STATE OF THE ART SYLLABUS

Overview of existing Cybersecurity standards and certification schemes

WG1 I Standardisation, certification, labelling and supply chain management

JUNE 2017

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg1_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The document was intended for reference purposes by ECSO WG1 and was allowed to be distributed outside ECSO. Despite the authors' best efforts, no guarantee is given that the information in this document is complete and accurate. Readers of this document are encouraged to send any missing information or corrections to the ECSO WG1, please use wg1_secretariat@ecs-org.eu.

This document integrates the contributions received from ECSO members until April 2017. Cybersecurity is a very dynamic field. As a result, standards and schemes for assessing Cybersecurity are being developed and updated frequently. To take these developments into account, this document may be updated on a regularly basis, each 6 months, based on received contributions.

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources including external websites referenced in this publication.

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION 1

2 Overview 5

2.1 Cybersecurity standards and schemes for products and components (SWG 1.1) 5

2.1.1 Standards and schemes for generic IT products 5
2.1.2 Standards and schemes for products used in Industry 4.0 and ICS (SWG3.1) .. 6
2.1.3 Standards and schemes for products used in energy networks and smart grids (SWG3.2) 6
2.1.4 Standards and schemes for products used in telecom, media and content (SWG3.8) 7
2.1.5 Standards and schemes for products used in the payment industry 7
2.1.6 Standards and schemes for cryptographic modules 8
2.1.7 Standards and schemes for web applications 8
2.1.8 Standards and schemes for IoT products 8
2.1.9 Standards and schemes for other IT products 9

2.2 Standards and schemes for cloud service providers (SWG 1.2) 9

2.3 Standards and schemes for service providers and organisations (SWG 1.3) 10

2.3.1 Standards and schemes for generic organisations 10
2.3.2 Standards and schemes for Industry 4.0 and ICS (SWG 3.1) 13
2.3.3 Standards for energy networks and smart grids (SWG 3.2) 14
2.3.4 Standards and schemes for transportation (road, rail, air, sea) (SWG 3.3) 15
2.3.5 Standards and schemes for financial services and insurance (SWG3.4) 15
2.3.6 Standards and schemes for public services / eGovernment / Digital Citizenship (SWG 3.5) 16
2.3.7 Standards and schemes for healthcare (SWG 3.6) 17
2.3.8 Standards and schemes for smart cities and smart buildings (SWG3.7) 17
2.3.9 Standards and schemes for telecom, media and content (SWG 3.8) 18
2.3.10 Standards and schemes for critical infrastructures 18
2.3.11 Standards and schemes for general secure software development 19
2.3.12 Standards and schemes for cybersecurity service providers 20
2.3.13 Standards and schemes for the payment industry 20
2.3.14 Standards and schemes for IoT device vendors 21

