC 29134:2017 specifies that the content of the PIA report depends greatly on the nature of PII being process, as well as on the scope and objectives of the PIA. Organisations are responsible for identifying the adequate audience for the report and its degree of confidentiality. Furthermore, the following elements should be addressed by the organisation:

- *"The report structure;*
- *The scope of the assessment;*
- *The privacy requirements;*
- *The risk assessment;*
- *The risk treatment plan;*
- *The conclusion and decisions taken on the basis of the outcome of the PIA;*
- *A PIA public summary to inform PII principals about the level of risk associated with the programme, information system, and the process implemented in which their PII will be involved."*[102]

[101] International Organisation for Standardisation, "ISO/IEC 29134:2017 Information Technology -- Security Techniques -- Guidelines for Privacy Impact Assessment," June 2017, https://www.iso.org/standard/62289.html.
[102] International Organisation for Standardisation.

5.3.8. ISO/IEC 29190:2015 – Information Technology – Security Techniques – Privacy Capability Assessment Model

The purpose of ISO/IEC 29190:2015[103] is to assist organisations with professional support about how to estimate the level of their capability to administer privacy-related processes. The standard is oriented towards the efficiency and effectiveness of privacy-related processes used by organisations.

Privacy-related management guidance is characterised as follows:

- "*The decision support information useful to a senior executive in formulating and executing a privacy strategy is different from the decision support useful to operational and line-of-business staff even though their various activities might all ultimately be directed towards the same goal;*
- *There are likely to be multiple "privacy stakeholders" (that is, parties who have an interest in the way the organisation manages privacy). Those stakeholders might impose very different requirements, for example, driven by legal and regulatory compliance requirements, but also by inter-related "good practice" provisions stipulated, for example, by policies, codes-of-conduct, business risk assessments, audit findings, reputational, and/or financial imperatives and/or personal privacy preferences."*[104]

Concretely, ISO/IEC 29190:2015:

- *"specifies steps in assessing processes to determine privacy capability,*
- *specifies a set of levels for privacy capability assessment,*
- *provides guidance on the key process areas against which privacy capability can be assessed,*
- *provides guidance for those implementing process assessment, and*
- *provides guidance on how to integrate the privacy capability assessment into organisations operations."*

According to ISO/IEC 29190, the evaluation of an organisation's privacy-related abilities is required to respect the following requirements:

- *"It needs to provide the organisation with information which is useful to the appropriate level or levels of management;*
- *It needs to cater for the fact that "capability" needs to be assessed in many different domains (legal compliance, risk management, reputation, and so on)."*[105]

ISO/IEC 29190 is destined both for professionals in charge of directing, managing, and operating an organisation's privacy management abilities, and for individuals responsible for advising the related stakeholders.

The document intends to help organisations with producing the following results:

[103] International Organisation for Standardisation, "ISO/IEC 29190:2015 Information Technology -- Security Techniques -- Privacy Capability Assessment Model," August 2015, https://www.iso.org/standard/45269.html.
[104] International Organisation for Standardisation.

[105] International Organisation for Standardisation.

- *"an overall "score" against a simple capability assessment model;*
- *a set of metrics indicating assessment against key performance indicators;*
- *the detailed outputs from privacy process management audits and management practices for input into improving capability in these specific areas."* [106]

The capability assessment model helps an organisation to position its processes on the following capability scale:

Table 5-3 : Capability assessment scale

Level	Description
Level 0	Incomplete process: the process is not implemented, or fails to achieve its process purpose
Level 1	Performed process: the implemented process achieves its process purpose
Level 2	Managed process: the implemented process is implemented in a managed fashion and its work products are appropriately established, controlled and maintained
Level 3	Established process: the managed process is implemented using a defined process capable of achieving its process outcomes
Level 4	Predictable process: the established process operates within defined limits to achieve its process outcomes
Level 5	Innovating process: the predictable process is continuously improved to respond to change aligned to organisational goals

Furthermore, each of the capabilities relevant to the target privacy capability level should be rated. The extent of achievement of a capability is evaluated on the following scale:

Table 5-4 : Achievement of a capability scale

Scale	Description
Not achieved (0-15%)	*"There is little or no evidence of achievement of the defined capability in the assessed process."*
Partially achieved (>15%-50%)	*"There is some evidence of an approach to, and some achievement of, the defined capability in the assessed process. Some aspects of achievement of the capability may be unpredictable."*
Largely achieved (>50%-85%)	*"There is evidence of a systematic approach to and significant achievement of, the defined capability in the assessed process. Some weaknesses related to this capability may exist in the assessed process."*
Fully achieved (>85%-100%)	*"There is evidence of a complete and systematic approach to and full achievement of the defined capability in the assessed process. No significant weaknesses related to this capability exist in the assessed process."*

[106] International Organisation for Standardisation.

Completing the analysis and evaluation of the privacy-related processes of an organisation allows to identify proposals for improvement processes, which seek to:

- *"improve the processing of PII;*
- *ensure the transparency of processing of PII;*
- *decrease development and maintenance costs of systems that manage PII;*
- *reduce the risk of breaches of privacy;*
- *improve the processes for dealing with privacy breaches."*[107]

The final step involves making relevant modifications in order to enhance the capability based on the existing capabilities.

5.4. National Institute of Standards & Technology (NIST)

5.4.1. NIST SP 800-30r1 – Guide for Conducting Risk Assessments

Information systems are targeted by important threats which may compromise the integrity of an organisation or an individual. Such threats may include intentional attacks, environmental disturbances, human/machine error and structural failures, all of which can severely impact the safety and economy of a nation. In this context, information security risk management becomes of crucial importance. Special Publication 800-30 is targeted at diverse group of risk management professionals and provides an overview of the nine risk assessment steps outlined by the US National Institute of Standards and Technology (NIST) used to characterise, estimate and rank risks. The purpose of such evaluations is to assist decision-makers and support risk responses. Risk assessments may be carried out at all three levels in the risk management structure including the organisation level, the mission/business process level and the information system level.

[107] International Organisation for Standardisation.

Special Publication 800-30[108] offers a detailed four step risk assessment process for organisations. The Table 5-5 below gives an overview of the main risk assessment steps and of their relevant sub-tasks:

Table 5-5 : Risk assessment steps

Main risk assessment steps	Sub-tasks
1. *Prepare* for risk assessments	- *"Identify the purpose of the assessment* - *Identify the scope of the assessment* - *Identify the assumptions and constraints associated with the assessment* - *Identify the sources of information to be used as inputs to the assessment* - *Identify the risk model and analytic approaches to be employed during the assessment"*
2. *Conduct* risk assessments	- *"Identify threat sources that are relevant to organisations* - *Identify threat events that could be produced by those sources* - *Identify vulnerabilities within organisations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation* - *Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful* - *Determine the adverse impacts to organisational operations and assets, individuals, other organisations, and the Nation resulting from the exploitation of vulnerabilities by threat sources* - *Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations"*
3. *Communicate* risk assessment results to key organisational personnel	- *"Communicate the risk assessment results* - *Share information developed in the execution of the risk assessment to support other risk management activities"*
4. *Maintain* the risk assessments over time	- *"Monitor risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors* - *Update the components of risk assessments reflecting the monitoring activities carried out by organisations"*

[108] Joint Task Force Transformation Initiative, "NIST SP 800-30r1 Guide for Conducting Risk Assessments" (Gaithersburg, MD: National Institute of Standards and Technology, 2012), https://doi.org/10.6028/NIST.SP.800-30r1.

5.4.2. NIST SP 800-53Ar4 – Assessing Security and Privacy Controls in Federal Information Systems and Organisations

Special publication 800-53 focuses on security and privacy controls in information systems, which are essential for safeguarding of confidentiality, integrity and availability of information. It is destined for professionals working in information systems, information security and privacy. The 800-53 document is a catalogue of security controls for US federal information systems, which seeks to provide:

- *"guidelines for building effective security assessment plans and privacy assessment plans*
- *a comprehensive set of procedures for assessing the effectiveness of security controls and privacy controls employed in information systems and organisations supporting the executive agencies of the federal government."*[109]

The results of control assessments may be used to:

- Point to potential weaknesses or difficulties in the organisation's implementation of the Risk Management Framework
- Detect security and privacy related limitations in information systems and their related environment.
- Prioritise risk mitigation activities and decisions
- Verify whether the detected privacy and security weaknesses and problems have been attended to
- Assist monitoring activities and information security and privacy situational awareness
- Ease security, privacy and authorisation decisions
- Communicate budgetary conclusions and the capital investment process

The process of conducting effective security and privacy control assessments consists in four essential steps. Table 5-6 below gives an overview of the security and privacy control assessment process.

Table 5-6 : Overview of the security and privacy control assessment process

Steps	Description
Preparing for security and privacy control assessments	- *"Determine which security and privacy controls/control enhancements are to be included in assessments based upon the contents of the security plan and privacy plan and the purpose and scope of the assessments* - *Select the appropriate assessment procedures to be used during assessments based on the security or privacy controls and control enhancements to be included in the assessments* - *Tailor the selected assessment procedures (e.g., select appropriate assessment methods and objects, assign depth and coverage attribute values)* - *Develop additional assessment procedures to address any security requirements or privacy requirements or*

[109] Ronald S. Ross, "NIST SP 800-53Ar4 Assessing Security and Privacy Controls in Federal Information Systems and Organisations: Building Effective Assessment Plans" (National Institute of Standards and Technology, December 2014), https://doi.org/10.6028/NIST.SP.800-53Ar4.

	controls that are not sufficiently covered by Special Publication 800-53; - *Optimise the assessment procedures to reduce duplication of effort (e.g., sequencing and consolidating assessment procedures) and provide cost-effective assessment solutions* - *Finalise assessment plans and obtain the necessary approvals to execute the plans"*
Developing security and privacy assessment plans	- *"Define assessment objectives* - *Determine elected assessment methods and objects* - *Assign depth and coverage attributes* - *Detail procedures tailored with organisation and system specific information* - *Define assessment cases for specific assessor actions* - *Outline the schedule and milestones"*
Executing the plan	- *"Implement security and privacy assessment plans* - *Execute assessment procedures to achieve assessment objectives* - *Maintain impartiality and report objectively* - *Produce assessment findings* - *Recommend specific remediation actions"* - *"Documenting results of the security assessments in security assessment results and privacy assessment reports"* - *Determining whether assessment objectives have been "satisfied" or "other than satisfied"*
Post-assessment process	- *"Review assessor findings and assess risk of weakness and deficiencies* - *Consult with organisational officials regarding security and privacy control effectiveness* - *Determine/initiate appropriate response actions* - *Develop/update plans of action and milestones* - *Update security and privacy plans"*

5.4.3. NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

NIST SP 800-115 introduces the necessary foundations in order to perform information security assessments. An information security assessment is the process of examining to what extent the assessment object meets specific security requirements.

The report suggests the following three methods to perform a security assessment:

- Testing, i.e. *"exercising one or more assessment objects under specified conditions to compare actual and expected behaviours".*
- Examination, i.e. *"checking, inspecting, reviewing, observing, studying, or analysing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence."*
- Interviewing, i.e. *"conducting discussions with individuals or groups within an organisation to facilitate understanding, achieve clarification, or identify the location of evidence."*

The document examines technical testing and assessment methods which may be used by an organisation. It also seeks to assist the organisations with the implementation of these methods into their systems and networks. A strong focus is put on effective planning and reporting throughout the process.

NIST SP 800-115 recommends the use of a 3-phase security assessment methodology to improve the effectiveness of the process:

- Phase 1: Planning – at this stage, organisations collect data necessary for the assessment process. Such data may include: assets, threats, tools to mitigate threats.
- Phase 2: Execution – at this stage, organisations detect system, network and organisational weaknesses and validate them when appropriate.
- Phase 3: Post-execution – in this final stage, organisations examine the vulnerabilities to define their underlying reasons, outline recommendations and draft a final report.

As far as testing and examination methods are concerned, NIST SP 800-115 identifies three techniques to undertake a security assessment. It is important to note that no technique can provide a comprehensive picture of the state of security, which is why it may be pertinent to use a combination of techniques during the assessment process. The relevant techniques are:

- Review techniques: These techniques are used "*to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities, and are generally conducted manually. They include documentation, log, ruleset, and system configuration review; network sniffing and file integrity checking.*" [110]
- Target identification and analysis techniques: These techniques can "*identify systems, ports, services and potential vulnerabilities, and may be performed manually but are generally performed using automated tools. They include network discovery, network port and service identification, vulnerability scanning, wireless scanning and application security examination.*"[111]
- Target vulnerability validation techniques: These techniques *"corroborate the existence of vulnerabilities and may be performed manually or by using automatic tools, depending on the specific technique used and the skill of the test team. Target vulnerability validation include password cracking, penetration testing, social engineering, and application security testing."*[112]

[110] K A Scarfone et al., "NIST SP 800-115 Technical Guide to Information Security Testing and Assessment." (Gaithersburg, MD: National Institute of Standards and Technology, 2008), https://doi.org/10.6028/NIST.SP.800-115.
[111] Scarfone et al.
[112] Scarfone et al.

The publication makes a clear distinction between "examinations" and "testing". Indeed, examinations are intended to determine whether a system is sufficiently documented. The examination process essentially consists in reviewing existing documents. Testing, on the other hand, requires practical work with systems and networks to detect weaknesses. Methods like scanning and penetration techniques may be used to carrying out testing. NIST argues that testing offers a more precise overview of an organisation's security situation than examination but recommends a combination of both testing and examination techniques for an optimal result.

The following types of testing are identified in the document:

- External security testing
- Internal security testing
- Overt security testing
- Covert security testing

Finally, in regards to policy making, NIST recommends to the following legal considerations:

- Developing a security assessment policy
- Prioritising and scheduling assessments
- Selecting and customising technical testing and examination techniques
- Determining the logistics of the assessment
- Developing the assessment plan
- Addressing any legal considerations

5.4.4. NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organisations

The following publication addresses the risks affecting information and communications technology (ICT) supply chains. Indeed, ICT supply chains are vulnerable to a series of risks including: *"counterfeits, unauthorised production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the ICT supply chain"*.[113] The purpose of SP 800-161 is to offer support to federal agencies in regards to identifying, evaluating and mitigating ICT supply chain risks.

ICT supply chain risk management addresses all issues relevant to the security, resilience, integrity and quality of the components of the supply chain. In order to guarantee a successful implementation, the document recommends that ICT supply chain risk management were directly included into organisations' broader risk management plans and follow the following steps:

- Risk framing
- Risk assessment
- Risk response
- Risk continuous monitoring

[113] Jon M. Boyens, "NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organisations," April 2015, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

NIST SP 800-161 refines and expands the controls established in the previously discussed NIST SP 800-53 Revision 4, adds a new control family named "Provenance" as well as four new controls particularly focused on ICT supply chain risk management. The "Provenance" control family seeks to document the source and modifications made to the supply chain elements. Additionally, the publication provides complementary support where applicable and explains to organisations how controls can be used in the context of ICT supply chain risk management. The document applies multi-tiered risk management practices. The three tiers are "organisation", "mission/business process" and "information systems".

This publication should be used as a complement to NIST SP 800-53 Revision 4 in order to guarantee the most profitable and comprehensive approach. The document serves as a foundation which requires to be adapted to the organisation's context and situation.

NIST strongly advises organisations to maintain close relationships with their suppliers in order to ensure that the components of the supply chain respect the ICT risk management requirements. It is encouraged for companies to establish a common strategy with the suppliers.

5.4.5. NIST IR 8062 – An Introduction to Privacy Engineering and Risk Management in Federal Systems

The internal report introduces a list of goals for privacy engineering and proposes a new model for evaluating risks in federal systems. Security in federal systems has been the focus point of an important number of documents. Recently, the concept of "privacy" has started being incorporated into security documents, suggesting that both concepts share similarities. Nonetheless, both terms have also very distinct meanings. For this reason, it is essential to distinguish information security from information privacy. This exercise will improve the general understanding of how to use the existing engineering and risk management process to respond to privacy issues.[114]

Security and privacy often go hand-in-hand in the public speech. It is certain that guaranteeing the confidentiality of personally identifiable information (PII) is essential in privacy protection. Nonetheless, not all security concerns are associated with privacy, and simultaneously, privacy concerns are not necessarily linked to security. For instance, certain individuals may be more reluctant to use certain technologies, not because they are worried that their device will fail to keep the information secure, but because they are alarmed that their personal information is being collected at all. Continuous monitoring and tracking may trigger concerns regarding the extent of PII that is given away. This situation shows that certain systems may unintentionally, or as a by-product, affect users' privacy (demonstrated through loss of trust or a chilling effect on ordinary behaviour), by the simple fact of collecting and processing their personal data.

NIST uses the Figure 5-4 below to illustrate the relationship security and privacy. Privacy concerns in information systems happen from by-product or authorised processing of PII, as well as unauthorised access to PII. Unauthorised access is generally well visible as it often triggers an emotional pain or creates embarrassment. Examples include economic loss, physical or psychological harm, etc. On the other hand, authorised PII processing is less noticeable but also affects the individuals' perception of risk and results in a series of problems including: loss of trust,

[114] Sean Brooks et al., "NIST IR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems" (Gaithersburg, MD: National Institute of Standards and Technology, January 2017), https://doi.org/10.6028/NIST.IR.8062.

loss of self-determination, discrimination and economic loss. The identification of the boundaries and of the point of overlap between security and privacy is indispensable to establish when the existing security risk models and guidance can be used to respond to privacy issues, and where an alternative solution needs to be conceived to address the matter.

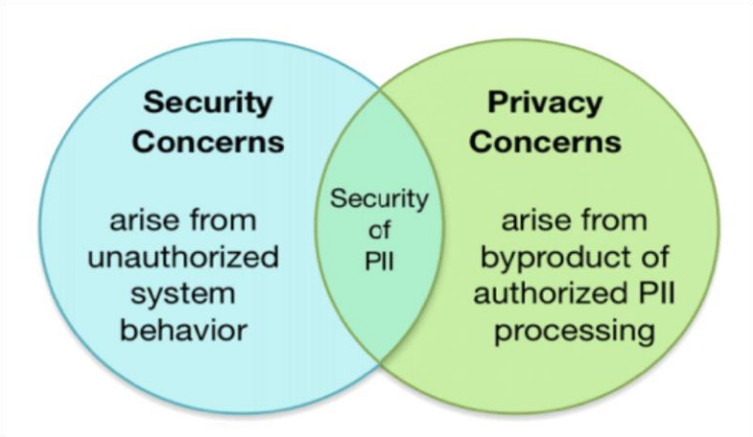

Figure 5-3 : Relationship between information security and information privacy

The document also makes a distinction between the security objectives and the privacy engineering objectives in the field of information security. Indeed, the three security objectives are 1) confidentiality, 2) integrity, 3) availability. NIST introduces 3 privacy engineering objectives in order to support system designers and engineers to concentrate their efforts on the essential requirements. The three privacy engineering objectives are:

- Predictability, defined as "enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system".
- Manageability, described as "providing the capability for granular administration of PII including alteration, deletion, and selective disclosure".
- Disassociability, outlined as "enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system".

The document makes use of the general risk terminology and adjusts it to the context of privacy risk assessment. Indeed, the concepts "threat" and "vulnerability" do not successfully encompass multiple privacy problems for individuals, such as the loss of trust or discomfort arising from the idea of having one's PII continuously monitored by a device. NIST prefers not to overload the privacy risk model, and instead, to pinpoint to the processes that a system is performing on PII, which could be bothersome to individuals in terms of privacy. Such a process is defined as "problematic data action". The report underlines that agencies will not only be required to evaluate the information security risk of their activities, but also carry out risk assessments to evaluate their actions which may be perceived as "problematic" in terms of privacy. The analysis shall assess both the likelihood that a data action is problematic for an individual, and the impact in terms of financial costs or harm deriving from such action. A comprehensive risk assessment should deliver a solution to address the users' concerns and respond to their needs.

5.5. International Telecommunication Union (ITU)

5.5.1. ITU-T X.1208 A Cybersecurity Indicator of Risk to Enhance Confidence and Security In The Use of Telecommunication/Information and Communication Technologies

This recommendation offers a methodology to use cybersecurity indicators to measure risk and outlines a prospective list of cybersecurity indicators. It seeks to support organisations in assessing their cybersecurity situation and potential risk. The guidelines are intended to improve the decision-making process, help organisations to decrease their risk and highlight the areas of interest which need to be improved.