2.4 Standards and schemes for security professionals 22

3 Cybersecurity standards and schemes for products and components 23

3.1 Standards and schemes for generic IT products 23
3.1.1 Certification de Sécurité de Premier Niveau (CSPN) 23

3.1.2 Commercial Product Assurance (CPA) 25
3.1.3 Common Criteria (CC)..... 27
3.1.4 European Privacy Seal..... 31
3.1.5 National IT Evaluation Scheme (NITES) 33
3.1.6 Software Improvement Group (SIG) Software Quality Model for Security..... 34
3.1.7 UL Cybersecurity Assurance Program (UL 2900-1 / 2)..... 35
3.1.8 ULD Datenschutz-Gütesiegel..... 37
3.2 Standards and schemes for products used in Industry 4.0 and ICS (SWG 3.1) 39
3.2.1 ISA/IEC 62443 (Security for Industrial Automation and Control Systems) 39
3.2.2 IACS Cybersecurity Certification Framework..... 40
3.3 Standards and schemes for products used in energy networks and smart grids (SWG 3.2)..... 42
3.3.1 IEEE 1686 (Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities)..... 42
3.3.2 IEEE C37.240 (Cybersecurity Requirements for Substation Automation, Protection, and Control Systems) 43
3.4 Standards and schemes for products used in the telecom industry (SWG3.8) 44
3.4.1 GSMA Network Equipment Security Assurance Scheme 44
3.5 Standards and schemes for products used in the payment industry..... 46
3.5.1 EMVCo Security Evaluation 46
3.5.2 PCI PTS HSM Security Requirements 48
3.5.3 PCI Payment Application Data Security Standard (PCI PA-DSS)..... 49
3.5.4 PCI PIN Transaction Security Point of Interaction Security (PCI PTS POI)..... 50
3.6 Standards and schemes for cryptographic modules 52
3.6.1 ASD Cryptographic Evaluation..... 52
3.6.2 CESG Assisted Products Scheme (CAPS)..... 53
3.6.3 FIPS 140-2..... 54
3.6.4 ISO/IEC 19790 (Security requirements for cryptographic modules)..... 56
3.7 Standards and schemes for web applications..... 58
3.7.1 OWASP Application Security Verification Standard (incl. OWASP Top 10) 58
3.7.2 OWASP Testing Guide..... 59
3.8 Standards and schemes for IoT products 60
3.8.1 ICSA Labs IoT Security Testing Framework..... 60
3.9 Standards and schemes for other IT products 61
3.9.1 MIFARE Security Certification..... 61
3.9.2 ISO/IEC 19792 (Security evaluation of biometrics)..... 63
4 Cybersecurity standards and schemes for ICT services 64
4.1 ANSSI SecNumCloud 64

4.2 Cloud Computing Compliance Controls Catalogue (C5) 65
4.3 Cloud Security Alliance Cloud Controls Matrix 67
4.4 Code of Practice for Cloud Service Providers 68
4.5 EuroCloud StarAudit Certification 70
4.6 ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services) 71
4.7 ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) 72
4.8 TüV Rheinland Cloud Security Certification 73
5 Cybersecurity standards and schemes for service providers and organisations 75
5.1 Standards and schemes for generic organisations 75
5.1.1 AEI Seal of Cybersecurity for Organisations 75
5.1.2 CIS Critical Security Controls / SANS Critical Security Controls 76
5.1.3 Cyber Essentials / 10 Steps to Cyber Security 79
5.1.4 Cyber Resilience Review 80
5.1.5 FINCSC – Finnish Cyber Security Certificate 81
5.1.6 ISF Standard of Good Practice for Information Security 82
5.1.7 IT Grundschutz 83
5.1.8 ISO/IEC 27001 (Information Security Management Systems — Requirements) 86
5.1.9 ISO/IEC 27002 (Code of practice for information security controls) 89
5.1.10 ISO/IEC 27032 (Guidelines for cybersecurity) 90
5.1.11 ISO/IEC 27033 (Network Security) 91
5.1.12 ISO/IEC 27034 (Application Security) 92
5.1.13 ISO/IEC 27035 (Information security incident management) 93
5.1.14 ISO/IEC 27036 (Information security for supplier relationships) 94
5.1.15 ISO/IEC 29100 (Privacy architecture framework) and related ISO standards .. 96
5.1.16 LEET Security Stamp 97
5.1.17 Open Trusted Technology Provider Standard (O-TTPS) 99
5.1.18 Service Organisation Controls (SOC) 100
5.1.19 Shared Assessments Program 103
5.1.20 ULD Datenschutzaudit 105
5.2 Standards and schemes for Industry 4.0 and ICS (SWG 3.1) 106
5.2.1 ANSSI Cybersecurity for Industrial Control Systems 106
5.2.2 API STD 1164 (Pipeline SCADA Security) 108
5.2.3 BSI ICS Security Compendium 110
5.2.4 Catalog of Control Systems Security 111
5.2.5 ICS-CERT assessments 112
5.2.6 ISA/IEC 62443 (Security for Industrial Automation and Control Systems) 114
5.2.7 NIST SP 800-82 (Guide to Industrial Control Systems (ICS) Security) 118

5.3 Standards and schemes for energy networks and smart grids (SWG 3.2). 119
5.3.1 Cybersecurity Capability Maturity Model 119
5.3.2 ISO/IEC 27019 (Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry)..... 121
5.3.3 NERC CIP 002-009..... 122
5.3.4 NIST IR 7628 (Guidelines for Smart Grid Cybersecurity)..... 124
5.4 Standards and schemes for transportation (road, rail, air, sea) (SWG 3.3) 125
5.4.1 RTCA DO-326A (Airworthiness Security Process Specification) 125
5.4.2 SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems) & ISO-SAE 21434 AWI (Road Vehicles – Cybersecurity Engineering) 127
5.4.3 The Guidelines on Cyber Security onboard Ships 128
5.5 Standards and schemes for financial services and insurance (SWG 3.4).. 129
5.5.1 BITS Software Assurance Framework..... 129
5.5.2 CBEST 130
5.5.3 ISO/IEC 27015 (Information security management guidelines for financial services) 131
5.6 Standards and schemes for public services / eGovernment / digital citizenship (SWG 3.5)..... 132
5.6.1 Application Security and Development Security Technical Implementation Guide (STIG) 132
5.6.2 National Security Framework (Esquema Nacional de Seguridad - ENS) 134
5.6.3 NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organisations)..... 136
5.7 Standards and schemes for healthcare (SWG3.6)..... 138
5.7.1 ISO/IEC 27799 (Health informatics - Information security management in health using ISO/IEC 27002)..... 138
5.7.2 ISO/IEC 62304 (Medical device software – Software life cycle processes).... 138
5.7.3 IT Health CHECK Service (CHECK)..... 139
5.8 Standards and schemes for smart cities and smart buildings (SWG3.7) ... 141
5.8.1 ISA/IEC 62433 (Security for Industrial Automation and Control Systems) 141
5.9 Standards and schemes for telecom, media and content (SWG 3.8) 142
5.9.1 GSMA Security Accreditation Scheme 142
5.9.2 ISO/IEC 27011 (Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations) 144
5.9.3 TL 9000 Quality Management System 145
5.10 Standards and schemes for critical infrastructures 146
5.10.1 AEI Seal of Cybersecurity for Organisations..... 146
5.10.2 KRITIS 146
5.10.3 NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)..... 147
5.10.4 Référentiel Général de Sécurité (RGS) 149
5.11 Standards and schemes for general secure software development..... 151

5.11.1 BSI PAS 754 151
5.11.2 BSIMM 152
5.11.3 ISO/IEC 21827 (Systems Security Engineering - Capability Maturity Model) 153
5.11.4 Microsoft Security Development Lifecycle 154
5.11.5 OWASP Software Assurance Maturity Model 156
5.12 Standards and schemes for Cybersecurity service providers 157
5.12.1 ANSSI requirements for security service providers (PDIS, PRIS, PASSI, PSCE, PSHE) 157
5.12.2 CREST Simulated Targeted Attack and Response (STAR) 160
5.13 Standards and schemes for the payment industry 161
5.13.1 PCI Data Security Standard (PCI DSS) 161
5.14 Standards and schemes for IoT device vendors 163
5.14.1 BITAG Internet of Things (IoT) Security and Privacy Recommendations 163
5.14.2 Future-proofing the Connected World 164
5.14.3 GSMA IoT Security Guidelines 165
5.14.4 Industrial Internet of Things Security Framework 167
5.14.5 IoT Security Compliance Framework 169
5.14.6 Online Trust Alliance IoT Trust Framework 170
5.14.7 OWASP Internet of Things Project 172
5.14.8 Strategic Principles for Securing the Internet of Things (IoT) 173
6 Cybersecurity standards and schemes for security professionals 175
6.1 CompTIA certifications 175
6.2 CREST certifications 176
6.3 EC-Council certifications 177
6.4 GIAC certifications 180
6.5 ISACA certifications 181
6.6 ISA/IEC 62443 Cybersecurity Certificate Programs 182
6.7 (ISC)² certifications 183
6.8 ISO/IEC 27021 (Competence requirements for ISMS professionals) 185
6.9 NCSC Certified Professional (CCP) certifications 186
7 Further Reading 189
Appendix 1 The JHAS attack rating methodology 192

1 INTRODUCTION

1.1 Goal of ECSO SWG1.4

The European Cyber Security Organisation (ECSO) is a not-for-profit organisation representing Europe's Cybersecurity Industry. ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations.