The cybersecurity indicator proposed in the publication is made of a number of cybersecurity indicators. The product offers a risk measure defining the risk situation and the effectiveness of the cybersecurity tools in use. The general principles are explained in the document's clause, which states that[115]:

- When calculating a cybersecurity indicator of risk, it is recommended to first use those included in a globally approved-upon pool of indicators.
- The selection of cybersecurity indicators should include indicators which can assess the cybersecurity situation or to evaluate the improvement from a security initiative.
- The selection should also maintain raw data integrity.
- Indicators which may support policy makers to assess the functioning of a security initiative should be privileged.
- Development of new indicators in line with the fast-paced state of ICT technologies should be put forward.

A cybersecurity indicator should allow for:

- *"The measurement of the major impact on performance results;*
- *Its use to address issues at the system level, the programme level and both level, as appropriate;*
- *The measurement of the progress in implementing a cybersecurity programme, specific security controls and associated cybersecurity policies and procedures;*
- *The measurement of aspects which would allow for the identification of effectiveness and efficiency in a cybersecurity programme;*
- *The measurement of the positive or negative impact of a cybersecurity programme on an organisation's mission;*
- *The measurement of the status of cybersecurity policy performance, with the ability to obtain results at the system level, the programme level or both levels;*
- *The measurement of the positive and negative impacts of the daily life of users."*[116]

The document further specifies that indicators may be classified into the three following categories:

- Implementation indicators used to evaluate the advancement of a security initiative
- Effectiveness/efficiency indicators used to assess whether the programme-level processes and system level security controls are well enforced
- Impact indicators used to elaborate on the impact of information security on an organisation's mission

[115] International Telecommunications Union, "Recommendation X.1208: A Cybersecurity Indicator of Risk to Enhance Confidence and Security in the Use of Telecommunication/Information and Communication Technologies," January 24, 2014, https://www.itu.int/rec/T-REC-X.1208-201401-I/en.
[116] International Telecommunications Union.

The recommendation offers the six following steps which may be used in the process of elaboration of a cybersecurity indicator suite:

1) *"Identification of the key indicators to be selected and used to compute the cybersecurity indicator of risk;*
2) *Identification of data sources;*
3) *Dealing with missing observations;*
4) *Making the indicators comparable to each other;*
5) *Converting the indicators into risk measurement values;*
6) *Leveraging a collection of the risk measurement values"* [117]

The document concludes with a list of 30 potential cybersecurity indicators which are relevant for the development of a cybersecurity indicators suite. These indicators include:

- Indicator 1: Vulnerability management
- Indicator 2: Audit log maintenance
- Indicator 3: Incident response
- Indicator 4: Mean time to mitigate vulnerabilities
- Indicator 5: Security patch program deployment
- Indicator 6: Mean time to patch
- Indicator 7: Mean time to complete a configuration change
- Indicator 8: Risk assessment coverage
- Indicator 9: Malware detection and treatment program coverage
- Indicator 10: Contingency planning coverage
- Indicator 11: Security assessment
- Indicator 12: Security Pledge
- Indicator 13: Remote access control with security gateway
- Indicator 14: Remote access control with security function for intrusion prevention or intrusion detection
- Indicator 15: Wireless access control
- Indicator 16: Personnel security
- Indicator 17: Personally identifiable information (PII) protection
- Indicator 18: Back-up data protection
- Indicator 19: Certified security management system coverage
- Indicator 20: Secure server deployment
- Indicator 21: Spam receipt ratio
- Indicator 22: Organisation's awareness programme
- Indicator 23: Security training and education
- Indicator 24: Cybersecurity role and responsibility
- Indicator 25: Malware infection
- Indicator 26: Personally identifiable information leakage
- Indicator 27: Security budget as a percentage of ICT budget
- Indicator 28: Ratio of authorised device
- Indicator 29: Ratio of authorised software
- Indicator 30: Application software security

[117] International Telecommunications Union.

5.6. European Telecommunications Standards Institute (ETSI)

5.6.1. ETSI TR 103 305_2 V1.1.1 (2016-08) CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and Auditing

The standard is an evolving repository for the evaluation of Critical Security Control implementations. Critical Security Controls are technical tools used to identify, avoid, address and mitigate the negative consequences of cyber-attacks.

The document presents a table containing the relevant measures for Critical Security Controls and their respective metrics and thresholds. The proposed values of metrics and thresholds are a reflection of the opinion of experts, and do not involve any empirical analysis.

Additionally, the standard describes an effectiveness test to evaluate the implementation of each Critical Security Control. The 20 Critical Security Controls covered by the document are:

1. *"Inventory of authorised and unauthorised devices;*
2. *Inventory of authorised and unauthorised software;*
3. *Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers;*
4. *Continuous vulnerability assessment and remediation;*
5. *Controlled use of administrative privileges;*
6. *Maintenance, monitoring & analysis of audit logs;*
7. *E-mail and web browser protections;*
8. *Malware defences;*
9. *Limitations and control of network ports, protocols and services;*
10. *Data recovery capability;*
11. *Secure configurations for network devices such as firewalls, routers and switches;*
12. *Boundary defence;*
13. *Data protection;*
14. *Controlled access based on the need to know;*
15. *Wireless access control;*
16. *Account monitoring and control;*
17. *Security skills assessment and appropriate training to fill gaps;*
18. *Application software security;*
19. *Incident response and management;*
20. *Penetration tests and red team exercises."*[118]

5.7. Information Systems Audit and Control Association (ISACA)

5.7.1. COBIT 5

COBIT 5 (Control Objectives for Information and Related Technologies) is a good-practice framework designed in 2012 by ISACA (Information Systems Audit and Control Association) for the management and governance of information technology. It has been designed to help enterprises obtain

[118] European Telecommunications Standards Institute, "ETSI TR 103 305-2 CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and Auditing," August 2016, http://www.etsi.org/deliver/etsi_tr/103300_103399/10330502/01.01.01_60/tr_10330502v010101p.pdf.

maximum value from IT by keeping a balance between profit-making, risk optimisation and resource use. Similarly to ISO/IEC 27001, COBIT addresses IT governance but its specific objective is to bridge the gap between business goals and IT process. It is important to note that both frameworks complement one another.

COBIT 5 delivers globally approved principles, guidelines, tools and models to improve the trust and value from IT systems. The framework is based on five key principles[119]:

1) Meeting stakeholder needs;
2) Covering the enterprise end to end;
3) Applying a single integrated framework;
4) Enabling a holistic approach;
5) Separating governance from management.

The uniqueness of COBIT5 resides in the fact it seeks to improve the governance of enterprise IT. This is achieved through the implementation of relevant governance enablers, which in turn will allow a sound implementation of frameworks, best practices and standards. Indeed, frameworks, best practices and standards are only useful if they are effectively implemented. The COBIT 5 approach is based on a holistic set of 7 generic enablers that support the implementation process and benefit the stakeholders. These enablers are[120]:

1) Principles, policies and frameworks;
2) Processes;
3) Organisational structures;
4) Culture, ethics and behaviour;
5) Information;
6) Services infrastructure applications;
7) People, skills and competencies.

[119] ISACA, "ISACA Outlines Five Principles for Effective Information and Technology Governance," accessed May 8, 2018, https://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/ISACA-Outlines-Five-Principles-for-Effective-Information-and-Technology-Governance.aspx.

[120] William Brown, "The Failed Vasa: COBIT 5 Governance and the Seven Enablers (Part 3)" (COBIT Focus, October 2014), http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Focus-The-Failed-VASA-COBIT-5-Governance-and-the-Seven-Enablers-Part-3_nlt_Eng_1014.pdf.

5.8. International Electrotechnical Commission (IEC)

5.8.1. IEC 62443-2-1:2010 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program

IEC 62443-2-1:2010[121], also known as ANSI/ISA 62443 outlines the key elements necessary to develop a cybersecurity management system (CSMS) for industrial automation and control systems (IACS) and delivers support on how to manage those elements.

IEC 62443-2-1:2010 derives from the works of the International Society of Automation (ISA) and seeks to define a normative reference system relevant to all industrial automation and control systems (IACS). The system is based on recognised standards for cybersecurity of information systems but takes into consideration the characteristics of industrial systems, as well as the opinions of diverse stakeholders involved in the design, development, integration and exploitation of IACS. The purpose of IEC 62443 is to enhance the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control and to offer criteria for delivering and administering secure IACS.

IEC 62443 builds on established standards for security, particularly the ISO/IEC 27000 series and follows the structure of the 11 categories presented in ISO 27002:

1) Security policy
2) Organisation of security
3) Asset management
4) Human resources security
5) Physical and environmental security
6) Communications and operations management
7) Access control
8) System acquisition, development and maintenance
9) Incident management
10) Business continuity management
11) Compliance

The standard uses a technical approach, based on the 7 “foundational requirements”. It offers a list of technical criteria which allow to define the “security level” of a system in a scale from 0 to 4, with respect to each of the foundational requirements. The foundational requirements are:

1) FR1. Identification, authentication control and access control
2) FR2. Use control
3) FR3. Data integrity
4) FR4. Data confidentiality
5) FR5. Restrict data flow
6) FR6. Timely response to events
7) FR7. Resource availability

[121] International Electrotechnical Commission, “IEC 62443-2-1:2010 Industrial Communication Networks - Network and System Security - Part 2-1: Establishing an Industrial Automation and Control System Security Program,” November 2010, https://webstore.iec.ch/publication/7030.

Meeting the requirements of IEC 62443 is expected to enhance electronic security and help identify and manage the vulnerabilities in IACS.

5.9. British Standards Institution (BSI)

5.9.1. Publicly Available Standard (PAS) 555

[This standard features in Fundamentals, Frameworks, Evaluation, and Systems.]

PAS 555, being a standard aimed at stipulating what governance arrangements organisations need to put in place in order to decide how to achieve a set of cyber security business objectives (rather than stipulating the controls required to achieve those objectives directly within the standard), is more detailed in the Governance domain than any other. Approximately a third of the document is dedicated to the issues of risk assessment, strategy formulation and compliance tracking; all of which are sub domains within the Governance domain. PAS 555 indicates high level business objectives within the main body of the text, supplemented by the identification of a relatively large number of indicative controls from other well-known cyber security standards.

PAS 555 emphases that the organisation must gather (and where appropriate share) intelligence regarding the prevailing threat that it faces through system monitoring, and then apply this knowledge through its continuous improvement processes. It does not indicate what information should be gathered, what process should be followed for the organisation to determine what should be gathered, or who should analyse it and how.

PAS 555 dedicates approximately a third of its text to clauses that address the Respond domain. Resilience is strongly reinforced as a key requirement; along with the organisation's ability to restore services as quickly as possible and investigate what happened after an incident. There is more detail provided regarding specifically what the organisation must do compared to the Prepare, Operations or Intelligence domains.[122]

5.10. Federal Office for Information Security (BSI, Germany)

5.10.1. BSI-Standard 100-1 Information Security Management Systems (ISMS)

BSI Standard 100-1[123] defines the general requirements for an ISMS. It is completely compatible with ISO Standard 27001 and moreover takes the recommendations in ISO Standards of the ISO 2700x family into consideration. It provides readers with easily understood and systematic instructions, regardless of which methods they wish to use to implement the requirements.

BSI presents the content of these ISO Standards in its own BSI Standard in order to describe some issues in greater detail and therefore facilitate a more didactic presentation of the contents.

This standard describes how an information security management system (ISMS) can be designed. A management system encompasses all the provisions as regards supervision and management so that the institution can achieve its objectives. An information security management system therefore specifies the instruments and methods that the administration/management level of an

[122] British Standards Institution, “PAS 555:2013:Cyber Security Risk. Governance and Management. Specification.”
[123] BSI, “BSI-Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS),” 2008, 37.

institution should use to comprehensibly manage the tasks and activities aimed at achieving information security.

Moreover, this BSI standard provides answers to, among other things, the following questions:

- What are the success factors with information security management?
- How can the IT security process be managed and monitored by the management responsible for this?
- How are security objectives and an appropriate IT security strategy developed?
- How are IT security measures selected and an IT security policy drawn up?
- How can an achieved level of security be maintained and improved?

This management standard provides a brief and clear overview of the most important tasks of security management. The BSI provides assistance with implementing these recommendations in the form of the IT-Grundschutz Methodology. The IT-Grundschutz provides a step-by-step guide to developing an information security management system in practice and gives very specific measures for all aspects of information security. The procedure in accordance with IT-Grundschutz is described in the BSI standard 100-2 and is designed such that an appropriate level of IT security can be achieved as cost effectively as possible. In addition to this, standard security measures for the practical implementation of the appropriate level of IT security are recommended in the ITGrundschutz catalogues.

According to BSI-Standard 100-1, the tasks and duties of the management level with regard to information security can be summarised in the following points:

- Assumption of overall responsibility for information security
- Integrating information security
- Managing and maintaining information security
- Setting achievable goals
- Weighing up security costs against benefits
- The function of role model

Figure 5-1 provides an overview of the lifecycle of a policy for information security, as described in this standard:

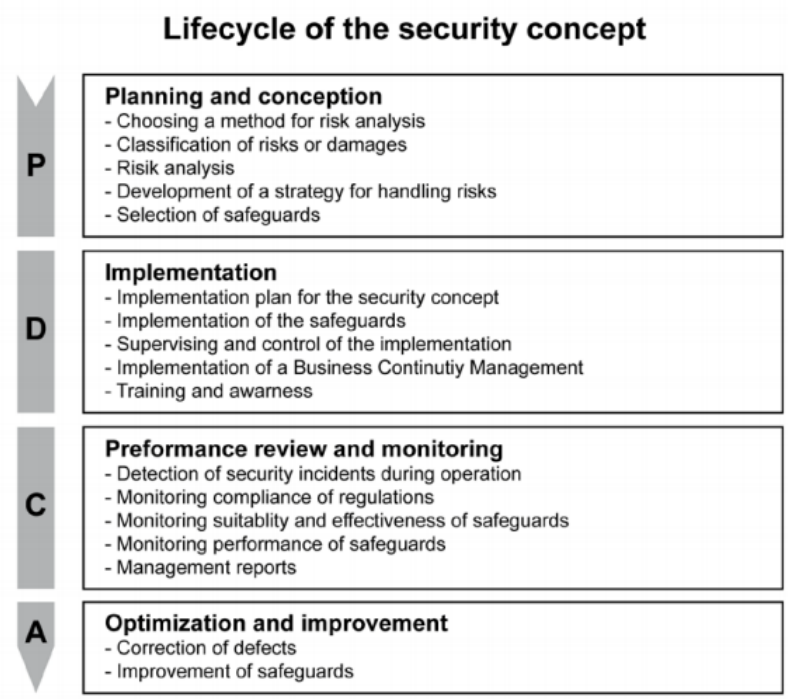

Figure 5-1 : Lifecycle of the Security Concept

5.10.2. BSI-Standard 100-2: IT-Grundschutz Methodology

The IT-Grundschutz Methodology[124] progressively describes (step by step) how information security management can be set up and operated in practice. The tasks of information security management and setting up a security organisation are important subjects in this context. The IT-Grundschutz Methodology provides a detailed description of how to produce a practical security concept, how to select appropriate security safeguards and what is important when implementing the security concept. The question as to how to maintain and improve information security in ongoing operation is also answered.

Thus, IT-Grundschutz interprets the very general requirements of the ISO Standards of the ISO 2700x family and helps the users to implement them in practice with many notes, background expertise and examples. The IT-Grundschutz Catalogues not only explain what has to be done, they also provide very specific information as to what implementation (even at a technical level) may look like. The IT-Grundschutz approach is therefore a tested and efficient opportunity to meet all the requirements of the ISO Standards mentioned above.

The IT-Grundschutz Methodology describes a method for setting up and integrating IS management in an organisation. If an organisation has effective IS management integrated into the business processes, it can be assumed that it is in a position to achieve the desired security level, to improve it where necessary, but that it will be able to meet new challenges as well.

In addition to the IT-Grundschutz Methodology, the IT-Grundschutz Catalogues also provide implementation aids for the security process in the form of field-proven, standard security

[124] BSI, “BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise,” 2008, 95.

safeguards. The IT-Grundschutz Catalogues describe how to create and monitor security concepts based on standard security safeguards. Suitable bundles ("modules") of standard security safeguards are available for common processes, applications, and components used in information technology. These modules are classified into five different layers according to their focus:

- Layer 1 covers all generic information security issues. These include the human resources, data backup concept, and outsourcing modules.
- Layer 2 covers the technical issues related to building construction. Examples include the modules for buildings, server rooms, and home offices.
- Layer 3 covers individual IT systems. Examples include the general client, general server, telecommunication system, laptop, and mobile telephone modules.
- Layer 4 concerns the issues relating to networking IT systems. Examples include the heterogeneous networks, WLAN, VoIP, network management, and system management modules.
- Finally, Layer 5 deals with the actual applications. Examples include the e-mail, web server, and database modules.

In order to achieve an appropriate level of security, a systematic approach is required to design the security process. The security process is comprised of the following phases in the context of ITGrundschutz:

- Initiation of the security process
- Accepting of responsibility by the management
- Designing and planning the security process
- Creation of the policy for information security
- Establishment of a suitable organisational structure for information security management
- Provision of financial resources, personnel, and the necessary time
- Integration of all employees in the security process
- Creation of a security concept
- Implementation of the security concept
- Maintenance of information security during live operations and implementation of a continuous improvement process

5.10.3. BSI-Standard 100-3: Risk Analysis Based on IT-Grundschutz

The IT-Grundschutz Catalogues of the BSI contain standard security safeguards required in the organisational, personnel, infrastructure and technical areas that are generally appropriate for normal security requirements and to protect typical information domains. Many users, who are already working successfully with the IT-Grundschutz, are confronted with the question, how they are to deal with areas, whose security requirements clearly go beyond the normal measure. It is important that the basic methodology does not produce a great deal of additional effort and expense and reuses as many approaches as possible from the IT-Grundschutz.

To cover these issues, the BSI has worked out a method of analysing risks that is based on IT-Grundschutz.[125] This approach can be used when companies or public authorities are already working successfully with the IT-Grundschutz Manual and would like to add an additional security

[125] BSI, “BSI Standard 100-3 - Risk Analysis Based on IT-Grundschutz,” 2008, 23.

analysis to the IT-Grundschutz analysis as seamlessly as possible. There may be different reasons for this:

- The protection requirements of the company or the public authority go beyond the normal measure (high or very high protection requirements);
- The institution operates important components, which are (still) not treated in the IT-Grundschutz Catalogues of the BSI;
- The target objects are operated in application scenarios, which are not designated within the framework of the IT-Grundschutz.

This approach is aimed both at the users of information technology (those responsible for information security) and at consultants and experts.

This document outlines the methodology for carrying out risk analyses to supplement an existing IT-Grundschutz security concept. The document draws on the threats specified in the IT-Grundschutz Catalogues.

Before starting the actual risk analysis, the following preliminaries should have been dealt with:

- A systematic information security process must have been initiated
- A scope for the security concept must be defined
- A structure analysis must have been performed for the information domain
- An assessment of protection requirements must have been performed
- A modelling process must have been performed
- Prior to the risk analysis a basic security check must be performed
- A supplementary security analysis must have been performed

The threats which are relevant to the target objects under review and are listed in the IT-Grundschutz Catalogues constitute an appropriate starting point for the risk analysis.

The aim of the following work steps is to produce a summary of the threats to which the target objects under review are subject:

- All target objects not under review are eliminated from the modelling process
- All the modules that remain in the table for which there is no target object or group of target objects left are deleted
- The result of these steps is a table in which the modules that are relevant for the target objects that have a high protection requirement are listed
- Each module from the IT-Grundschutz Catalogues refers to a list of threats. For each target object in the table the number and title of these threats are inserted from the modules and assigned to the relevant target object.
- The result is a table that assigns a list of relevant threats to each target object
- Subsequently, the threats in the table should be sorted for each target object by subject
- In order to facilitate the subsequent analysis, the protection requirement for each target object that was determined for the three basic parameters of confidentiality, integrity and availability when determining the protection requirement should be listed in the table.

For the target objects under review there are, in some circumstances, additional isolated threats over and above those foreseen in the IT-Grundschutz Model. These must also be taken into consideration.

The next step works through the threat summary systematically. It checks whether the security measures already implemented or at least planned in the security concept provide adequate protection for each target object and threat. As a general rule, these will be standard security measures taken from the IT-Grundschutz Catalogues.