With the ECSO, several Working Groups have been created, being the goal of WG 1, to propose one or more harmonised, common certification framework(s), as much as possible based on existing standards, to assess the Cybersecurity of the European Digital Single Market.

This work is undertaken in a number of subgroups of WG1:

- **SWG 1.1.** "Manufacturing of Subcomponents, Components, Devices and Products"

  Taking care of manufacturing of simple subcomponents, such secure IC components, up to complex products, such as cars, aircraft and others that require the integration of several components or even devices. Software as a product will be covered by this SWG too.
  This SWG will focus mainly on manufacturing of cyber secure products including the respective supply-chain during integration of components.

- **SWG 1.2.** "ICT infrastructure providers and other cloud based services"

  Taking care of Telco or other ICT infrastructure providers, but also cloud -based ones.
  This SWG will mainly focus of delivery of cyber secure services but with a big effort on the privacy of data handling.

- **SWG 1.3.** "IT Integrators, Critical Infrastructure Operators, End Users and Supply Chain Management."

  Taking care of the IT Integrators and End Users (including also critical infrastructure) and the organizational and IT infrastructure changes needed to have a market of companies and suppliers able to deliver their services (ICT or non) to citizen in a secure way.
  This SWG will mainly focus on organizations and their IT infrastructure.

- **SWG 1.4.** "Base Layer"

  This SWG will deliver required specific capabilities to other SWGs as advanced research, definition of common terms, structures and procedures.
  This SWG will mainly focus on having one single outcome for WG1, instead of several non-coordinated ones.

Alongside with the creation of a document containing the Challenges_Of_The_Industry (COTI), made by SWG 1.1, 1.2 and 1.3, the task to create a document that will record all available

standards and initiatives that might be considered in order to have a good view of the state of the art in this field have been given to the SWG 1.4.

The purpose of this document, will be to deliver a good understanding of existing standards and methodologies, so the WG, can have a comprehensive way to evaluate what can be used (if existing) in order to address the challenges expressed in the document of Challenges_Of_The_Industry (COTI).

1.2 Scope of this document

This document lists all standards and specifications related to Cybersecurity[1] known to and deemed relevant by the authors at the moment of writing. 'Relevant' here means that a standard can (potentially) be used for assessing the overall Cybersecurity stance of a product, service or organisation. See the next section for a more explicit discussion of the criteria for inclusion.

For each of these standards, the following questions are briefly discussed:

- **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?
- **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?

1.2.1 Out of scope

There are many more standards and schemes that can be said to be 'related to Cybersecurity' than are discussed in this document. As said, this syllabus focuses on standards that can be (potentially) used as the basis for assessing the overall Cybersecurity stance of a product or component, an ICT service, a service provider or organisation or a critical infrastructure. By

[1] There are many overlapping definitions of the word 'Cybersecurity'. In keeping with the ENISA recommendation, this document does not adopt a specific definition. Refer to ref. [6] for an overview and discussion of definitions.

definition, such standards are quite broad in scope. Excluded from this document are therefore standards describing only a single aspect of (cyber)security, such as:

- Cryptographic primitives, algorithms, modes, protocols, etc.
- Generic techniques for securing the confidentiality, integrity and availability of data, such as digital signatures, MACs or encryption, plus associated techniques (such as Public Key Infrastructures) and practices (such as key management).
- Techniques for securing generic IT technologies such as XML, TCP-IP, HTTP etc.
- Individual aspects of secure software development, such as requirements engineering and management, language-specific secure development guidelines, security testing and test management, etc.
- Functional specifications of components that might be used in cyber secure products or infrastructures, such as smart cards, trusted execution environments, hardware security modules, etc.
- Cybersecurity-related business practices such as IT service management, information management, risk management, quality management, device management etc.