The risk assessment provides an overview as to which threats are adequately covered for the target objects under review by the measures contained in the IT-Grundschutz Catalogues, and as to where there may still be risks.

In practice, the risk assessment usually identifies a number of threats which are not adequately counteracted by the measures contained in the IT-Grundschutz Catalogues. Risks for operating the information domain may arise from these residual threats. Therefore, a decision on how to deal with the remaining threats has to be taken. In all cases management must be involved in this decision because there may under some circumstances be substantial risks or additional costs.

During the risk analysis, threats may be identified under some circumstances that lead to risks which may be acceptable now, but which will probably increase in the future. This means that it may be necessary to take action during further development. In such cases, it is appropriate and common to prepare and create supplementary security safeguards in advance.

If additional security measures must be added when handling the remaining threats, the security concept must subsequently be consolidated.

Once the security concept has been consolidated, the security process, as specified in the IT-Grundschutz Methodology, can be resumed. Therefore, the adjusted security concept becomes the basis for the following work steps:

- Basic security check
- Implementing the security concept
- Reviewing the information security process on all levels
- Information flow in the information security process
- ISO 27001 Certification on the basis of IT-Grundschutz

5.10.4. BSI-Standard 100-4: Business Continuity Management

The BSI Standard 100-4[126] points out a systematic way to develop, establish and maintain an agency-wide or company-wide internal business continuity management system.

The goal of business continuity management is to ensure that important business processes are only interrupted temporarily or not interrupted at all, even in critical situations. To ensure the operability, and therefore the survival, of a company or government agency, suitable preventive measures must be taken to increase the robustness and reliability of the business processes as well as to enable a quick and targeted reaction in case of an emergency or a crisis.

In this standard, BSI Standard 100-4, a methodology for establishing and maintaining an agency-wide or company-wide internal business continuity management system is presented. The methodology described here builds on the IT-Grundschutz methodology described in BSI Standard 100-2. By fully implementing this standard and the corresponding modules in the IT-Grundschutz catalogues, as a business continuity management system that also completely fulfils the less technically-oriented standards like the British standard BS 25999 Parts 1 and 2 can be established.

BSI Standard 100-4 is written so that the methodology can be used by organisations of any type or size and from any industry. It completely describes the optimal method of implementation and is directed towards large organisations.

This standard, BSI Standard 100-4, builds on the previous standards but describes a stand-alone management system for business continuity and business continuity response. The goal of this standard is to point out a systematic method for enabling fast reactions to emergencies and crises of all types and origins that could lead to a disruption of business operations. It describes more than just IT service continuity management and therefore should not be viewed as a subset of ISMS. BSI Standard 100-4 describes how the results of the classic IT-Grundschutz methodology performed according to BSI Standard 100-2 and the risk analysis according to BSI Standard 100-3 can be used as a basis for appropriately preventing and avoiding emergencies as well as a basis for minimising the damages resulting from an emergency. It points out the need to co-operate closely with security management to establish efficient business continuity management in an organisation. The more intensely the business processes utilise information technology, the more synergy effects can be gained through co-operation with the ISMS. Close co-operation between these two disciplines is recommended due to the large number of overlapping areas of responsibility.

The business impact analysis (BIA) described in this standard is introduced as an additional tool for performing the protection requirements determination according to the IT-Grundschutz methodology. With the help of the BIA, the critical business processes are identified and the availability requirements for the processes and their resources are determined.

Information security management focuses on protecting the information in an organisation while business continuity management focuses on the critical business processes. The information in an organisation is considered to be a valuable resource requiring protection (also referred to as assets), and the critical business processes form the backbone of an organisation. Both management

[126] BSI, "BSI-Standard 100-4: Business Continuity Management," 2008, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1.

systems apply a holistic approach. The business areas are the drivers behind business continuity management as well as information security management.

The business continuity management process, according to BSI Standard 100-4, consists of the following phases: initiation of business continuity management, contingency planning, implementation of the contingency planning concept, business continuity response, tests and exercises, as well as maintenance and continuous improvement of the business continuity management process. The above mentioned are also presented in the following Figure 5-2:

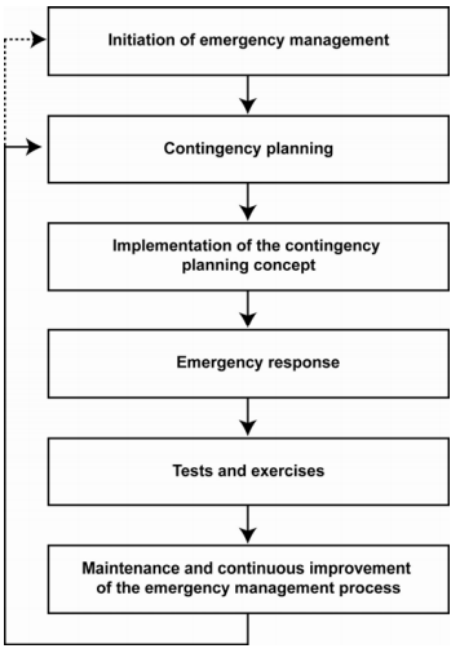

Figure 5-2: Business Continuity Management Process

5.11. Spanish Ministry of Public Administrations

5.11.1. MAGERIT

This section summarises the Methodology for Information Systems and Risk Analysis and Management - MAGERIT[127] standard. We can assign the MAGERIT to the section 4.4 ("Implementing Risk Management) of the ISO 31000 standard and it deals with the Risk Management Process with focus on governing bodies to help them correctly assess risks which arise with the information technologies usage ("ICT risks") and implement this into their decision-making process. The primary goal of MAGERIT is to outline a clear methodical approach of ICT risks assessment and description of appropriate measures to be taken in order to control ICT risks. This should avoid unclear and ambiguous ICT risk assessments heavily dependent on analysts' opinions and views.

First of all, the risk analysis and treatment should form an integral part of the security management, which is incorporated in the organisations' objectives, overall strategy and policies. Based on that, a security plan is prepared, implemented and operated. The active participation of the staff working in the information system is necessary for the design and implementation of ICT security controls. Moreover, it is crucial to establish a "security culture" coming from the top management and support awareness raising. The four main processes of the Information Security Management

[127] High Council of the Electronic Administration, *Risk Analysis and Management Methodology for Information Systems*, n.d.

Systems (ISMS) [ISO 27001] (PDCA cycle) are: Plan (planning), Do (implementation and operation), Check (monitoring and assessment) and Act (maintenance and improvement). It is worth noting that the trustworthiness of the information system plays an important role in the organisations. This could be achieved by regular evaluations, certifications, auditing and accrediting. In general, risk analysis should be carried out in any organisation whose operations rely on information and communication systems. However, sometimes risk analysis is required by a legal percept (links).

The MAGERIT standard consists of three parts – Book I The Method, II Catalogue of Elements, III Techniques.

Risk Management

The MAGERIT distinguishes two main task of risk management: risk analysis and risk treatment. The diagram below as shown in the MAGERIT standard (ISO 31000) depicts the clear overview of the risk management process including different activities as a part of it.

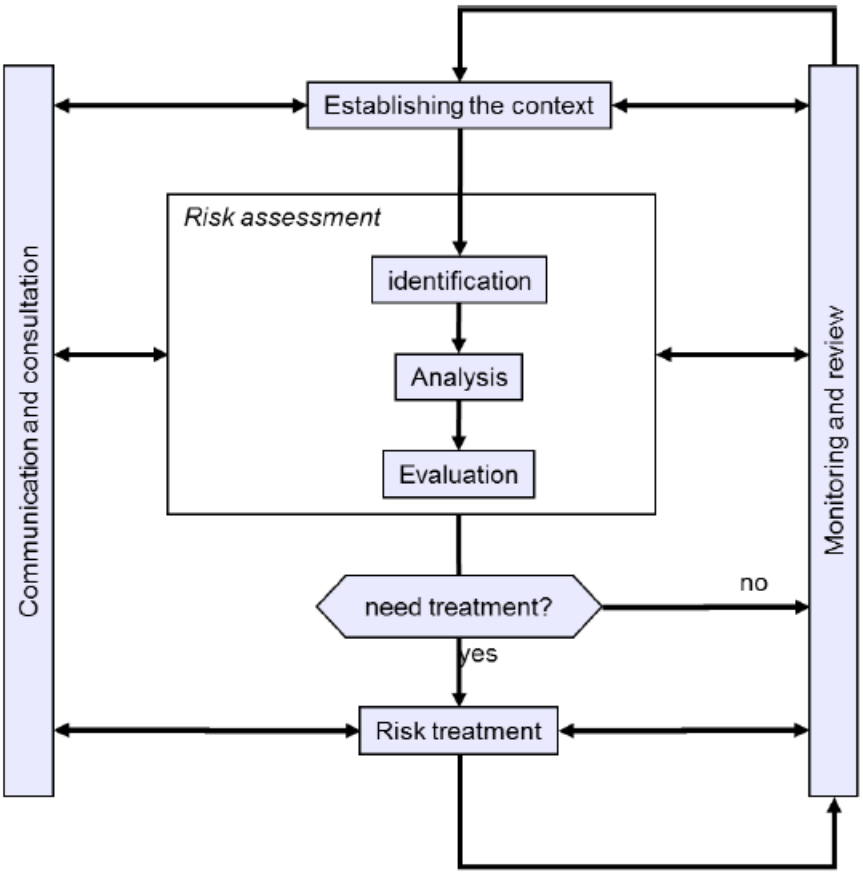

Figure 5-4 : Risk management process (source: ISO 31000)

Based on the assets, threats and safeguards evaluation, the potential impact and risk is estimated and ideally, the corresponding measures should be taken.

Risk Analysis Method

The MAGERIT standard specifies six steps of risk analysis.

Step 1: Assets Valuation
Assets are information, data, services, applications (software), equipment (hardware), communications, media, facilities and personnel. The standard distinguishes two key types of an information system – information and services. For the proper evaluation, dependencies between the different types of assets should be modelled and taken into account. A detailed information including lists of types of assets, valuation dimensions and criteria is in Book II Catalogue of Elements, chapters 2-4.

Step 2: Determination of Threats
The definition of the threat as in MAGERIT, is: "Events that can cause an incident in the organisation, causing damage to property or intangible losses on its assets." For an easy and structured threat identification, Chapter 5 of the "Elements catalogue" provides an overview of typical threats. For the threats valuation, the determination of the degradation (the amount of damage done to the value of the asset) and the likelihood (how often the threat occurs) is crucial.

Step 3: Safeguards
Based on the asset valuation and threats identification, the available safeguards are summarised and their effectiveness against the risk is assessed. The Chapter 6 of the "Elements" catalogue provides a list of suitable safeguards for each type of assets.

Step 4: Residual Impact
When several types of safeguards are implemented and the management process can be considered as being mature, it can still undergo an impact called "residual". The calculation of the residual impact is based on the calculation of the impact with the new degradation level.

Step 5: Residual Risk
When several types of safeguards are implemented and the management process can be considered as being mature, there is still a risk called "residual". The calculation of the residual risk is based on the updated impact (residual impact) and the updated likelihood (new rate of occurrence) of threats.

Step 6: Re-evaluation
The theoretical values of impact and potential risk from steps 2 and 3 are updated every time a safeguard is implemented and then the new residual impact and the new residual risk is computed to give more realistic values.

Risk Management Process

Once having the correct assessment of risks and impacts to which the system is exposed (see previous point), several decisions have to be taken, e.g. obligations from the law, sectorial regulations and various contractual agreements. Factors like public image, internal policy, relationship with clients, users, employees, providers and other organisations, and also new business opportunities have to be taken into account. The figure 5-6 below shows the risk treatment decision making, where the risk assessment stands for the risk analysis and further evaluation. It is

important to keep in mind that the risk decreases sharply with small investments, but the cost of security level at nearly 100% usually increases a lot beyond the value that we want to protect. There are several risk treatment options such as risk elimination (in the case of non-acceptable risks it is usually the best option to eliminate the source of risk), risk mitigation (degradation reduction or likelihood of threat reduction), risk sharing (outsource system components or purchase insurance), funding (reserve funds as a cushion after the risk is materialised.

In MAGERIT, several different actors (e.g. governing bodies, executive board etc.) and their responsibilities are listed. In addition, the whole process has to be documented.

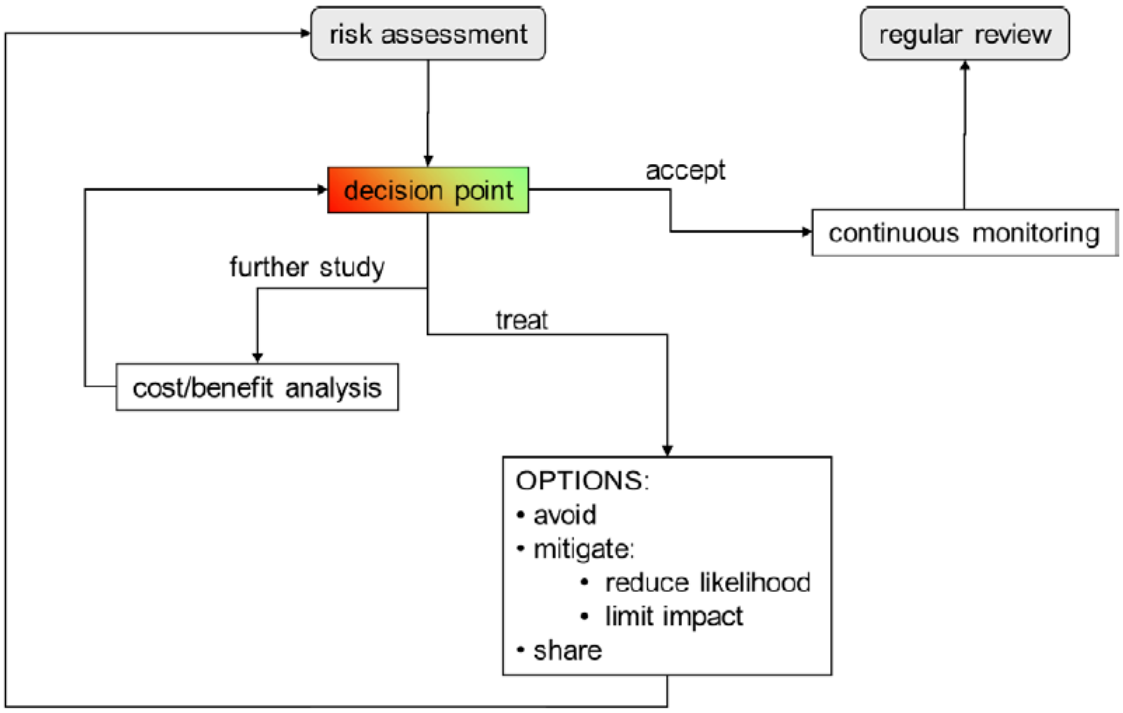

Figure 5-5 : Risk treatment decision making (source: MAGERIT).

Risk Analysis Projects

Risk analysis has to be reviewed and updated on a regular basis. This standard suggests the creation of specific roles such as the follow-up committee, the project team, contact persons, promoters, project directors or operational liaison. It also describes preliminary activities (study of timeliness, definition of the scope of the project, project planning or project launch). A necessary part is the development of risk analysis and the clear communication of results.

Security Plan

This section of MAGERIT shows the implementation of security plans, i.e. projects focused on the implementation of the decisions made to manage risks. The different steps described in detail include: identification of security projects, implementation plan, implementation itself and the security plan control list. The standard also describes general rules for the development of information systems.

Practical Guidance and Appendix

The standard concludes with practical advice with respect to the steps and sections described above. It provides a more detailed guidance in the discovering and modelling of the dependencies between assets, shows typical mistakes and describes thoroughly the asset valuation and threats identification and valuation, safeguard choice. In Book III Techniques describes several techniques to be used in risk analysis and management projects (e.g. algorithmic analysis, attack trees, data flow diagrams, working sessions etc.).

5.12. H2020 Privacy Flag

5.12.1. Universal Privacy Risk Area Assessment Methodology (UPRAAM)

A methodology for the assessment of privacy risk is developed in the H2020 European Research Project entitled "Privacy Flag".[128] This project is a European Research project merging juridical know-how with technological considerations to address the issue of user privacy on the Internet. Questions of data protection are addressed globally, including Internet surfing and the use of smart-phone based applications, and security concerns in smart-cities are discussed. The main objective of the Privacy Flag project is to empower citizens to have an active control on their own data. In order to do so, the project offers a user-friendly privacy protection application for smart-phones, a web browser add-on and a website.

The privacy risk assessment methodology is described in detail in the deliverable D2.3 of the Privacy Flag project. It is labelled "Revision with Simplified Universal Privacy Risk Area Assessment Methodology (UPRAAM)". In section 5 of the UPRAAM framework, the legal obligations ruling privacy and data protection are outlined, including in particular the European General Data Protection Regulation (GDPR). Other relevant legal acts studied are the directive on electronic commerce (Dir 2000/31/EC [D31-1]) and the directive on privacy & electronic communications (Dir 2002/58/EC [D58-1]). International organisations conventions from the United Nations (UN), the World Trade Organisation (WTO), the Organisation for Economic Cooperation and Development (OECD), the International Telecommunication Union (ITU) and the Council of Europe (CoE) are also examined. Finally, Swiss regulations are also granted a specific focus, including the Federal Act on Data Protection (FADP) and its two Ordinances.

This consortium of legal measures helps structuring the analysis of the protection of the privacy of end-users. Based on these measures, the definition and scope of personal data is first determined with respect to (i) the protection of end-user information, (ii) legal requirements for data collection, (iii) data management and (iv) data processing procedures. We briefly describe these four categories.

End-User Information

Strengthening the protection of users' privacy rights can be implemented through controlling access rights, asking to sign informed consent forms, defining data portability rights, allowing users to modify their personal data, allowing them to object to undesired use of their personal data, the right not to have their data subjected to automated processing such as profiling for example, and finally the right to be forgotten in an online environment.

Data Collection

[128] Mandat International, "Privacy Flag Project, Deliverable D2.3 Revision with Simplified UPRAAM" (Geneva, 2016).

Data collection requirements aim at limiting the control of personal data by authorised parties. They include limiting the collection of the data by restraining its use for specific purposes only (e.g. for research). Obligations to document every use and processing of personal data constitutes another way to limit data collection. By designating an officer responsible for data protection purposes, the collection of data can also be restrained. Then, requirements subject's consent for data profiling,[129] geolocation and the use of personal data for direct marketing participate to protect the use of consumers' data. Finally, stronger legal measures for the protection of data for specific categories of end-users, such as minors for instance, also limit the collection and therefore strengthens the privacy of consumers. To sum up, data collection requirements aim at minimising the agglomeration of personal data about users by any type of digital application in order to protect users of a service from any undesired handling of their personal data (including selling the data to a third party).

Data Management

By subjecting data management to third party disclosures and data transfer obligations, data management can be made more transparent.

Data Processing

Limitations on data processing also participates in placing guardrails for the protection of privacy rights. These guardrails can take the form of categorising data into special sensitive classes, protecting the traffic of personal data, securing the ways data are processed, relying on cloud-based services and implementing data protection impact assessments (DPIA).

Based on the analysis of the legal measures outlined above, the UPRAAM framework identifies the set of legal obligations most relevant from an end-user and a SME perspective. We briefly describe these obligations for both end-users and SME's before addressing the technical risks associated with the protection of privacy rights.

An End-User Perspective

Adopting such a perspective is relevant in the context of an end-user who wishes to be aware about the extent to which the personal information he or she reveals when using a digital service. Indeed, when using a smart-phone application, when surfing on the Internet or when interacting with an IoT-based network, the user has the right to know about the potential privacy risks that arise from her or her actions. Under the term "end-user awareness", one can regroup all the knowledge that an individual need to be provided with when his or her data is recorded, collected and kept for potential future use. In other words, any appliance that from near from far deals with personal data about its users need to request consent prior to any prior to any interaction with the user. In addition to information rights, privacy rights from an end-user perspective include the right to amend or delete the information he or she has conceived, the right to access this data and to possibly refute its processing.

[129] Data profiling stands for collecting and/or using an end-user's contact information, his or her browsing history, the duration of web-navigation, the frequency of given queries acquired through cookies for instance.