Obviously, such standards will in fact be used by subjects complying with the standards discussed in this syllabus. E.g. a cyber secure product would be expected to use cryptography according to well-defined standards. Similarly, an organisation boasting a high level of Cybersecurity will also be expected to follow best practices regarding quality management and thus be certified against ISO 9001.

1.3 Intended audience

Although this document was initially described as basically an ECSO-internal document, the need of this kind of methodical approaches for compiling existing standards and initiatives in areas as European Commission, Member States Agencies and Public Bodies and Normalization ones, made that the document was now intended for public dissemination, in order to help to improve general awareness on Standardization, Certification and Labelling in Cybersecurity, either on Subcomponents, Components, Devices, Products, Systems, Services and Organizations.

1.4 Glossary

This document does not contain a glossary giving exact definitions of terms. Rather, every section uses terminology as provided by (or in accordance with) the standard or scheme in question. Readers should be aware that the exact meaning of words may consequently differ slightly from section to section. In case of doubt, original documentation should be consulted.

1.5 Document structure

This document is structured as follows:

- Chapter 2 gives an overview of Cybersecurity standards discussed in this document, listing the body responsible for the standard and/or the certification scheme, the country of origin, the industry for which the standard is intended, and giving a link to the main document(s).

- Chapter 3 describes Cybersecurity standards and schemes for products and components. These standards cover primarily the scope of ECSO Sub WG 1.1.
- Chapter 4 describes Cybersecurity standards and schemes for ICT and cloud service providers. These standards cover primarily the scope of ECSO Sub WG 1.2.
- Chapter 5 describes Cybersecurity standards and schemes for service providers and end-user organisations. These standards cover primarily the scope of ECSO Sub WG 1.3.
- Chapter 6 describes Cybersecurity standards and schemes for security professionals.
- Chapter 7 contains a bibliography of documents for further reading. These are not standards in themselves, but contain background information of various natures.

Chapter 3 is subdivided into section for different industry verticals. This includes some of the verticals distinguished in WG3. However, verticals for which no product standard was found have been omitted. In addition, some other verticals are added for which specific product standards are present.

Chapter 5 is also subdivided into sections for different industry verticals. This includes all of the verticals distinguished in WG3, and also a number of other verticals:

- Generic organisations not associated with any particular vertical
- Industry 4.0 and ICS (SWG 3.1)
- Energy Networks and Smart Grids (SWG 3.2)
- Transportation (road, rail, air, sea) (SWG 3.3)
- Financial Services and Insurance (SWG 3.4)
- Public Services / eGovernment / Digital Citizenship (SWG 3.5)
- Healthcare (SWG 3.6)
- Smart Cities and Smart Buildings (SWG 3.7)
- Telecom, Media and Content (SWG 3.8)
- Critical Infrastructures
- Secure Software Development
- Cybersecurity service providers
- Payment industry[2]
- IoT device vendors

[2] The payment industry is about making payments, from card payments in brick-and-mortar shops to online payments in web shops. This could be considered a subset of financial services, but in practice it is a quite separate industry, notably with different parties (the payment schemes) setting the rules.