Broadly speaking, the end-user perspective on users' privacy rights include the limitations outlined in the four categories summarised above. The SMEs perspective, which targets companies that offer digital services, adds to these obligations further data management duties at every stage of the data acquiring process. This add to the list of data processing limitations. Examples include setting-up "anonymisation techniques" of users' personal information to prevent companies from directly linking the acquired data to users, the necessary "compatibility of new purposes with the original aim of the processing" or joint data controllability shared by the data processor and the user. Compliance to these limitations that are edified in data protection laws need to be verified on a frequent basis.

In addition to the detailed list of obligations on data protection and privacy, technical risks embedded in the UPRAAM framework are described in section 6.[130] These risks comprise, among others, the risk of (i) "tracking and profiling of users" and (ii) "personal data leakages". Tracking of users can be done through the introduction of cookies in browsers, through web browser or device fingerprinting, physical observations and the like. Personal data leakage can arise from poor encryption mechanisms, from the exploitation of security vulnerabilities and from traffic analysis, etc. Both categories of technical risks are described in tables 5-7 and 5-8 below.

Table 5-7 : Technical risk - tracking of users

Risk	Description	Threat level (1..9)	Detectable by user	Detectable by technical means	Website	Smartphone	Smart City
Cookies	Textfile created on the user's computer	1	Yes	Yes	X	X	
Advanced Cookies	Special cookie mechanisms that are, e.g., automatically recreated after deletion, such as Zombie cookies,Evercookies, Flash Cookies	6	No	Maybe	X	X	
Webbrowser fingerprinting	Creation of a unique fingerprint of a webbrowser installation	8	No	Maybe	X	X	
Device Fingerprinting	Identification of characteristics specific to a unique physical device	8	No	No	X	X	X
Physical observation	Tracking by use of cameras, microphones, or other surveillance techniques	4	Maybe	Maybe		X	X
Geolocation Leakage	Using the device's geolocation API to reveal a user's location	9	No	Yes	X	X	X
Indirect location data leakage	Aggregating indirect location data, when the user uses NFC-enabled devices to buy a bus ticket or usesasmart city's parking system	6	No	No		X	X

[130] Mandat International, "Privacy Flag Project, Deliverable D2.3 Revision with Simplified UPRAAM."

Table 5-8 : Technical risk – data leakage

Risk	Description	Threat level (1..9)	Detectable by user	Detectable by technical means	Website	Smartphone	Smart City
Missing End-to-end encryption	The traffic is transmitted without being encrypted	9	Yes	Yes	X	X	X
Use of unsecure or obsolete cypher suites	The traffic is encrypted, but the encryption methods have known vulnerabilities	8	No	Yes	X	X	X
Man-in-the-middle attacks	Circumvention of mutual authentication between client and server by an attacker	8	Maybe	Yes	X	X	
Missing transparency of service storage method	Data stored within a third-party-service may be leaked because the user has no control over storage security	8	No	No	X	X	X
Security vulnerabilities in service backend	The backend (e.g., data storage methods) deployed by a service provider may be susceptible to security vulnerabilities	6	No	No	X	X	X
Traffic analysis	Information is leaked and exploited through passive eavesdropping and analysis of encrypted transmission	5	No	No	X	X	X
DNS request leakage	Secure DNS is not used and DNS request are visible to everyone	8	No	Maybe	X	X	X

6. Privacy Certification Mechanisms

6.1. Entry into Force of the General Data Protection Regulation (GDPR)

Among the trends identified in section 2, the entry into force of the GDPR on May 25, 2018 will bring forward particularly tangible changes to the European cybersecurity panorama[131]. Not only will the Regulation introduce the greatest overhaul of European personal data protection law in 20 years; it will introduce new and specific cybersecurity requirements and approaches[132] that will undoubtedly change the status quo and require organisations to take extra cybersecurity measures to further protect personal data.

According to the EU GDPR portal, the new legislation seeks to harmonise data privacy laws in the EU, guarantee greater protection to EU citizens and change the way in which the business and organisations in the EU address data privacy.[133] The GDPR introduces a series of changes to the existing legislation. The key points include:

- *Territorial scope:* The GDPR has an international scope and the responsibilities and obligations it entails cannot be avoided simply because an organisation is outside the EU jurisdiction. According to art. 3 GDPR, "this regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not"[134].The GDPR also applies to the processing of personal data of data subjects by a controller or processor outside of the EU, where the activities include offering goods or services to EU citizens and the monitoring of their behaviour which takes places in the EU.
- *Penalties:* According to art. 83 GDPR, organisations in violation of the GDPR risk a fine representing 4% of their annual global turnover or an administrative fine up to €20 Million, whichever is higher.[135] The GDPR follows a tiered approach to penalties and the amount will depend on the circumstances of each individual case.
- *Consent:* According to art. 7 GDPR, the data's subject consent shall be explicitly asked for in a clear and easily understandable manner. Indeed, companies will no longer be able to use complex terms and conditions documents difficult to understand to their customers. [136]
- *Breach notification:* According to art. 33 GDPR, "in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority

[131] Indeed, the new legislation will replace the "Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data" adopted in 1995, when the Internet as we know today was still in its early development stage.
[132] Such as the privacy and security by design approach, see: https://www.avepoint.com/blog/protect/privacy-and-security-by-design-gdpr/
[133] EU GDPR Information Portal, "EU GDPR Information Portal," EU GDPR Portal, accessed May 3, 2018, http://eugdpr.org/eugdpr.org.html.
[134] European Parliament, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[135] European Parliament.
[136] European Parliament.

competent". Data processors shall also be required to notify their customers "without undue delay" about data violation.[137]

- Right to access and right to be forgotten*:* Articles 15 and 17 GDPR grant greater power to data subjects by giving them to the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, where and for what purpose. Furthermore, under certain conditions, the data subject can request the data controller to delete their personal data, stop its dissemination and prevent third parties from processing it.[138]
- *Data Protection Officers (DPO):* According to art. 37 GDPR, DPO appointment will be mandatory for those controllers and processors whose core activities consist of processing operations, require regular and systematic monitoring of data subjects on a large scale or of specific personal data relating to criminal conviction and offences. The tasks and duties of a DPO are clearly outlined in art. 39 GDPR.[139]

The GDPR provides for the creation of certification mechanisms[140] in order to show compliance with the requirements provided by the regulation. Certification mechanisms are therefore conformity assessment activities against specific requirements performed and attested by a third party. The purpose of a data protection certification is to demonstrate compliance with the GDPR[141].

In the greater scope of this deliverable, these certification mechanisms might be relevant to businesses and other stakeholders which might be interested in benchmarking their privacy and security measures and demonstrating compliance with the GDPR. While several options are being developed (see ENISA, "Recommendations on European Data Protection Certification," November 2017.), two of these certification mechanisms will be briefly introduced to analyse their potential relevance in section 8 of this deliverable.

[137] European Parliament.
[138] European Parliament.
[139] European Parliament.
[140] According to article 42.1 of the GDPR: "The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account".
[141] ENISA, "Recommendations on European Data Protection Certification," November 2017.

6.2. EuroPrivacy

The EuroPrivacy certification is designed to address emerging technologies such as IoT deployments, data analytics, smart cities. It is based on the UPRAAM methodology[142] as developed in the context of the Privacy Flag research project and benefits from ongoing Horizon2020 European research projects on privacy and cybersecurity such as ANASTACIA (privacy and security seal); SAINT (cybersecurity); Create-IoT (Trusted IoT label); and U4IoT which is in charge of promoting personal data protection in the context of the five European Large Scale Pilots (LSPs) on the Internet of Things which are financed by the European Commission. The LSPs cover different domains ranging from smart cities to wearables to smart homes and smart transportation.

The EuroPrivacy certification scheme encompasses several regulations and standards which are relevant for cybersecurity purposes:

- The European General Data Protection Regulation
- Swiss and International data protection obligations
- Relevant ISO standards

The certification mechanism developed by EuroPrivacy can be extended also to complementary obligations such as:

- National obligations, including the Swiss Federal Act on Data Protection (FADP) and its two ordinances;
- European Directive 2002/58/EC (E-Privacy)
- European Regulation 910/2014 (eIDAS)
- European Directive 1148/2016 (NIS Directive)

Moreover, EuroPrivacy complies with ISO standards for certification including:

- ISO/IEC 17021
- ISO/IEC 17065
- ISO/IEC 17030

It can be also combined with ISO/IEC 27001 certification.

By combining these standards the certification scheme is capable of assessing and validate technical measures for personal data protection such as: encryption and strong authentication; securing network and data transmission, servers security, personal data dissociation, pseudonomysation and anonymisation; prior informed consent mechanisms; real time intrusion detection tools; data ownership and end user data control; role-based access control.

EuroPrivacy can therefore be used for several purposes: audit and certify compliance with the GDPR; identify legal, financial and reputational risks, enhance data protection through surveillance audit, build trust and confidence.

[142] Mandat International, “Privacy Flag Project, Deliverable D2.3 Revision with Simplified UPRAAM.”

6.3. EuroPriSe

The EuroPriSe Privacy Seal is a tool that allows to certify that an IT-based service or an IT-product is compliant with EU regulations on privacy and data protection and also takes into account the legislation of EU Member States. All the vendors and manufacturers of IT-products and service providers can apply for the seal in order to prove their compliance with EU regulations. In order to evaluate the compliance with EU regulations EuroPriSe follows four main sets of criteria:

- A) Overview of fundamental issues
- B) Legitimacy of Data Processing
- C) Technical-Organisational Measures
- D) Data Subjects' Rights

The aim of certification is increasing market transparency for privacy relevant products and an enlargement of the market for Privacy Enhancing technologies and increase of trust in IT by certifying privacy compliance with data protection regulations. As far as the requirements and normative basis are concerned they are bases on the ePrivacy Directive and the GDPR and the criteria are formulated as questions.

The EuroPriSe seal is awarded after:

A) An evaluation by an independent accredited auditor;
B) The validation of the produced evaluation report by the EuroPriSe certification body.

EuroPriSe criteria are updated on demand and are constantly adapted to changes in EU privacy legislation and developments in information technology. The seal is valid cross the EU and can be used both in consumer marketing and public procurement.

7. Reference documents on Privacy and Security

7.1. Introduction

This section features reference documents to be considered[143] when implementing any of the aforementioned standards. Particularly it introduces Privacy Impact Assessment Guides from different countries around the world, as well as reports and recommendations on privacy and security generated by various industry groups.

7.2. Summary

Table 7-1: Summary of documents in section 7

Section	Document(s)	For…
7.3.1.1 7.2.1.1 7.3.1.1 7.3.5.1 7.3.5.3	How to do a Privacy Impact Assessment (PIA) Guide to Undertake Privacy Impact Assessments Planning for Success Conducting Privacy Impact Assessments Guide Conducting Privacy Impact Assessments Code of Practice	Privacy Impact Assessments
7.3.4.1 7.3.4.2 7.3.5.1	Guia Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos Sujetas al RGPD Anonymisation: Managing Data Protection Risk Code of Practice	Personal Data Protection Risk Management
7.3.5.2	Data Sharing Code of Practice	Data sharing
7.4.1	ECSO State of the Art Syllabus	Standards overview
7.5.1 7.6.1 7.7.1 7.8.1 7.9 7.10.1 7.11.1 7.13.2	Industrial Internet of Things, Volume G4: Security Framework Strategic Principles for Securing the Internet of Things (IoT) BITAG Report – Internet of Things (IoT) Security and Privacy Recommendations IoT Security Guidance OneM2M technical specification Security Guidance for Early Adopters of the Internet of Things (IoT) IoT Security Guidelines Overview Security requirements for wireless sensor network routing	Internet of Things

[143] Given the nature and scope of these reference documents, the contents of this section shall not be introduced to the matrix that is to be generated in supra section 8. Regardless of this, it is advisable that they are considered whenever their territorial or domain-specific scope makes them relevant to the reader's context.

7.10.2	Security Guidance for Critical Areas of Focus in Cloud Computing v4.0	Cloud computing
7.12.1	Guide to Industrial Control System (ICS) Security	Industrial Control Systems
7.13.1	Security architecture for systems providing end-to-end communications	Communications

7.3. National Privacy Impact Assessment Guides and Recommendations

7.3.1. New Zealand's Privacy Commissioner's Office

7.3.1.1. How to do a Privacy Impact Assessment (PIA)

The document entitled "How to do a Privacy Impact Assessment (PIA)" released by the Privacy Commissioner's Office "Te Mana Matapono Matatapu" in New Zealand is structured around the three following topics:

- The questions to address before starting a Privacy Impact Assessment (PIA)
- The main steps of a PIA
- Extra steps to consider, depending on the risks and gravity of the case

Furthermore, the publication also contains practical tools such as a PIA report template to document the information gathered throughout the assessment and a risk management template to document any encountered risks and identify ways to address them.

The questions to address before starting a Privacy Impact Assessment (PIA)

Before starting a PIA, the following questions need to be answered:

- *"At what point in my project will a PIA be most helpful?*
- *How long do I need, and how detailed should the PIA be?*
- *Who should do the PIA?*
- *Who do I need to talk to as a part of the PIA?*
- *Do I need to involve the Privacy Commissioner? And if so at what stage? What can they do to help?"*[144]

The main steps of a PIA

The main steps of a PIA include:

1) *"Gather all the information you need to do the PIA and sketch out the information flows*
2) *Check against the privacy principles*
3) *Identify any real privacy risks and how to mitigate them*
4) *Produce a report (use our report template to help)*
5) *Take action*
6) *Review and adjust the PIA as necessary as the project develops."*[145]

Extra steps to consider, depending on the risks and gravity of the case

[144] New Zealand's Privacy Commissioner's Office, "How to Do a Privacy Impact Assessment (PIA)," July 2015.
[145] New Zealand's Privacy Commissioner's Office.

In the situation where the project is more complicated, extra steps may be considered, such as:

- *"Get an external view of your PIA*
- *Consult with stakeholders*
- *Establish better governance structures to manage personal information*
- *Manage any risks with using third party contractors*
- *Align the PIA with the organisation's existing project-management methodologies*
- *Publish your PIA"*[146]

7.3.2. Office of the Australian Information Commission

7.3.2.1. Guide to Undertake Privacy Impact Assessments

The "Guide to Undertake Privacy Impact Assessments" has been issued in 2014 by the Office of the Australian Information Commission.[147] It outlines the procedure for privacy impact assessments. According to the publication, a PIA consists of the ten following steps:

1) Threshold assessment
   The first step consists in evaluating whether a PIA is necessary. There is no general rule about PIAs and each case should be reviewed individually. A threshold assessment should include a brief description of the project with special attention to whether the project will require collection, storage, use or disclosure of personal data.
2) Plan the PIA
   Planning should take into account a number of elements, including: how detailed the PIA should be, the period of the PIA, the people in charge of the PIA, the financial resources allocated to the project, the degree and timing of stakeholder consultations, steps to be taken after the PIA, such as enforcing the recommendations and continuous monitoring.
3) Describe the project
   The description should contain: the general purpose of the project, the place of this project within the organisation's objectives, the scope and extent of the project, connections with existing programs and projects, the people responsible for the project, the timeline, main privacy information.
4) Identify and consult with stakeholders
   The list of identified stakeholders should booth include internal and external stakeholders affected by the project. The consultation is indispensable in order to highlight the vulnerabilities and risks that have not been discovered previously. In order to guarantee efficiency, stakeholders should be provided appropriate information about the project, and granted the possibility to express their opinions. The mode of consultation (telephone, survey, interviews, etc.) should be chosen specifically for each target group.
5) Map information flows
   Information flows should be clearly outlined in order to explain what data will be gathered, used and disclosed, but also how it will be stored and safeguarded. Mapping the information requires close communication with staff and project stakeholders.
6) Privacy impact analysis and compliance check
7) Privacy management – addressing risks

[146] New Zealand's Privacy Commissioner's Office.
[147] Office of the Australian Information Commission, "Guide to Undertaking Privacy Impact Assessments," May 2014, 42.

When facing risks, the following factors should be considered: necessity, proportionality, transparency and accountability, implementation of privacy protections, flexibility, privacy by design, privacy enhancing technologies

8) Recommendations
   Recommendations should highlight possible vulnerabilities and address ways of responding to them.
9) Report
   The key output of the PIA is the report which should include: a description of the project, the methodology, an outline of data flows, outcome of PIA, recommendations, list of vulnerabilities which cannot be addressed, extra information (if necessary) in the appendices.
10) Respond and review
    The PIA assessment should be viewed as a continuous process. Recommendations should be responded to, in order to create better privacy outputs. Independent audit is also an option to consider, as it allows for a more comprehensive evaluation. Finally, the PIA should be updated if necessary, to address new privacy impacts. If necessary, a new PIA should be carried out.

7.3.3. Information and Privacy Commissioner of Ontario

7.3.3.1. Planning for Success: Privacy Impact Assessment Guide

"Planning for Success"[148], the guide issued by the Information and Privacy Commissioner of Ontario, Canada, offers recommendations on how to conduct a PIA in order check whether an organisation is in line with the legislation. They are intended as support to existing PIAs within an organisation or as a foundation which can be used by an organisation to develop their own PIA.

The publication starts with background information about the importance and benefits of conducting PIAs. It addresses the timeframe for conducting a PIA, which is recommended early in project development. It also calls for each organisation to clearly outline the roles and responsibilities of the parties involved in the PIA process.

The publication presents a four steps methodology to follow in the context of a PIA:

1) Preliminary analysis: analyse the project to find out whether it includes collection, use, storage, disclosure, security or disposal of personal data. If the project does include any of these processes, a PIA should be conducted. Otherwise, the PIA is not necessary.
2) Project analysis: gather the data about the project, the stakeholders and the method in which personal data will be collected, used, retained, disclosed, secured or disposed of.
3) Privacy analysis: based on the information collected previously, identify Freedom of Information and Protection of Privacy Act (FIPPA) or Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) requirements and possible risks to privacy. Furthermore, methods on how to lower or eliminate the risks should be identified. The related recommendations should be evaluations.
4) PIA report: authorisation should be received in order to carry out the recommendations. Conclusions and preferred solutions should be related in the PIA Report. Finally, the project

[148] Information and Privacy Commissioner of Ontario, "Planning for Success: Privacy Impact Assessment Guide," May 2015, https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf.

should be continued, making sure that the recommendations from the PIA are included in the project's agenda and enforced.

The particularity of the publication is that it includes five appendixes: "Preliminary Analysis Questionnaire", "Project Analysis Questionnaire", "Privacy Analysis Checklist", "PIA Report Template" and "Additional Resources". The latter can be used as ready tools for the PIA.

7.3.4. Spanish Agency for Data Protection

The Spanish Agency for Data Protection issued two publications on personal data protection. These guidelines form the Spanish personal data protection agency recommend the measures and techniques that should be applied to the identification, evaluation and management of risks and potential impact of personal data processing activities.

7.3.4.1. Guia Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD

These guidelines[149] are fundamentally based on the historic and scenario-specific risk identification for data processing activities. As such they require companies and organisations to consider technologies, applications, and devices used; nature, scope, context and purpose of the processing; classification of the database to determine its purpose, sensitivity and value/criticality of the data, data lifecycle, authorised individuals to access the personal data; the potential impact of the processing activity; and the recommendations of the Article 29 WP on Data Protection Impact Assessment (DPIA). Upon the consideration of all these elements, the guidelines recommend a risk classification is performed (high risk, risk & low risk) based on the potential impact to data subjects' rights and freedoms. This step should be accompanied by a thorough documentation of the assessment performed and should lead to the implementation of the necessary technical and organisational security measures to appropriately manage the risks (and, if necessary to the performance of a DPIA).

7.3.4.2. Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos Sujetas al RGPD

These guidelines[150] develop the recommended methodology for carrying out a Data Protection Impact Assessment, amongst its elements it calls for a necessity/proportionality assessment of processing vis-à-vis its purposes; a systematic description of: the processing operation, the data lifecycle and related data flows, the nature, scope, context, purposes and basis of the processing, any technologies, applications, devices and techniques involved; an assessment of the risks, possible threats and damages to the data subject's risk and freedoms; and an analysis of any existing legal, technical and organisational measures to determine their potential for risk minimisation.

7.3.5. UK Information Commissioner's Office

[149] The Spanish Agency for Data Protection, "Guia Práctica de Análisis de Riesgos En Los Tratamientos de Datos Personales Sujetos Al RGPD," n.d., https://iapp.org/media/pdf/resource_center/Guia_EvaluacionesImpacto.pdf.
[150] The Spanish Agency for Data Protection, "Guía Práctica Para Las Evaluaciones de Impacto En La Protección de Los Datos Sujetas Al RGPD," n.d., https://iapp.org/media/pdf/resource_center/AnalisisDeRiesgosRGPD.pdf.

The Information Commissioner's Office (ICO), is the UK's independent body set up to "uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals".[151] ICO has published a number of documents in the field of data protection and privacy impact assessments. The following section gives an overview of the most relevant ones.

7.3.5.1. Anonymisation: Managing Data Protection Risk Code of Practice

The document issued by the UK's Information Commissioner's Office (ICO) describes the effects of anonymising personal data. The code covers the issues regarding the anonymisation of personal data, and the disclosure of data once it has been anonymised. The ICO underlines the importance and necessity of anonymising personal data and offers guidelines about the topic, as well as recommendations about evaluating the risks related with the production and publishing of anonymised data. Putting these recommendations to good use shall mitigate the risk of privacy infringements due to inappropriate exposure of personal information.[152] The code is intended for public, private and tertiary organisations dealing with personal and anonymised data.
The code of practice offers a number of recommendations at the level of governance, including the following:

- Organisations should create their own governance structure in relation to their anonymisation process, in order to effectively respond to issues related to the production and disclosure of anonymised information.
- A risk analysis is highly necessary in order to evaluate the probability and the impact of re-identification at the early stage of producing and disclosing anonymised information.
- The risk of re-identification depends on whether the anonymised data is disclosed, shared or published. If the implications arising from the re-identification of anonymised data are important, the organisations are required to:
    - Reach the data owner's approval for the disclosure of the information and clarify the potential outcome;
    - Perform a more thorough risk evaluation and anonymisation;
    - Under certain circumstances, only share the data with a limited audience and with appropriate safeguards.
- Obtaining consent may be onerous and for that reason, consent is not always required to anonymise personal information. Indeed, in the case where there is no possibility of the anonymisation process resulting in harm or concern to the individual, and that the anonymisation is carried out successfully, consent is not necessary. However, the collection of personal information through a re-identification method without the user's knowledge or approval is considered illegal by the Information Commissioner and will result in legal actions.

[151] ICO, "Who We Are," February 26, 2018, https://ico.org.uk/about-the-ico/who-we-are/.
[152] ICO, "Anonymisation: Managing Data Protection Risk Code of Practice," n.d., 108.

7.3.5.2. Data Sharing Code of Practice

The 2011 'Data Sharing Code of Practice'[153] issued by the ICO provides guidelines on data sharing and offers insight into the data sharing laws, particularly on how the Data Protection Act 1998 (DPA) applies to the sharing of personal data. The guide also contains recommendations on guaranteeing transparency and preventing common mistakes. The code is intended for data controllers and intends to ease data sharing in accordance with the DPA. The ICO believes that by following the code of practice, organisations will prove their customers that they handle personal data properly.

Although information can be shared, as long as it complies with the DPA and other existing laws, the ICO recommends the organisation to consider a list of factors and figure out whether data sharing is justified at all. Furthermore, organisations are requested to study the risks and benefits, and have clear motivations before sharing the data. Special conditions apply for sensitive data sharing, such as a person's health, and require the person's consent.

Good practice requires the data controllers to inform the concerned person about their personal information being shared, through the use of a "privacy notice". The privacy notice should be provided to the individual the very first time that their data is collected and needs to include the data controller's name, the motivation for sharing personal data, and the parties the data is shared with. It is also advised for all third parties involved in the data sharing process to be make sure that the individuals are informed that their personal data is being used, and what for.

The disclosure of personal data must respect the DPA, and ensure that the individual's rights and freedoms are intact. Good practice requires the data controllers to consider alternative methods of achieving their interest than disclosing data.

Good practice also requires organisations to design a data sharing agreement with all the relevant stakeholders involved in data sharing, and to update it frequently. This document should address the objectives of data sharing, potential data recipients, data to be shared, data quality, data security, data retention, individual's rights, procedures to review or terminate the data sharing agreement and sanctions, in case of infringements. A privacy impact assessment is recommended before entering into any data sharing agreement in order to identify its benefits and potential risks.

7.3.5.3. Conducting Privacy Impact Assessments Code of Practice

This code issued by ICO in 2014 sets out the basic steps which an organisation can follow to conduct a privacy impact assessment. The document is supplemented with annexes which seek to facilitate the implementation of the PIA. The annexes contain screening questions to determine the best time for a PIA, and a template which can help draft a PIA report.

The code starts with an introduction to PIAs. The introduction provides the organisations with a definition of a PIA, discusses the circumstances under which a PIA is recommended and presents the benefits of conducting a PIA.

[153] ICO, "Data Sharing Code of Practice," 2011, https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf.

The PIA process is the focal point of the code of practice. ICO underlines that the PIA process is flexible and can be incorporated into the organisation's management. The PIA process consists of the following steps[154]:

1) "Identifying the need for a PIA" – the need for a PIA can be determined as a regular part of the organisation's management process or by using the screening questions in the annex questions.
2) "Describing information flows" – explain what data is used, for what purpose and with whom.
3) "Identifying privacy and related risks" – identify the existing and potential privacy and related risks for the individuals and for the organisation.
4) "Identifying and evaluating privacy solutions" – describe how each risk could be managed (eliminated, reduced or accepted).
5) "Signing off and recording the PIA outcomes" – ensure that the privacy risks have been signed-off at a suitable level. The PIA report should include the identified risks and the steps taken in order to manage them. It is good practice to publish the report, to guarantee transparency.
6) "Integrating the PIA outcomes back into the project plan" – the outcomes of the PIA and actions should be incorporated into the project plan. Continuous reviewing and monitoring is advised.
7) Consulting with internal and external stakeholders as needed throughout the process" – discuss the risks and relevant solutions with relevant stakeholders who may be affected by the project.

7.4. European Cyber Security Organisation (ECSO)

7.4.1. ECSO State of the Art Syllabus

The "State of the Art Syllabus" published by the European Cyber Security Organisation (ECSO) provides an overview of all known relevant standards in the field of cybersecurity. The document has been developed in the context of Working Group 1 on "Standardisation, certification, labelling and supply chain management". The "State of the Art Syllabus" seeks to provide a solid understanding of the existing standards and methodologies. Each standard is analysed from the following angles:

- *"Focus: What is (main) area of applicability of this standard?*
- *Associated Scheme and Governance: Does a scheme exist to assess, test or certify*
- *people, products, services, organisations or infrastructures against this standard? If there is an associated scheme, how is the scheme governed? Who is the Standard Developing Organisation, who is the certification scheme owner? What are the accredited third-party labs, if any?*
- *Process: how does the assessment or certification process work? Is self-declaration allowed? Are several different levels of security defined?*
- *Practice: Is this standard actually being used in practice for assessments or certifications? If so, what is the experience and perceived value in the market? How many subjects are certified?*

[154] ICO, "Conducting Privacy Impact Assessments Code of Practice," 2014, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

- *Formal Status: Is there any associated legislation, official mandate or other government involvement?*
- *Relation to other standards/schemes: Is there any official relation with other standards or schemes described in this document?"*

The document respects the following structure:

- Chapter 2 provides an overview of all cybersecurity standards and certification schemes covered in the publication and indicates the organisation responsible for each standard or scheme, the country of origin, the targeted industry and the link to access the website describing the document.
- Chapter 3 covers cybersecurity standards and schemes in the context of products and components.
- Chapter 4 tackles cybersecurity standards and schemes for ICT and cloud service providers.
- Chapter 5 outlines cybersecurity standards and schemes for service providers and end-user organisations. It is subdivided into sections for various industry verticals including: generic organisations not associated with any particular vertical, industry 4.0 and ICS, energy and smart grids, transportation, financial services and insurance, public services/eGovernment/Digital citizenship, healthcare, smart cities and smart buildings, telecom, media and content, critical infrastructures, secure software development, cybersecurity service providers, payment industry, and IoT device vendors.
- Chapter 6 addresses the cybersecurity standards and schemes for security professionals.
- Chapter 7 lists a bibliography of materials for further reading.

7.5. Industrial Internet Consortium (IIC)

7.5.1. Industrial Internet of Things, Volume G4: Security Framework

This document is relevant to enhancements to existing implementations and new implementations. It provides guidance for improving organisational approaches, processes and the use of technologies for creating a trustworthy system.

The purpose of this document, 'Industrial Internet of Things, Volume G4: Security Framework' (IISF[155]) is to identify, explain and position security-related architectures, designs and technologies, as well as identify procedures relevant to trustworthy Industrial Internet of Things (IIoT) systems. It describes their security characteristics, technologies and techniques that should be applied, methods for addressing security, and how to gain assurance that the appropriate mix of issues have been addressed to meet stakeholders' expectations.

This document is informative in nature and not a normative technical specification. It does not contain specifications for conformance or compliance. Implementations may use a variety of mechanisms to address the concerns noted in the document.

The framework breaks the industrial space down into three roles – the component builders, the system builders, and the operational users and mandates that industrial users assess the trustworthiness of the complete system to achieve end to end security.

[155] Sven Schrecker et al., "Industrial Internet of Things, Volume G4: Security Framework' (IISF)," *2016*, n.d., 173.

The document initiates a process to create broad industry consensus on how to secure Industrial Internet of Things (IIoT) systems. The IIoT is being shaped by many participants from the energy, healthcare, manufacturing, transportation and public sectors, each of which needs to consider security.

To avoid security hazards, especially as systems from different sectors interoperate and exploitation attempts are made in the gaps between them, it is important and urgent to build early consensus among the participants on IIoT security.

This work builds on 'Industrial Internet of Things, Volume G1: Reference Architecture' (IIRA, [IICIIRA2016]) that lays out the most important architecture components, how they fit together and how they influence each other. Each of these components must be made secure, as must the key system characteristics that bind them together into a trustworthy system.

This document extends naturally from a chapter in the IIRA describing security concerns. It moves into security-specific territory to ensure security is a fundamental part of the architecture, not bolted onto it.
This document has several parts that do not mirror the IIRA document structure exactly. Part I examines key system characteristics, how they should be assured together to create a trustworthy system, and what makes IIoT systems different from traditional IT systems.

Part II reviews security assessment for organisations, architectures and technologies. It outlines how to evaluate attacks as part of a risk analysis and highlights the many factors that should be considered, ranging from the endpoints and communications to management systems and the supply chains of the elements comprising the system. Different roles are identified that should be considered in conjunction with the key characteristics, including, owner/operator, system integrator/builder and equipment vendor. Each role offers different risk management perspectives that affect the decisions regarding security and privacy.

Part III covers the functional and implementation viewpoint of the IIRA (and subsumes its usage viewpoint). It describes good practices for achieving confidentiality, integrity and availability, and considerations for trusting data when it is communicated and stored, as well as establishing trust in the code and overall execution environment. It also includes patterns for protecting against and limiting risks, including firewalls, separation of networks, separation of privilege, unidirectional gateways, identity management, cryptography, public key infrastructure and trusted execution environment.

The annexes cover topics that apply to more specific segments of the security domain. One covers numerous guidelines, standards and regulations relating to protection of industrial internet systems and discusses the role of standards and compliance in industrial internet Security. Another provides an example of a cybersecurity capability maturity model for evaluating the maturity of the security posture and associated processes within an organisation. The last annex lists some security techniques and processes, their mapping to important security objectives, and their high-level requirements.

7.6. U.S. Department of Homeland Security

7.6.1. Strategic Principles for Securing the Internet of Things (IoT)

The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT) creates immense opportunities and benefits for our society. IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks. This document explains these risks and provides a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate.

The 'Strategic Principles for Securing the Internet of Things (IoT)'[156] published by the U.S. Department of Homeland Security sets the stage for engagement with the public and private sectors on these key issues. It is a first step to motivate and frame conversations about positive measures for IoT security among IoT developers, manufacturers, service providers, and the users who purchase and deploy the devices, services, and systems.

The following principles and suggested practices provide a strategic focus on security and enhance the trust framework that underpins the IoT ecosystem.

Many of the vulnerabilities in IoT could be mitigated through recognised security best practices, but too many products today do not incorporate even basic security measures. There are many contributing factors to this security shortfall. One is that it can be unclear who is responsible for security decisions in a world in which one company may design a device, another supplies component software, another operates the network in which the device is embedded, and another deploys the device. This challenge is magnified by a lack of comprehensive, widely adopted international norms and standards for IoT security. Other contributing factors include a lack of incentives for developers to adequately secure products, since they do not necessarily bear the costs of failing to do so, and uneven awareness of how to evaluate the security features of competing options.

The following principles offer stakeholders a way to organise their thinking about how to address these IoT security challenges:

- Incorporate Security at the Design Phase
- Advance Security Updates and Vulnerability Management
- Build on Proven Security Practices
- Prioritise Security Measures According to Potential Impact
- Promote Transparency across IoT
- Connect Carefully and Deliberately

As with all cybersecurity efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector. Companies and consumers are generally responsible for making their own decisions about the security features of the products they make or buy. The role of government, outside of certain specific regulatory contexts and law enforcement activities, is to provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security.

[156] U.S. Department of Homeland Security, "Strategic Principles for Securing the Internet of Things (IoT)," November 2016, 17.

The purpose of these non-binding principles is to equip stakeholders with suggested practices that help to account for security as they develop, manufacture, implement, or use network-connected devices.

Specifically, these principles are designed for:

- IoT developers to factor in security when a device, sensor, service, or any component of the IoT is being designed and developed;
- IoT manufacturers to improve security for both consumer devices and vendor managed devices;
- Service providers, that implement services through IoT devices, to consider the security of the functions offered by those IoT devices, as well as the underlying security of the infrastructure enabling these services; and
- Industrial and business-level consumers to serve as leaders in engaging manufacturers and service providers on the security of IoT devices.
- The Department of Homeland Security (DHS) identifies four lines of effort that should be undertaken across government and industry to fortify the security of the IoT:
- Coordinate across federal departments and agencies to engage with IoT stakeholders and jointly explore ways to mitigate the risks posed by IoT.
- Build awareness of risks associated with IoT across stakeholders.
- Identify and advance incentives for incorporating IoT security.
- Contribute to international standards development processes for IoT.

7.7. Broadband Internet Technical Advisory Group (BITAG)

7.7.1 BITAG Report – Internet of Things (IoT) Security and Privacy Recommendations

Observations

From the analysis made in the report 'Internet of Things (IoT) Security and Privacy Recommendations'[157] and the combined experience of its members when it comes to Internet of Things devices, the BITAG Technical Working Group makes the following observations:

- Security Vulnerabilities: Some IoT devices ship "from the factory" with software that either is outdated or becomes outdated over time. Other IoT devices may ship with more current software, but vulnerabilities may be discovered in the future. Vulnerabilities that are discovered throughout a device's lifespan may make a device less secure over time unless it has a mechanism to subsequently update its software.
- Insecure Communications: Many of the security functions designed for more general-purpose computing devices are difficult to implement on IoT devices and a number of security flaws have been identified in the field, including unencrypted communications and data leaks from IoT devices.
    - Unauthenticated Communications: Some IoT devices provide automatic software updates. Without authentication and encryption, however, this approach is insufficient because the update mechanism could be compromised or disabled. In

[157] Broadband Internet Technical Advisory Group, "Internet of Things (IoT) Security and Privacy Recommendations" (Broadband Internet Technical Advisory Group, November 2016), https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

addition, many IoT devices do not use authentication in the course of communicating.
    - Unencrypted Communications: Many IoT devices send some or all data in cleartext, rather than in an encrypted form. Communications in cleartext can be observed by other devices or by an attacker.
    - Lack of Mutual Authentication and Authorisation: A device that allows an unknown or unauthorised party to change its code or configuration, or to access its data, is a threat. The device can reveal that its owner is present or absent, facilitate the installation or operation of malware, or cause its core IoT function to be fundamentally compromised.
    - Lack of Network Isolation: These devices also create new risks and are susceptible to attacks inside the home. Because many home networks do not, by default, isolate different parts of the network from each other, a network-connected device may be able to observe or exchange traffic with other devices on the same home network, thus making it possible for one device to observe or affect the behaviour of unrelated devices.
- Data Leaks: IoT devices may leak private user data, both from the cloud (where data is stored) and between IoT devices themselves.
    - Leaks from the Cloud: Cloud services could experience a data breach due to an external attack or an insider threat. Additionally, if users rely on weak authentication or encryption methods for these cloud-hosted services, user data may also be compromised.
    - Leaks from and between Devices: In some cases, devices on the same network or on neighbouring networks may be able to observe data from other devices such as the names of people in a home, the precise geographic location of a home, or even the products that a consumer purchases.
- Susceptibility to Malware Infection and Other Abuse: Malware and other forms of abuse can disrupt IoT device operations, gain unauthorised access, or launch attacks.
- Potential for Service Disruption: The potential loss of availability or connectivity not only diminishes the functionality of IoT devices, but also may degrade the security of devices in some cases, such as when an IoT device can no longer function without such connectivity (e.g., a home alarm system deactivating if connectivity is lost).
- Potential That Device Security and Privacy Problems Will Persist: IoT device security issues are likely to persist because many devices may never receive a software update, either because the manufacturer (or other party in the IoT supply chain, or IoT service provider) may not provide updates or because consumers may not apply the updates that are already available.
    - Many IoT Devices Will Never Be Fixed: Deploying software updates that patch critical security vulnerabilities is difficult in general. Many device vendors and manufacturers do not have systems or processes to deploy software updates to thousands of devices, and deploying over-the-network iv updates to devices that are operating in consumer homes is difficult, as updates can sometimes interrupt service and sometimes have the potential to “brick” the device, if done improperly. Additionally, some devices may not even be capable of software updates.
    - Software Updates Address More Than Just Bugs: Software updates are not simply intended to fix security or privacy bugs. They may also be intended to introduce major new functions or improve performance and security.

  - Consumers Are Unlikely to Update IoT Device Software: Few end users consistently update device software of their own accord; it is best to assume that most end users will never take action on their own to update software.
- Device Replacement May be an Alternative to Software Updates – for Inexpensive or "Disposable" Devices: In some cases, replacing a device entirely may be an alternative to software updates. Certain IoT devices may be so inexpensive that updating software may be impractical or not cost-effective.

Recommendations

The BITAG Technical Working Group also has the following recommendations[158]:

- IoT Devices Should Use Best Current Software Practices:
  - IoT Devices Should Ship with Reasonably Current Software: BITAG recommends that IoT devices should ship to customers or retail outlets with reasonably current software that does not contain severe, known vulnerabilities.
  - IoT Devices Should Have a Mechanism for Automated, Secure Software Updates: Software bugs should be minimised, but they are inevitable. Thus, it is critical for an IoT device to have a mechanism for automatic, secure software updates. BITAG recommends that manufacturers of IoT devices or IoT service providers should therefore design their devices and systems based on the assumption that new bugs and vulnerabilities will be discovered over time. They should design systems and processes to ensure the automatic update of IoT device software, without requiring or expecting any type of user action or even user opt-in.
  - IoT Devices Should Use Strong Authentication by Default: BITAG recommends that IoT devices be secured by default (e.g. password protected) and not use common or easily guessable user names and passwords (e.g., "admin", "password").
  - IoT Device Configurations Should Be Tested and Hardened: Some IoT devices allow a user to customise the behaviour of the device. BITAG recommends that manufacturers test the security of each device with a range of possible configurations, as opposed to simply the default configuration.

- IoT Devices Should Follow Security & Cryptography Best Practices: BITAG recommends that IoT device manufacturers secure communications using Transport Layer Security (TLS) or Lightweight Cryptography (LWC). If devices rely on a public key infrastructure (PKI), then an authorised entity must be able to revoke certificates when they become compromised, and manufacturers should take care to avoid encryption methods, protocols, and key sizes with known weaknesses. Additional encryption best practices include:
  - Encrypt Configuration (Command & Control) Communications by Default
  - Secure Communications To and From IoT Controllers
  - Encrypt Local Storage of Sensitive Data
  - Authenticate Communications, Software Changes, and Requests for Data
  - Use Unique Credentials for Each Device
  - Use Credentials That Can Be Updated
  - Close Unnecessary Ports and Disable Unnecessary Services
  - Use Libraries That Are Actively Maintained and Supported

[158] Broadband Internet Technical Advisory Group.

- IoT Devices Should Be Restrictive Rather Than Permissive in Communicating: When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.

- IoT Devices Should Continue to Function if Internet Connectivity is Disrupted: BITAG recommends that an IoT device should be able to perform its primary function or functions (e.g., a light switch or a thermostat should continue to function with manual controls), even if it is not connected to the Internet because Internet connectivity may be disrupted due to causes ranging from accidental misconfiguration to intentional attack. IoT devices that have implications for user safety should continue to function under disconnected operation to protect the safety of consumers.

- IoT Devices Should Continue to Function If the Cloud Back-End Fails: Many services that depend on or use a cloud back-end can continue to function, even if in a degraded or partially functional state, when connectivity to the cloud back-end is interrupted or the service itself fails.

- IoT Devices Should Support Addressing and Naming Best Practices: Many IoT devices may remain deployed for a number of years after they are installed. Supporting the latest protocols for addressing and naming will ensure that these devices remain functional for years to come.
    - IPv6: BITAG recommends that IoT devices support the most recent version of the Internet Protocol, IPv6.
    - DNSSEC: BITAG recommends that IoT devices support the use or validation of DNS Security Extensions (DNSSEC) when domain names are used.
    - IoT Devices Should Ship with a Privacy Policy That is Easy to Find & Understand: BITAG recommends that IoT devices ship with a privacy policy, but that policy must be easy for a typical user to find and understand.

- Disclose Rights to Remotely Decrease IoT Device Functionality: BITAG recommends that if the functionality of an IoT device can be remotely decreased by a third party, such as by the manufacturer or IoT service provider, this possibility should be made clear to the user at the time of purchase.

- The IoT Device Industry Should Consider an Industry Cybersecurity Program: BITAG recommends that the IoT device industry or a related consumer electronics group consider the creation of an industry-backed program under which some kind of “Secure IoT Device” logo or notation could be carried on IoT retail packaging. An industry-backed set of best practices seems to be the most pragmatic means of balancing innovation in IoT against the security challenges associated with the fluid nature of cybersecurity, and avoiding the “checklist mentality” that can occur with certification processes.

- The IoT Supply Chain Should Play Their Part In Addressing IoT Security and Privacy Issues: End users of IoT devices depend upon the IoT supply chain, from manufacturer to retailer, to protect their security and privacy, and some or all parts of that IoT supply chain play a critical role throughout the entire lifecycle of the product. In addition to other

recommendations in this section, BITAG recommends that the IoT supply chain takes the following steps:

- Privacy Policy: Devices should have a privacy policy that is clear and understandable, particularly where a device is sold in conjunction with an ongoing service.
- Reset Mechanism: Devices should have a reset mechanism for IoT devices that clears all configuration for use when a consumer returns or resells the device. The device manufacturers should also provide a mechanism to delete or reset any data that the respective device stores in the cloud.
- Bug Reporting System: Manufacturers should provide a bug reporting system with a well-defined bug submission mechanisms and documented response policy.
- Secure Software Supply Chain: Manufacturers should protect the secure software supply chain to prevent introduction of malware during the manufacturing process; vendors and manufacturers should take appropriate measures to secure their software supply chain.
- Support IoT Device for Entire Lifespan: Manufacturers should support an IoT device throughout the course of its lifespan, from design to the time when a device is retired, including transparency about the timespan over which they plan to provide continued support for a device, and what the consumer should expect from the device's function at the end of the device's lifespan.
- Clear Contact Methods: Manufacturers should provide clear methods for consumers to determine who they can contact for support and methods to contact consumers to disseminate information about software vulnerabilities or other issues.
- Report Discovery and Remediation of Vulnerabilities: Manufacturers should report discovery and remediation of software vulnerabilities that pose security or privacy threats to consumers.
- Clear Vulnerability Reporting Process: Manufacturers should provide a vulnerability reporting process with a well-defined, easy-to-locate, and secure vulnerability reporting form, as well as a documented response policy.

7.8. OWASP

7.8.1. IoT Security Guidance

The Open Web Application Security Project (OWASP) published a list of guidelines on IoT security with the purpose to educate manufacturers, developers and consumers on how to design, develop and purchase IoT products that are more robust against cyber-incidents. A set of general recommendations is outlined for the three categories of stakeholders. Here, we summarise these general guidelines for manufacturers, developers and consumers of IoT goods. The list of detailed recommendations can be found in OWASP, 2017.[159]

Manufacturers

The utility of IoT devices depends on the network in which they are used. As such, each device needs to be, by design, flexible enough to allow for updates in case a security flaw is discovered which threatens the network. The ability to update devices as frequently as necessary is a necessary attribute for a robust appliance against enduring vulnerabilities. All devices need to be accurately arranged, in particular rebranded applications, to avoid accidentally having overlapping or useless connection paths active.

Developers

Developers should focus on *proactively* addressing specific concerns that have been identified in relation to IoT devices to develop a robust and secure structure for IoT-based networks. These concerns include avoiding problems of account harvesting in all types of user interfaces. For instance, developers should (i) develop security systems that require stronger passwords from users, (ii) strengthen accounts' lockout options after a given number of erroneous passwords trials, and (iii) guarantee that "valid user accounts" cannot be "identified by interface error messages". These recommendations apply to any application level, from mobile and cloud-based applications to the use of local devices such as a user's own computer.

Consumers

Consumers include users who wish to acquire a device or who are looking to connect to a system. How secure a device or a system is will determine how attractive it is for the buyer. Among others, the protection of consumers' privacy rights is a fundamental component that needs to be included in the design of IoT devices. Applications that entail security characteristics will hence be considered more favourably than others by the end-user. Consumers need to be informed about the build-in security options of the devices that they wish to acquire and need to adopt, in parallel, security best practices in their use of these devices. For instance, best practices include using firewalls when displacing an IoT appliance from a network to another.

[159] OWASP, "IoT Security Guidance - OWASP," accessed May 4, 2018, https://www.owasp.org/index.php/IoT_Security_Guidance.

7.9. OneM2M

7.9.1. OneM2M technical specification

From a technical perspective, the protection of privacy can be addressed in different ways. In order to facilitate such task, OneM2M has released technical specifications for a machine to machine communication system (M2M).[160] M2M designates the communication between various appliances based on wired or wireless connections (see (Machine-to-Machine (M2M) communication challenges established (u)sim card technology, 2018)[161] and Watson, 2018[162]). It is mostly used to communicate data recorded from a device peripheral to a system to a software at the centre of the system. For instance, remote sensors record levels of temperature and communicate this information to a system software to be analysed. With IoT appliances, M2M communication patterns are more complex and form a system of networks communications between nodes. Thanks to a well-designed M2M system, installed in either hardware or software or both, an infinite number of devices can be connected to each other, thereby facilitating the connectivity of IoT devices.

To guarantee the protection of privacy rights, OneM2M propose a data management framework which architecture builds on users' own preferences. Its embedded privacy policy manager (PPM) establishes access controls based on individual preferences over privacy and protects people's personally identifiable information (PII) against illegitimate users. The PPM is managed by a *M2M* service provider who can only transmit information about the IPP of a user to other a third party after having received her explicit consent. Each user thus has a control on the policy ruling the privacy of their personally identifiable information (PII).

7.10. Cloud Security Alliance

7.10.1. Security Guidance for Early Adopters of the Internet of Things (IoT)

The Internet of Things (IoT) represents a technologically optimistic future where objects will be connected to the internet and make intelligent collaborations with other objects anywhere, anytime. Although it makes appreciable development, there are still uncertainties about security concepts of its usage that is usually considered as a major concern in the design of IoT architectures.

This paper presents a general survey of all the security issues in IoT along with an analysis of IoT architectures. The study defines security requirements and challenges that are common in IoT implementations and discusses security threats and related solutions on each layer of IoT architecture to make this technology secure and more widespread accordingly.

More specifically, the paper is aimed at helping early adopters understand the security challenges surrounding the Internet of Things (IoT), and providing recommended security controls and sample use-cases for organisations implementing IoT capabilities. These controls have been tailored to IoT-specific characteristics to allow early adopters to mitigate many of the risks associated with this new technology.

[160] OneM2M technical specification, 2016, oneM2M Partners Type 1 (ARIB, ATIS, CCSA, ETSI, TIA, TSDSI, TTA, TTC)
[161] "Machine to Machine," *Wikipedia*, April 16, 2018, https://en.wikipedia.org/w/index.php?title=Machine_to_machine&oldid=836694555.
[162] David Watson et al., "Machine to Machine (M2M) Technology in Demand Responsive Commercial Buildings," 2004.

CSA is supporting the industry by decomposing the common devices types, markets and architectures of the IoT, and subsequently analysing and recommending appropriate security mitigations across these commonalities

Recommended security controls detailed in the report include:

- Analyse privacy impacts to stakeholders and adopt a privacy-by-design approach to IoT development and deployment.
- Apply a Secure Systems Engineering approach to architecting and deploying a new IoT SoS.
- Implement layered security protections to defend IoT assets.
- Define life-cycle controls for IoT devices.
- Define and implement an authentication/authorisation framework for the organisation's IoT deployments.
- Define and implement a logging/audit framework for the organisation's IoT ecosystem.
- Develop safeguards to assure the availability of IoT-based systems and data.
- Information sharing and support of a global approach to combating security threats by sharing threat information with security vendors, industry peers and Cloud Security Alliance.

7.10.2. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

The "Security Guidance for Critical Areas of Focus in Cloud Computing" gives an overview of the best practices in the field of cloud computing and serves as a practical roadmap for organisations using cloud services. The document offers an update about the technological advances in cloud security, discusses cloud security practices and provides guidance for related technologies.

The document is structured around 14 domains, including:

- Domain 1: Cloud computing concepts and architectures – which offers a conceptual framework, describes cloud computing, outlines the terminology and explains the architectural framework used in the publication.
- Domain 2: Governance and enterprise risk management – discusses how governance and risk management change in the field of cloud computing.
- Domain 3: Legal issues, contracts and electronic discovery – addresses the legal concerns arising by moving data to the cloud, contracting with cloud service providers and managing litigation issues.
- Domain 4: Compliance and audit management – presents the interaction between cloud computing and the auditing bodies.
- Domain 5: Information governance – tackles the ways in which information should be managed so that it complies with regulatory, contractual and business objectives.
- Domain 6: Management plane and business continuity – highlights the importance of the management plane in connecting and configuring the cloud.
- Domain 7: Infrastructure security – addresses infrastructure and networking security, as well as the fundamentals for private cloud computing.
- Domain 8: Virtualisation and containers – explains the impacts of virtualisation on security.
- Domain 9: Incident response – identifies the incident response vulnerabilities created by the unique characteristics of cloud computing.

- Domain 10: Application security – focuses on: "How application security differs in cloud computing; Reviewing secure software development basics and how those change in the cloud; Leveraging cloud capabilities for more secure cloud applications."[163]
- Domain 11: Data security and encryption – discusses the controls related to securing data, with special focus being granted to encryption mechanisms.
- Domain 12: Identity, entitlement and access management – addresses the identity, entitlement and access management issues between an organisation and cloud providers or between cloud providers and services.
- Domain 13: Security as a service – presents the most common 'security as a service' providers available on the market.
- Domain 14: Related technologies – discusses technologies related to cloud computing which bring new concerns into the cybersecurity picture.

7.11. Global System for Mobile Communications Association (GSMA)

7.11.1. IoT Security Guidelines Overview

The GSMA has published its "IoT Security Guidelines Overview"[164] for the benefit of service providers who are looking to develop new IoT services.

More specifically, this document is the first part of a set of GSMA security guideline documents that are intended to help the nascent "Internet of Things" industry establish a common understanding of IoT security issues.

The set of guideline documents promotes a methodology for developing secure IoT Services to ensure security best practices are implemented throughout the life cycle of the service. The documents provide recommendations on how to mitigate common security threats and weaknesses within IoT Services. They serve as an overarching model for interpreting what aspects of a technology or service are relevant to implementer. Once these aspects, or components, are identified, the implementer can evaluate the risks associated with each component, and determine how to manage them.

The primary audience for this document are:

- IoT Service Providers - enterprises or organisations who are looking to develop new and innovative connected products and services. Some of the many fields IoT Service Providers operate in include smart homes, smart cities, automotive, transport, heath, utilities and consumer electronics.
- IoT Device Manufacturers - providers of IoT Devices to IoT Service Providers to enable IoT Services.
- IoT Developers - build IoT Services on behalf of IoT Service Providers.
- Network Operators who are themselves IoT Service Providers or build IoT Services on behalf of IoT Service Providers.

[163] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," 2017, https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf.
[164] GSMA, "IoT Security Guidelines Overview Document," *Internet of Things* (blog), accessed May 4, 2018, https://www.gsma.com/iot/iot-security-guidelines-overview-document/.

The following recommendations are taken from the list of critical and high priority recommendations developed in the documents.

For mobile devices, the recommendations are:
- Implement an Endpoint Trusted Computing Base
- Manage terminals passwords
- Use a trusted certificate
- Detecting anomalies
- Use of components resistant to attack
- Ensure secure communications

For mobile services, the recommendations are:
- Develop a public systems safety.
- Set an incident response model.
- Establish a clear authorisation model.
- Manage the cryptographic architecture.
- Define a communication model.
- Prepare the servers.

For network security, the recommendations are:
- Ensure identification and authentication.
- Protect data and communications.

7.12. National Institute of Standards & Technology (NIST)

7.12.1. NIST SP 800-82r2 – Guide to Industrial Control Systems (ICS) Security

This special publication focuses on securing industrial control systems (ICS). ICS are found in a multitude of industries including electric, water, oil, natural gas, pharmaceutical, chemical, food and beverage, and manufacturing. Such widespread technologies come with various levels of risks. The document seeks to provide support for "securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control system (DCS), and other systems performing control functions."[165] The standard provides a general overview of ICS typologies, identifies recurrent threats and vulnerabilities and suggests security countermeasures to alleviate related risks.

The second chapter of the document is dedicated to a brief overview of industrial control system, their link with SCADA, distributed control systems and programmable logic controllers. Industrial system can be fully automatic or require human participation. The chapter is complemented with the chapter 2.1 on the evolution of industrial controls, which describes the evolution of industrial control systems and their progressive integration with IT-systems.

[165] Keith Stouffer et al., "NIST SP 800-82r2 Guide to Industrial Control Systems (ICS) Security" (National Institute of Standards and Technology, June 2015), https://doi.org/10.6028/NIST.SP.800-82r2.

One of the most important sections of the chapter, section 2.3.1, is entitled "ICS system design consideration" and describes the factors affecting the design and the security needs of the system:

- Control timing requirements
- Geographic distribution
- Hierarchy
- Control complexity
- Availability
- Impact of failures
- Safety

The third chapter of the document focuses on ICS risk management and assessment. The list of risk and vulnerabilities and incidents is tackled in Appendix C. Additionally, the chapter puts a strong focus on the risk management process and identifies four interdependent elements:

- Framing: establishing a framework for the risk management decisions to be made
- Assessing: identifying the risks and vulnerabilities and estimating their likelihood of occurrence
- Responding: identifying the possible responses to risk and selecting the best one
- Monitoring: continuous monitoring of strategies, of the environment and of the effectiveness of the strategies.

In the case of an ICS risk assessment, the following additional considerations need to be taken into account:

- "impacts on safety and use of safety assessments
- physical impact of a cyber incident on an ICS, including the larger physical environment; effect on the process controlled, and the physical effect on the ICS itself
- the consequences for risk assessments of non-digital control components within an ICS."[166]

The chapter 4 of NIST SP 800-82r2 entitled "ICS security program development and deployment". It elaborates on how organisations should develop and deploy an ICS security programme. The six stages of the programme are summarised in the table below.

Table 8-2 : ICS security program process

ICS security program process	Details
Develop a business case for security	"The business case provides the business impact and financial justification for creating an integrated information security program."
Build and train a cross-functional team	The information security team should consist of members with a diverse knowledge. The team should report to the information security manager.
Define charter and scope	A specific policy should detail the rules of the information security organisation and specify the roles, responsibilities and accountabilities of system owners, managers and users.

[166] Stouffer et al.

Define specific ICS policies and procedures	ICS policies and procedures should be included with operation/management policies and procedures.
Implement an ICS Security Management Framework	Managers should refer to NIST.SP 800-39 to define their risk management programme. Additionally, the following elements are required: - ICS assets should be defined and inventoried - A security plan for ICS systems should be established - Risk assessment should be carried out - Mitigation controls should be outlined
Provide training and raise security awareness for ICS staff	Staff should be educated on security issues around ICS systems

The fifth chapter of NIST SP 800-82r2 entitled "ICS security architecture" tackles network security, particularly:

- Network segmentation and segregation
- Boundary protection
- Firewalls
- Logically separated control networks
- Recommended defence-in-depth architecture for the protocols DHCP, SSH, SOAP

Furthermore, in the sixth chapter "Applying security controls to ICS", the document states that the use of a single security measure or technology does not fully protect ICS. Indeed, the following questions should be answered:

1. "*Which security controls are needed to adequately mitigate risk to an acceptable level that supports the organisational missions and business functions?"*
2. *"Have the selected security controls been implemented or is there a realistic implementation plan in place?"*
3. *"What is the required level of assurance that the selected security controls are implemented correctly, operating as intendent and producing a desired outcome?"*

The chapter also outlines the six relevant steps on how the Risk Management Framework (RMF) should be applied to ICS:

Step 1: Categorise the information system according to the potential impact loss.
Step 2: Select security controls
Step 3: Implement security controls
Step 4: Assess security controls
Step 5: Authorise information system
Step 6: Monitor security controls

7.13. International Telecommunication Union (ITU)

7.13.1. ITU-T X.805 Security Architecture for Systems Providing End-To-End Communications

This ITU recommendation defines a network security architecture for delivering end-to-end network security. It is applicable to any network technology (including wireless, optical networks, voice, data,

video, etc.) and to various networks (service provider networks, government networks, administrative networks, company networks, etc.). The document is intended as a base for drafting more elaborate recommendations on end-to-end network security. The security architecture covers three principal questions, each of them tackled by three architectural components: security dimensions, security layers and security planes. The questions are:

1) What type of protection is required and against what type of threat?
2) What specific kinds of network equipment and facility groupings require protection?
3) What specific kinds of network activities require protection?

The publication introduces the topic of security dimensions. A security dimension is a collection of security measures which seeks to respond to a specific facet of the network security. In this recommendation, the ITU outlines eight security dimensions which protect against the main security hazards:

1) Access control: limit and control access to network elements, services and applications
2) Authentication: confirm the identity of the entities engaging in communication
3) Non-repudiation: prevent the faculty to deny that an action on the network took place
4) Data confidentiality: guarantee confidentiality of data
5) Communication security: guarantee information is only transferred from the source to destination
6) Data integrity: guarantee that information is delivered as sent or regained as stored
7) Availability: guarantee that network elements, services and applications are accessible to authentic users
8) Privacy: guarantee that both identification and network use are private

Furthermore, the document also introduced the concept of security layers which offer a hierarchical method to securing a network. The three security layers are:

- The infrastructure security layer: the infrastructure security layer is made out of the network transmission facilities and individual network elements protected by the security dimensions.
- The services security layer: the services security layer tackles the services delivered by service providers to customers.
- The application security layer: the application security layer covers the security of the network-based applications accessed by service provider customers.

The document further specifies that “the security layers identify where security must be addressed in products and solutions by providing a sequential perspective of network security. For example, first security vulnerabilities are addressed for the infrastructure layer, then for the services layer and, finally, security vulnerabilities are addressed for the applications layer.”[167]

Next, the report discusses the concept of “security planes”, defined as a “type of network activity protected by security dimensions”. The three security planes identified are:

[167] International Telecommunications Union, “Recommendation X.805: Security Architecture for Systems Providing End-to-End Communications,” October 29, 2003.

1) Management plane: the management plane addresses the management and provisioning of network elements, services and applications
2) Control plane: the control plane involves activities which allow effective performance of the network
3) End-user plane: it addresses the access and use of the network by the customers

Finally, the Recommendation reminds of the relevant security threats previously described in ITU-T Rec. X.800:

- Destruction of information and/or other resources
- Corruption or modification of information
- Theft, removal or loss of information and/or other resources
- Disclosure of information
- Interruption of services

The final product of the recommendation is a mapping of security dimensions to security threats, showed under the Figure 6-1 below. The intersection between each security layer with each security plane indicates a security perspective where security dimensions are applied to counteract the threats. The letter "Y" indicates that a specific security threat is opposed by a corresponding security dimension.

Security dimension	Security threat				
	Destruction of information or other resources	Corruption or modification of information	Theft, removal or loss of information and other resources	Disclosure of information	Interruption of services
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Data confidentiality			Y	Y	
Communication security			Y	Y	
Data integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

Figure 8-1 : Mapping of security dimensions to security threats (source: X.805)

7.13.2. ITU-T X.1313 Security Requirements for Wireless Sensor Network Routing

This recommendation outlines the security requirements for wireless sensor network (WSN) routing and discusses:

- General network topologies and routing protocols for WSN
- Security threats in WSN routing
- Security requirements for WSN routing

A wireless sensor network consists of more than one base station and multiple sensors. WSN nodes can be classified into three types of network typology:

- The star typology, where each node is linked to a central node called the base station. All sensors transmit data with their base station. The principle of neighbour discovery is used between the base station and the sensors, through which the base station notifies its presence with its ID and location data. In this case scenario, routing configuration is not required since the sensors transmit the sensed information to their base station.
- The tree typology, in which the base station and sensors establish their presence by notifying each other so that the tree network can be set up. In this configuration, each sensor locates the path to the base station for arranging the routing table after neighbour discovery.
- The mesh typology, with at least two nodes with two or more paths connecting them. The routing set-up is similar to the one in the tree typology.

The ITU-T highlights the following requirements for the sensor and base station:

- "The base station and sensor are each required to have an authenticator and the key to identify and authenticate each other initially.
- Information stored in the base station and all sensors – especially information on sensed data, ID, and location is required for encryption and authentication.
- To counter insider attacks, it is recommended that the base station guarantees node integrity such as TPM.
- It is recommended that the base stations are allowed the sensor-node list initially for access control before configuration of the sensor network.
- It is recommended that the sensor authorises the ID for access control before configuration of the sensor network.
- It is recommended that the base station be fault-tolerant, i.e., with regard to duplication and smooth replacement.
- It is recommended that the base station is recommended to have a tamper-proofing mechanism installed in its hardware support, secure bootstrapping, OS enhancements, and software authentication and validation, i.e., by using TPM or sandbox technology.
- The sensor can optionally have fault-tolerance or tamper-proofing.
- The base station can optionally be protected by IDS/IPS or a firewall if it is a wire-lined device.
- For countering insider attacks, sensors can optionally support node integrity."[168]

8. Analysis

This section will be divided into three distinct elements. First, 8.1 explains the methodology we have used to identify the most relevant standards in the field of cybersecurity. 8.2 presents the cybersecurity management matrix where the standards analysed throughout sections 3 through 6 will be examined with regards to the cybersecurity threats identified in section 2.2. Finally, 8.3 will aim to define the optimal combinations of standards necessary to maximize protections vis-à-vis today's top cybersecurity threats.

[168] International Telecommunications Union, "Recommendation X.1313: Security Requirements for Wireless Sensor Network Routing," October 14, 2012, http://www.itu.int/rec/T-REC-X.1313-201210-I/en.

8.1. Methodology to Identify the Most Relevant Cybersecurity Standards

As previously discussed in section 2.1 of this deliverable, cybersecurity threats rapidly grow not only in number but also in nature and intensity. With the introduction of the GDPR, organisations worldwide are required to adapt to the new European regulation in the field of data protection, and may find themselves in financial, legal and image ruins shall they fail to comply.

In the context of this research, we have followed a methodology to help identify the most relevant standards in the field of cybersecurity. To this end, we have created a cybersecurity management matrix that analyses all the international standards covered in sections 3 to 6 of this deliverable and indicates whether or not they address today's most pressing cybersecurity risks. In order to build our matrix, we have based ourselves on our selection of the top 18 cybersecurity risks previously outlined in section 2.3, which reflects the priorities and the main cybersecurity challenges faced by the public and private sectors. The purpose of the cybersecurity management matrix is twofold:

- It allows to identify the smallest combinations of standards offering the best coverage against the greatest number of risks. These "optimal" combinations will be a useful tool for organisations looking for cybersecurity solutions and struggling to navigate through the myriad of complex international standards available on the market. Additionally, the output of the cybersecurity management matrix may serve as an original certification model which could be recommended to insurance companies.

- It allows to identify the cybersecurity gaps which are not readily addressed in the international standards but are listed as important cybersecurity threats, and therefore require additional attention from organisations and standardisation bodies.

Our methodology is based on the following two criteria:

1) Maximum risk coverage at lower cost: Due to financial limitations, organisations cannot afford to implement an unlimited number of international standards to protect themselves against cybersecurity threats. Indeed, the implementation of an international standard comes with internal and external costs, and often requires time-consuming employee training. In order to minimise these costs, we recommend the smallest combination of standards offering the maximum cybersecurity risk coverage.

2) Complementarity: In our analysis, we favour a systemic and holistic approach which strives to put forward those standards that are compatible and complementary to each other. The objective of a systemic approach is to identify the most effective way to deliver reliable and optimal outputs.

The results of the cybersecurity management matrix are presented in the section below. An "x" indicates that a specific cybersecurity risk has been addressed by the related international standard.

8.2. Cybersecurity Management Matrix

	Standard	Cybersecurity threat																	
		Malware	Ransomware	Web-based attacks	Mobile threats	Denial of service	Botnets	Identity theft	Data breaches	Cloud service abuse	Information leakage	Insider threat	Phishing	Spam	Darknet	Child sexual exploitation online	Cyberespionage	Cyberterrorism	Personal data breach
Fundamental Sources	ISO/IEC 27000	x	x		x			x	x		x	x							
	NIST SP 800-183					x			x		x								
	NIST IR 7628 Revision 1			x					x										
	NIST SP 1500-201							x	x		x								
	ITU-T X.1205							x	x		x								
	ITU-T X.1275							x	x		x								
	ETSI TR 103 304	x	x		x			x	x	x	x								
	Publically Available Standard (PAS) 555							x	x		x								
Frameworks	ISO/IEC 24760							x	x		x	x							
	ISO/IEC 27001	x	x	x		x		x	x		x	x	x	x					
	ISO/IEC 27002	x	x		x			x	x		x	x							
	ISO/IEC 27017									x									
	ISO/IEC 27018							x	x	x	x	x							
	ISO/IEC 29100							x	x		x								
	ISO/IEC 29101							x	x		x								
	ISO/IEC 29151							x	x		x								
	ISO/IEC 29180					x			x		x								
	ISO/IEC 31000	x	x	x	x	x	x	x	x	x	x	x	x	x			x	x	
	ISO 22301:2012	x	x	x	x	x	x	x	x	x	x	x	x					x	
	ISO 22313:2012	x	x	x	x	x	x	x	x	x	x	x	x					x	
	BS 10012:2009								x										x
	NIST SP 800-37	x	x	x	x	x	x	x	x	x	x	x					x	x	
	NIST SP 800-53r4	x	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x
	NIST SP 800-121 Revision2								x		x								
	NIST SP 800-122					x		x	x		x								
	NIST SP 800-126 Revision 2	x			x				x				x						
	NIST SP 800-144							x	x	x	x								
	NIST SP 800-150							x	x		x								
	NIST - Framework for Improving Critical Infrastructure Cybersecurity	x	x	x	x	x	x	x	x	x	x	x	x	x			x	x	
	ITU-T X.810							x	x		x								
	ITU-T X.816	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x
	ITU-T X.1171			x				x	x		x								
	ITU-T X.1206	x	x	x	x	x	x	x	x	x	x	x	x	x					
	ITU-T X.1209								x										
	ITU-T X.1251							x	x		x		x						
	ETSI TR 103 331	x	x	x	x	x	x	x	x	x	x	x	x	x					
	ETSI TR 103 305	x	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x
	COBIT 5			x				x	x		x	x	x	x	x	x	x	x	
	ISA 62443	x	x	x	x	x	x		x	x									
	Publicly Available Standard (PAS) 555							x	x		x								
Evaluation	ISO/IEC 15408	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	ISO/IEC 18043	x															x		
	ISO/IEC 18045	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	ISO/IEC 27005	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	ISO/IEC 27006	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	ISO/IEC 27007	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	ISO/IEC 29134	x	x	x	x	x	x	x	x		x	x	x				x		x
	ISO/IEC 29190							x	x		x	x					x		x
	NIST SP 800-30r1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	NIST SP 800-53Ar4	x	x	x	x	x	x	x	x	x	x	x	x	x			x	x	
	NIST SP 800-115	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	NIST SP 800-161	x	x	x	x	x	x	x	x	x	x	x	x	x			x	x	x
	NIST IR 8062							x	x		x	x							x
	ITU-T X.1208	x			x			x	x		x	x		x					x
	ETSI TR 103 301	x		x	x			x	x		x		x	x					
	Publically Available Standard (PAS) 555							x	x		x								
	BSI Standard 100	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	MAGERIT	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	UPRAAM							x	x		x								x
Cert	EuroPrivacy	x	x	x	x	x		x	x		x								x
	EuroPriSe								x		x								x

8.3. Selection of Relevant Combinations of Standards

A standard is seldom implemented in isolation. Typically, given the constant interaction between technologies, processes, and management practices, organisations will opt for a combination of standards.

In the context of this research, we have established our own selection of relevant combinations of standards. As explained in section 9.1, our approach consisted in choosing the smallest combination of standards, which guarantees the maximum cybersecurity risk coverage. Furthermore, complementarity amongst the standards was also a pertinent criterion that has played a role in our selection.

Our combination of standards contains a variety of sources, including from ISO and NIST. Although NIST standards are proper to the United States, they are largely used by European industry and are de facto applied as global standards.

We started by selecting standards and references that are covering at least a third of the identified threats: 6 or more threats. According to our matrix, we get a selection of the following references and standards:

- BSI Standard 100
- COBIT5
- ETSI TR 103 305
- ETSI TR 103 331
- ETDI TR 103 304
- EuroPrivacy
- ISA 62443
- ISO/IEC 15408
- ISO/IEC 22301
- ISO/IEC 27000
- ISO/IEC 27001
- ISO/IEC 27002
- ISO/IEC 29190
- ISO/IEC 31000
- ITU-T X.1206
- ITU-T X.1208
- ITU-T X.816
- MAGERIT
- NIST - Framework for Improving Critical Infrastructure Cybersecurity
- NIST SP 800-53

After analysing this initial list, a number of standards and references were considered to be either too closely related or inadequate for our purposes, namely:

- ISO/IEC 31000 is implicitly used by ISO/IEC 27001 which requires a formal risk analysis by the certified organisation. It can be used as a complementary reference in the context of an ISO/IEC 27001 certification.
- ISO/IEC 27002 constitutes a detailed catalogue of security measures which are included in and mapped by the Annex of ISO/IEC 27001 - the latter constituting the de facto reference formal Information Security Management Systems (ISMS) certification.
- ETSI TR 103 331 constitutes a very interesting technical report on information sharing but is not adequate for cybersecurity conformance assessment.
- ETSI TR 103 304 - Personally Identifiable Information (PII) Protection in mobile and cloud services is a report and is not detailed enough to serve as a comprehensive certification scheme.
- MAGERIT and BSI's 100 family of standards introduce a nationally recognised methodologies and recommendations, however their potential for implementation might be limited as they have been generated by a national authority, which might clash with similar tools available at a national level in other countries.
- NIST - Framework for Improving Critical Infrastructure Cybersecurity provides a comprehensive framework that refers formally to formal requirements specified in other standards, mainly: COBIT 5, ISO/IEC 27001, and NIST SP 800-53.

As a result, the following standards are to be considered:

- BSI Standard 100
- COBIT5
- ETSI TR 103 305
- EuroPrivacy
- ISA 62443
- ISO/IEC 15408
- ISO/IEC 22301
- ISO/IEC 27000
- ISO/IEC 27001
- ISO/IEC 29190
- ITU-T X.1206
- ITU-T X.1208
- ITU-T X.816
- NIST SP 800-53

From this list, several standards covering a similar scope can be identified and implemented depending on the context of each organisation, namely:

- COBIT5: The latest revision of this standard has aimed to enhance its compatibility with IT functions and processes with business strategy. Furthermore, it represents a significant resource for the development of a governance framework within an organisation which is not only compatible with other standards (such as ISO 27001 and NIST SP 800-53), but can be adapted to the specific needs of the organisation through a customisation process. Despite this situation, it is difficult for any organisation to implement the standard in its entirety, as it not only requires precise tailoring to meet organisational needs, but also

requires a strong organisational commitment to the performance of regular internal audits which might be considered intrusive in certain contexts.

- ISO 27001: The standard's international nature, adaptable scope and conciseness of the controls it introduces has led to its wide implementation by multiple industries. Indeed, the simple and flexible language used by the standard makes it easy for newcomers and experienced implementers alike to modify their organisational processes to better protect and manage their IT resources from attacks. Despite this, this standard remains focused on risk management, not security, and for this reason it cannot ensure that the systems (and the information contained therein) will be safe from all and any threats.
- NIST SP 800-53: by introducing the most detailed set of controls, NIST's practical approach when developing this standard led to a wide recognition and implementation of its publication's recommendations by the industry. Despite this situation, the detailed nature of this standard requires significant commitment from the organisation, as continuous monitoring of such a large range of controls is challenging and risks may arise if such monitoring does not take place.

Complementary standards:

- ISA 62443: This standard has a narrower focus, as it is tailored to address the needs of a specific industry group. In this context, some of its elements might be better fitted to address risks in industrial networks than the more generic controls found in NIST SP 800-53.
- ISO 22301: Pursuing implementation of this standard can in some case lead to a higher level of consumer trust. While focused on business continuity, this standard introduces elements which are highly relevant to some of the threats identified in section 2 (particularly those related to disruptions of service).

By comparing the effective scope of each standard, it appears that ISO 27001 and NIST SP 800-53 emerge as leading solutions to provide a comprehensive coverage of cybersecurity threats and risks, and while their scopes could be further enhanced through the introduction of some of the governance models found in COBIT 5.

However, the introduction requires to extend the scope of cybersecurity risks with the obligations related to personal data protection. Effectively, the main problem identified so far is the potential issues that might arise when attempting to implement their controls and methodologies in the European context, where certain elements (such as the different relevance and organisational outlook involved in the protection of personal data) can be significant enough to limit the organisational incentives necessary to develop a (properly) tailored system for each organisation.

Indeed, while ISO 27001 does not by itself raise any major problem in the European context, it lacks the specific and practical set of controls that can be found in NIST SP 800-53. While this might be addressed by the introduction of some of the controls found in other documents like ETSI TR 103 305, the opportunity cost involved in

In this context, both EuroPrivacy and EuroPriSe could be used as a complementary mechanisms to assess the tailored approach introduced by an organisation that chooses to pursue a hybrid approach. In order to determine which of the two certification standards could better assess a tailored approach and easily integrate with cybersecurity standards, a cross examination of relevant documentation reveals that only EuroPrivacy has been specifically designed to be easily combined with ISO/IEC 27001 certification.

As a result, the following combination of certification schemes would enable to ensure a rather comprehensive coverage of cybersecurity risks:

A – Cybersecurity:

- ISO/IEC 27001
- or NIST SP 800-53Ar4 (optional: further tailoring of COBIT5 governance elements)

B – Personal Data Protection (in line with the GDPR):

- EuroPrivacy
- or EuroPriSe

C – Threat Information Dissemination:

- ITU X.1206

D – Evaluation and Benchmarking:

- ISO/IEC 15408
- ITU X.816
- ITU X.1208

9. Recommendations

The following section offers recommendations about cybersecurity standards and discusses 1) the standardisation gaps to be addressed, 2) the need for a better complementarity among standards, 3) potential standard combinations, 4) benchmarking and risk monitoring and 5) the European Strategy and Leadership in Standardisation.

9.1. Standardisation Gaps to Be Addressed

The analysis of the cybersecurity management matrix has shed some light on those cybersecurity areas which are insufficiently covered by international standards and guidelines. Indeed, standardisation gaps indicate the absence of a distinct standard targeted to certain cybersecurity areas. Our research has shown that out of our top 18 cybersecurity risks, two critical areas are not directly addressed in the documents. Those areas include: the darknet and child sexual exploitation online. Furthermore, three other cybersecurity areas are insufficiently covered in the international standards. Those areas are: botnets, cyberespionage and cyberterrorism.

Standards gaps usually appear when technological progress or political realities develop at such a fast pace that standards development cannot keep up. Additionally, such gaps may also reflect the lack of unanimity from standardisation bodies on either the technology or on the details of the standard. Our recommended approach is to put forward these five critical cybersecurity areas on the standardisation organisations' agendas in order to address those standardisation gaps through future standards. Furthermore, in the absence of distinct international standards on these topics, it is recommended that companies and organisations consider preventive solutions against these threats.

9.2. Need for a Better Complementarity Among Standards

Standards may interact in various ways with each other. Indeed, certain standards are "*complementary"*, which signifies that they support or strengthen one another. Usually, in this case, the purpose of the second standard is to further elaborate on a specific aspect of a central issue. For example, ISO/IEC 27002 has been developed to complement the original ISO/IEC 27000. Similarly, ISO/IEC 27018 uses the principles outlined in ISO/IEC 29100. Conversely, certain standards may "*conflict"* with each other, which suggests that certain ambiguities or contradictions between them may lead to technical incompatibility or legal noncompliance. For example, while extensive in their reach and potential for addressing multiple risk vectors, NIST standards are usually focused on the North American context and their implementation might fall short from (or contradict) the tendencies and/or legal contexts of EU countries. An example of this situation can be found in NIST SP 800-53r4: while this standard has great intrinsic value due to the great detail in which it defines security controls and the broad range of interoperable standards available; the way it seeks to protect personally identifiable data and privacy concerns are markedly distant from the views and requirements of the EU GDPR (which considers personal data protection from a holistic and data subject-focused perspective). Finally, a number of standards are "*discrete"*, which means that they have no direct interaction with each other.

The analysis of the cybersecurity management matrix has shown a degree of complementarity between several ISO standards, particularly within the ISO 27000 series. While we have not noted

any conflicting standards, a large number of standards were "discrete" and did not show interaction with one another. Given that cybersecurity management requires a holistic and systemic approach, we recommend a better complementarity between the different families of standards, rather than stand-alone standards.

9.3. European holistic framework for cybersecurity and data protection

We recommend the development and specification of an European comprehensive framework on cybersecurity and data protection, in line with the NIST Framework for Improving Critical Infrastructure Cybersecurity. Such framework would enable the identification of adequate standards and references to be used by European public administrations, SMEs and industry.

9.4. Potential Hybrid Standard Model

According to our analysis, we propose the adoption of a formal standard combination that would enable the delivery of a comprehensive certification. This "SAINT" certificate could be delivered to European legal entities that have a comprehensive coverage of cyber security risks mitigation. Instead of developing a completely new certification scheme, the label could be delivered to any company that is already certified for the identified risks for A and B according to the following matrix, and which performs a complementary certification assessment for C:

Standard		Malware	Ransomware	Web-based attacks	Mobile threats	Denial of service	Botnets	Identity theft	Data breaches	Cloud service abuse	Information leakage	Insider threat	Phishing	Spam	Darknet	Child sexual exploitation online	Cyberespionage	Cyberterrorism	Personal Data Protection breach
A	ISO/IEC 27001	x	x	x	x	x		x	x		x	x	x	x			x		
	NIST SP 800-53Ar4	x	x	x	x	x	x	x	x	x	x	x	x	x			x	x	
	ETSI TR 103 305-4 V1.1.1 (2016-08)	x		x	x			x	x		x		x	x					
B	EuroPrivacy								x		x								X
	EuroPriSe								x		x								X
C	SAINT - complementary certification scheme														X	X			

9.5. Benchmarking and Risk Monitoring

It is proposed to define and use a comprehensive cybersecurity index encompassing the major identified risks. This index could be used to assess the level of risk as well as to benchmark and compare companies and other legal entities. The proposed index can take the following form:

$$SCI = MCT / CT$$

Where:

- SCI refers to SAINT Cybersecurity Index
- MCT refers to the number of threats whose mitigation is certified according to the matrix
- CT refers to the total number of major threats specified by SAINT (currently the 19 identified major threats)

This index can be easily used to assess the level of risk of a specific organisation, as well as to assess, compare and benchmark organisations, public administrations and companies.

9.6. European Strategy and Leadership in Standardisation

The usual strategy for standardisation in Europe is to start by developing regional standards, through ETSI or CENELEC. Once the standard is agreed at the regional level, it is proposed as a global standard to SDOs such as ITU.

By focussing on the regional standardisation, the European voice is often underrepresented and its visions arrive often too late at the ITU to efficiently impact the global standards.

We recommend the adoption of a dual strategy that would encourage Europe to work at both levels in parallel:

- Regional standardisation with a focus on ETSI and CENELEC
- Global standardisation with a focus on ITU, ISO, and IEC

10. Conclusion

In this deliverable, we provide summaries of 22 ISO standards, 20 NIST standards, 11 ITU standards, 6 ETSI standards, and numerous other reports and recommendations from various countries and global organisations. For legibility, we split the standards into four categories: Fundamentals, which describe terminology or what we understand by a particular type of system; Frameworks, which describe procedures and processes for conducting certain tasks; Evaluation, which describes how to assess the effectiveness of certain frameworks and systems; and Systems, which describe technical standards and their implementation.

In section 2, we offer a Contextual Overview in which we address the evolution of cybercrime and cybersecurity risks, the entry into force of the GDPR and propose our own selection of 19 most relevant cybersecurity risks.

In Section 3, Fundamentals, we summarise the requirements for ISMSs, NoTs, Smart Grids, and Cyber-Physical Systems. We also summarise the kinds of cyber-attacks that may affect RFID technologies, mobile and Cloud services, and IoT.

In Section 4, Frameworks, we summarise the best practices for implementing ISMSs, various kinds of security controls, privacy and protection for PII, risk management, business continuity, and cyberthreat information exchange.

In Section 5, Evaluation, we summarise best practices for assessing IT systems and products, risk management systems, security systems, and privacy systems.

In Section 6, Privacy Certification Mechanisms, we introduce the changes brought forward by the GDPR and focus on two certification mechanisms including EuroPrivacy and EuroPriSe.

In Section 7, we present multiple reference documents on privacy and security with the aim to enrich the scope of this deliverable with additional information that will be useful when implementing any of the standards examined in previous sections. As part of this effort, recommendations and guidelines on data protection and privacy impact assessment from several countries are summarised before introducing sector-specific cybersecurity recommendations, reports and publications.

In Section 8, we delve in the analysis section. We outline the methodology for selecting the most relevant standards and present the results of our analysis in a cybersecurity management matrix. In section 8.3, we extract the most relevant combinations of standards.

Finally, in Section 9, we focus on recommendations and discuss 1) the standardisation gaps to be addressed, 2) the need for a better complementarity among standards, 3) potential standard combinations, 4) benchmarking and risk monitoring and 5) the European Strategy and Leadership in Standardisation.

Together, this deliverable presents a sizeable repository of standards and best practices from around the world that one can use to coordinate a cybersecurity strategy for organisational bodies at practically any level.

11. Bibliography

Boyens, Jon M. “NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organisations,” April 2015. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf.

British Standards Institution. “BS 10012:2009 Data Protection. Specification for a Personal Information Management System,” May 2009. https://shop.bsigroup.com/ProductDetail/?pid=000000000030175849.

———. “PAS 555:2013:Cyber Security Risk. Governance and Management. Specification.” BSI, May 2013. https://shop.bsigroup.com/ProductDetail/?pid=000000000030261972.

Broadband Internet Technical Advisory Group. “Internet of Things (IoT) Security and Privacy Recommendations.” Broadband Internet Technical Advisory Group, November 2016. https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

Brooks, Sean, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman, and Ellen Nadeau. “NIST IR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems.” Gaithersburg, MD: National Institute of Standards and Technology, January 2017. https://doi.org/10.6028/NIST.IR.8062.

Brookson, Charles, Scott Cadzow, Ralph Eckmaier, Jörg Eschweiler, Berthold Gerber, Alessandro Guarino, Kai Rannenberg, et al. *Definition of Cybersecurity: Gaps and Overlaps in Standardisation.* Heraklion: ENISA, 2015. http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115934:EN:HTML.

Brown, William. “The Failed Vasa: COBIT 5 Governance and the Seven Enablers (Part 3).” COBIT Focus, October 2014. http://www.isaca.org/Knowledge-Center/Research/Documents/COBIT-Focus-The-Failed-VASA-COBIT-5-Governance-and-the-Seven-Enablers-Part-3_nlt_Eng_1014.pdf.

BSI. “BSI Standard 100-3 - Risk Analysis Based on IT-Grundschutz,” 2008, 23.

———. “BSI-Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS),” 2008, 37.

———. “BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise,” 2008, 95.

———. “BSI-Standard 100-4: Business Continuity Management,” 2008. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1.

Cisco. “Cisco 2018 Annual Cybersecurity Report,” February 2018. https://www.cisco.com/c/en/us/products/security/security-reports.html.

Cloud Security Alliance. “Security Guidance for Critical Areas of Focus in Cloud Computing v4.0,” 2017. https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf.

“ECSO - European Cyber Security Organisation.” ECSO - European Cyber Security Organisation. Accessed May 3, 2018. https://www.ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management.

ECSO - European Cyber Security Organisation. “ECSO State of the Art Syllabus V2,” December 2017, 210.

ENISA. “ENISA Threat Landscape Report 2017.” Heraklion, Greece, January 2018.

———. “Recommendations on European Data Protection Certification,” November 2017.

———. “Towards a New Role and Mandate for ENISA and the European Cyber Security Month.” Brussels, January 2018.

EU GDPR Information Portal. “EU GDPR Information Portal.” EU GDPR Portal. Accessed May 3, 2018. http://eugdpr.org/eugdpr.org.html.

European Parliament, European Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Pub. L. No. 32016R0679, 119 OJ L (2016). http://data.europa.eu/eli/reg/2016/679/oj/eng.

European Telecommunications Standards Institute. “ETSI TR 103 304 - CYBER; Personally Identifiable Information (PII) Protection in Mobile and Cloud Services,” July 2016. http://www.etsi.org/deliver/etsi_tr/103300_103399/103304/01.01.01_60/tr_103304v010101p.pdf.

———. “ETSI TR 103 305 CYBER; Critical Security Controls for Effective Cyber Defence,” May 2015. http://www.etsi.org/deliver/etsi_tr/103300_103399/103305/01.01.01_60/tr_103305v010101p.pdf.

———. “ETSI TR 103 305-2 CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and Auditing,” August 2016. http://www.etsi.org/deliver/etsi_tr/103300_103399/10330502/01.01.01_60/tr_10330502v010101p.pdf.

———. “ETSI TR 103 305-3 CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations,” August 2016. http://www.etsi.org/deliver/etsi_tr/103300_103399/10330503/01.01.01_60/tr_10330503v010101p.pdf.

———. “ETSI TR 103 305-4 CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms,” August 2016. http://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/01.01.01_60/tr_10330504v010101p.pdf.

———. “ETSI TR 103 331 CYBER; Structured Threat Information Sharing,” August 2016. http://www.etsi.org/deliver/etsi_tr/103300_103399/103331/01.01.01_60/tr_103331v010101p.pdf.

Europol. “Child Sexual Exploitation.” Europol. Accessed May 3, 2018. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation.

Griffor, Edward R, Chris Greer, David A Wollman, and Martin J Burns. “NIST SP 1500-201 - Framework for Cyber-Physical Systems: Volume 1, Overview.” Gaithersburg, MD: National Institute of Standards and Technology, June 26, 2017. https://doi.org/10.6028/NIST.SP.1500-201.

GSMA. “IoT Security Guidelines Overview Document.” *Internet of Things* (blog). Accessed May 4, 2018. https://www.gsma.com/iot/iot-security-guidelines-overview-document/.

High Council of the Electronic Administration. *Risk Analysis and Management Methodology for Information Systems*, n.d.

ICO. “Anonymisation: Managing Data Protection Risk Code of Practice,” n.d., 108.

———. “Auditing Data Protection: A Guide to ICO Data Protection Audits,” June 2015. https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf.

———. “Conducting Privacy Impact Assessments Code of Practice,” 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

———. “Data Sharing Code of Practice,” 2011. https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf.

———. “Who We Are,” February 26, 2018. https://ico.org.uk/about-the-ico/who-we-are/.

Information and Privacy Commissioner of Ontario. “Planning for Success: Privacy Impact Assessment Guide,” May 2015. https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf.

International Electrotechnical Commission. “IEC 62443-2-1:2010 Industrial Communication Networks - Network and System Security - Part 2-1: Establishing an Industrial Automation and Control System Security Program,” November 2010. https://webstore.iec.ch/publication/7030.

International Organisation for Standardisation. “ISO 22301:2012 Societal Security -- Business Continuity Management Systems -- Requirements,” May 2012. https://www.iso.org/standard/50038.html.

———. “ISO 22313:2012 Societal Security -- Business Continuity Management Systems -- Guidance,” December 2012. https://www.iso.org/standard/50050.html.

———. “ISO 31000:2018, Risk Management – Guidelines,” 2018. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.

———. “ISO/IEC 15408-1:2009 Information Technology -- Security Techniques -- Evaluation Criteria for IT Security -- Part 1: Introduction and General Model,” January 2014. https://www.iso.org/standard/50341.html.

———. “ISO/IEC 18043:2006 Information Technology -- Security Techniques -- Selection, Deployment and Operations of Intrusion Detection System,” June 2006. https://www.iso.org/standard/35394.html.

———. “ISO/IEC 18045:2008 Information Technology -- Security Techniques -- Methodology for IT Security Evaluation,” August 2008. https://www.iso.org/standard/46412.html.

———. “ISO/IEC 24760-1:2011 Information Technology -- Security Techniques -- A Framework for Identity Management -- Part 1: Terminology and Concepts,” December 2011. https://www.iso.org/standard/57914.html.

———. “ISO/IEC 27000:2016 Information Technology -- Security Techniques -- Information Security Management Systems -- Overview and Vocabulary,” February 2016. https://www.iso.org/standard/66435.html.

———. “ISO/IEC 27001:2013 Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements,” October 2013. https://www.iso.org/standard/54534.html.

———. “ISO/IEC 27002:2013 Information Technology -- Security Techniques -- Code of Practice for Information Security Controls,” October 2013. https://www.iso.org/standard/54533.html.

———. “ISO/IEC 27005:2011 Information Technology -- Security Techniques -- Information Security Risk Management,” June 2011. https://www.iso.org/standard/56742.html.

———. “ISO/IEC 27006:2015 Information Technology -- Security Techniques -- Requirements for Bodies Providing Audit and Certification of Information Security Management Systems,” October 2015. https://www.iso.org/standard/62313.html.

———. “ISO/IEC 27007:2011 Information Technology -- Security Techniques -- Guidelines for Information Security Management Systems Auditing,” November 2011. https://www.iso.org/standard/42506.html.

———. “ISO/IEC 27017:2015 Information Technology -- Security Techniques -- Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services,” December 2015. https://www.iso.org/standard/43757.html.

———. “ISO/IEC 27018:2014 Information Technology -- Security Techniques -- Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors,” August 2014. https://www.iso.org/standard/61498.html.

———. “ISO/IEC 29100:2011 Information Technology -- Security Techniques -- Privacy Framework,” December 2011. https://www.iso.org/standard/45123.html.

———. “ISO/IEC 29101:2013 Information Technology -- Security Techniques -- Privacy Architecture Framework,” October 2013. https://www.iso.org/standard/45124.html.

———. “ISO/IEC 29134:2017 Information Technology -- Security Techniques -- Guidelines for Privacy Impact Assessment,” June 2017. https://www.iso.org/standard/62289.html.

———. “ISO/IEC 29151:2017 Information Technology -- Security Techniques -- Code of Practice for Personally Identifiable Information Protection,” August 2017. https://www.iso.org/standard/62726.html.

———. “ISO/IEC 29180:2012 Information Technology -- Telecommunications and Information Exchange between Systems -- Security Framework for Ubiquitous Sensor Networks,” December 2012. https://www.iso.org/standard/45259.html.

———. “ISO/IEC 29190:2015 Information Technology -- Security Techniques -- Privacy Capability Assessment Model,” August 2015. https://www.iso.org/standard/45269.html.

International Telecommunication Union. “Recommendation X.1251 A Framework for User Control of Digital Identity,” September 2009. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9619.

———. “Recommendation X.1275: Guidelines on Protection of Personally Identifiable Information in the Application of RFID Technology,” December 2010. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1275.

International Telecommunications Union. “Recommendation X.805: Security Architecture for Systems Providing End-to-End Communications,” October 29, 2003.

———. “Recommendation X.810: Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Overview,” November 21, 1995. http://www.itu.int/rec/T-REC-X.810-199511-I.

———. “Recommendation X.816: Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Security Audit and Alarms Framework,” November 21, 1995. https://www.itu.int/rec/T-REC-X.816-199511-I/en.

———. “Recommendation X.1171: Threats and Requirements for Protection of Personally Identifiable Information in Applications Using Tag-Based Identification,” February 20, 2009. https://www.itu.int/rec/T-REC-X.1171-200902-I/en.

———. “Recommendation X.1205: Overview of Cybersecurity,” April 18, 2008. https://www.itu.int/rec/T-REC-X.1251-200909-I.

———. “Recommendation X.1206: A Vendor-Neutral Framework for Automatic Notification of Security Related Information and Dissemination of Updates,” April 18, 2008. http://www.itu.int/rec/T-REC-X.1206-200804-I/en.

———. “Recommendation X.1208: A Cybersecurity Indicator of Risk to Enhance Confidence and Security in the Use of Telecommunication/Information and Communication Technologies,” January 24, 2014. https://www.itu.int/rec/T-REC-X.1208-201401-I/en.

———. “Recommendation X.1209: Capabilities and Their Context Scenarios for Cybersecurity Information Sharing and Exchange,” December 17, 2010. https://www.itu.int/rec/T-REC-X.1209-201012-I/en.

———. “Recommendation X.1313: Security Requirements for Wireless Sensor Network Routing,” October 14, 2012. http://www.itu.int/rec/T-REC-X.1313-201210-I/en.

Interpol. “The Threats / Cybercrime / Crime Areas / Internet / Home - INTERPOL.” Accessed May 3, 2018. https://www.interpol.int/Crime-areas/Cybercrime/The-threats.

ISACA. “ISACA Outlines Five Principles for Effective Information and Technology Governance.” Accessed May 8, 2018. https://www.isaca.org/About-ISACA/Press-room/News-

Releases/2014/Pages/ISACA-Outlines-Five-Principles-for-Effective-Information-and-Technology-Governance.aspx.

Jansen, W, and T Grance. "NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing." Gaithersburg, MD: National Institute of Standards and Technology, 2011. https://doi.org/10.6028/NIST.SP.800-144.

Johnson, Christopher S., Mark Lee Badger, David A. Waltermire, Julie Snyder, and Clem Skorupka. "NIST SP 800-150 Guide to Cyber Threat Information Sharing." National Institute of Standards and Technology, October 2016. https://doi.org/10.6028/NIST.SP.800-150.

Joint Task Force Transformation Initiative. "NIST SP 800-30r1 Guide for Conducting Risk Assessments." Gaithersburg, MD: National Institute of Standards and Technology, 2012. https://doi.org/10.6028/NIST.SP.800-30r1.

———. "NIST SP 800-37r1 - Guide for Applying the Risk Management Framework to Federal Information Systems : A Security Life Cycle Approach." National Institute of Standards and Technology, June 2014. https://doi.org/10.6028/NIST.SP.800-37r1.

"Machine to Machine." *Wikipedia*, April 16, 2018. https://en.wikipedia.org/w/index.php?title=Machine_to_machine&oldid=836694555.

Mandat International. "Privacy Flag Project, Deliverable D2.3 Revision with Simplified UPRAAM." Geneva, 2016.

McAfee Labs. "McAfee Labs 2018 Threats Predictions," November 2017, 1.

McCallister, E, T Grance, and K A Scarfone. "NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." Gaithersburg, MD: National Institute of Standards and Technology, 2010. https://doi.org/10.6028/NIST.SP.800-122.

McKay, Kerry A, Larry Bassham, Meltem Sonmez Turan, and Nicky Mouha. "NIST IR 8114 Report on Lightweight Cryptography." Gaithersburg, MD: National Institute of Standards and Technology, March 2017. https://doi.org/10.6028/NIST.IR.8114.

National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." National Institute of Standards and Technology, February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

———. "NIST SP 800-53, Revision 4 Security and Privacy Controls for Federal Information Systems and Organisations," April 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

New Zealand's Privacy Commissioner's Office. "How to Do a Privacy Impact Assessment (PIA)," July 2015.

Office of the Australian Information Commission. "Guide to Undertaking Privacy Impact Assessments," May 2014, 42.

OWASP. "IoT Security Guidance - OWASP." Accessed May 4, 2018. https://www.owasp.org/index.php/IoT_Security_Guidance.

Padgette, John, John Bahr, Mayank Batra, Marcel Holtmann, Rhonda Smithbey, Lily Chen, and Karen Scarfone. "NIST SP 800-121r2 Guide to Bluetooth Security." Gaithersburg, MD: National Institute of Standards and Technology, May 2017. https://doi.org/10.6028/NIST.SP.800-121r2.

PwC. "Cyber Becomes the Fastest Growing Economic Crime - PwC's Global Economic Crime Survey 2016 - PwC in the North." Accessed May 3, 2018. https://www.pwc.co.uk/who-we-are/regional-sites/yorkshire-north-east/insights/cyber-becomes-the-fastest-growing-economic-crime-pwcs-global-economic-crime-survey-2016.html.

Regenscheid, Andrew. "NIST SP 800-147B BIOS Protection Guidelines for Servers." National Institute of Standards and Technology, January 2008. https://doi.org/10.6028/NIST.SP.800-147B.

Ross, Ronald S. “NIST SP 800-53Ar4 Assessing Security and Privacy Controls in Federal Information Systems and Organisations: Building Effective Assessment Plans.” National Institute of Standards and Technology, December 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4.

Scarfone, K A, M P Souppaya, A Cody, and A D Orebaugh. “NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.” Gaithersburg, MD: National Institute of Standards and Technology, 2008. https://doi.org/10.6028/NIST.SP.800-115.

Schrecker, Sven, Hamed Soroush, Jesus Molina, Jeff Caldwell, David Meltzer, Frederick Hirsch, Jean Pierre Leblanc, and Marcellus Buchheit. “Industrial Internet of Things, Volume G4: Security Framework’ (IISF).” *2016*, n.d., 173.

Singer, Peter W. “The Cyber Terror Bogeyman.” *Brookings* (blog), January 11, 2012. https://www.brookings.edu/articles/the-cyber-terror-bogeyman/.

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. “NIST SP 800-82r2 Guide to Industrial Control Systems (ICS) Security.” National Institute of Standards and Technology, June 2015. https://doi.org/10.6028/NIST.SP.800-82r2.

Symantec Corporation. “Internet Security Threat Report 2018.” Mountain View, California, March 2018.

The Smart Grid Interoperability Panel–Smart Grid Cybersecurity Committee. “NIST IR 7628r1 - Guidelines for Smart Grid Cybersecurity.” National Institute of Standards and Technology, September 2014. https://doi.org/10.6028/NIST.IR.7628r1.

The Spanish Agency for Data Protection. “Guia Práctica de Análisis de Riesgos En Los Tratamientos de Datos Personales Sujetos Al RGPD,” n.d. https://iapp.org/media/pdf/resource_center/Guia_EvaluacionesImpacto.pdf.

———. “Guía Práctica Para Las Evaluaciones de Impacto En La Protección de Los Datos Sujetas Al RGPD,” n.d. https://iapp.org/media/pdf/resource_center/AnalisisDeRiesgosRGPD.pdf.

U.S. Department of Homeland Security. “Strategic Principles for Securing the Internet of Things (IoT),” November 2016, 17.

Voas, Jeffrey M. “NIST SP 800-183 Networks of ‘Things’:” Gaithersburg, MD: National Institute of Standards and Technology, July 2016. https://doi.org/10.6028/NIST.SP.800-183.

Waltermire, David, Stephen Quinn, Karen Scarfone, and Adam Halbardier. “NIST SP 800-126, Revision 2 The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2,” September 2011, 66.

Watson, David, Mary Piette, Osman Sezgen, and Naoya Motegi. “Machine to Machine (M2M) Technology in Demand Responsive Commercial Buildings,” 2004.

Wilson, Matthew. “What Are the 12 Biggest Cloud Computing Security Threats? - Cloud Computing News,” January 4, 2016. https://www.ibm.com/blogs/cloud-computing/2016/04/01/12-biggest-cloud-computing-security-threats/.