2 Overview

2.1 Cybersecurity standards and schemes for products and components (SWG 1.1)

2.1.1 Standards and schemes for generic IT products

Standard / Scheme	Body	Country / Industry	Link	Ref.
Certification de Sécurité de Premier Niveau (CSPN)	ANSSI	France Generic	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-procedures-formulaires-et-methodologies	3.1.1
Commercial Product Assurance (CPA)	NCSC	UK Generic	https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa	3.1.2
Common Criteria	Signatories of the CCRA Signatories of the SOG-IS	International Generic	https://www.commoncriteriaportal.org/ www.sogis.org	3.1.3
European Privacy Seal	EuroPriSe	Europe Generic products, websites	https://www.european-privacy-seal.eu/EPS-en/Home	3.1.4
National IT Evaluation Scheme (NITES)	CSA Singapore	Singapore General	https://www.csa.gov.sg/	3.1.5
Software Improvement Group (SIG) Software Quality Model for Security	Software Improvement Group	The Netherlands General	https://www.sig.eu/insight/practical-model-rating-software-security	3.1.6
UL Cybersecurity Assurance	UL	USA	http://www.ul.com/cybersecurity/	3.1.7

Program (UL 2900-1 / 2)		Generic		
ULD Datenschutz-Gütesiegel	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Germany (Schleswig-Holstein)	https://www.datenschutzzentrum.de/guetesiegel/ (German only)	3.1.8

2.1.2 Standards and schemes for products used in Industry 4.0 and ICS (SWG3.1)

Standard / Scheme	Body	Country	Link	Ref.
ISA/IEC 62433 (Security for Industrial Automation and Control Systems)	ISA/IEC	International	https://webstore.iec.ch/searchform&q=62443 http://www.isasecure.org/en-US/	3.2.1
IACS Cybersecurity Certification Framework (proposed)	JRC	Europe	https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs	3.2.2

2.1.3 Standards and schemes for products used in energy networks and smart grids (SWG3.2)

Standard / Scheme	Body	Country	Link	Ref.
IEEE 1686 (Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities)	IEEE	International Power transmission	https://standards.ieee.org/findstds/standard/1686-2013.html	3.3.1
IEEE C37.240 (Cybersecurity Requirements for Substation Automation, Protection, and Control Systems)	IEEE	International Power transmission	https://standards.ieee.org/findstds/standard/C37.240-2014.html	3.3.2

2.1.4 Standards and schemes for products used in telecom, media and content (SWG3.8)

Standard / Scheme	Body	Country	Link	Ref.
GSMA Network Equipment Security Assurance Scheme	GSMA and 3GPP	International	http://www.3gpp.org/news-events/3gpp-news/1569-secam_for_3gpp_nodes	3.4.1

2.1.5 Standards and schemes for products used in the payment industry

Standard / Scheme	Body	Country / Type	Link	Ref.
EMVCo Security Evaluation	EMVCo	International Payment cards	https://www.emvco.com/approvals.aspx?id=31	3.5.1
PCI PTS HSM Security Requirements	PCI SSC	International HSMs used in the payment industry	https://www.pcisecuritystandards.org/	3.5.2
PCI Payment Application Data Security Standard (PCI PA-DSS)	PCI SSC	International Payment applications	https://www.pcisecuritystandards.org/	3.5.3
PCI PIN Transaction Security Point of Interaction Security (PCI PTS POI) Requirements	PCI SSC	International Payment point of interaction devices	https://www.pcisecuritystandards.org/	3.5.4

2.1.6 Standards and schemes for cryptographic modules

Standard / Scheme	Body	Country	Link	Ref.
ASD Cryptographic Evaluation	Australian Signals Directorate (ASD)	Australia	http://www.asd.gov.au/infosec/evaluations.htm	3.6.1
CESG Assisted Products Scheme (CAPS)	NCSC	UK	https://www.ncsc.gov.uk/scheme/products-cesg-assisted-products-service	3.6.2
FIPS 140-2	NIST	USA	http://csrc.nist.gov/groups/STM/cmvp/standards.html#02	3.6.3
ISO/IEC 19790 (Security requirements for cryptographic modules)	ISO/IEC	International	https://www.iso.org/standard/52906.html	3.6.4

2.1.7 Standards and schemes for web applications

Standard / Scheme	Body	Country	Link	Ref.
OWASP Application Security Verification Standard (including OWASP Top Ten)	OWASP	International	https://www.owasp.org/index.php/Top_10_2013	3.7.1
OWASP Testing Guide	OWASP	International	https://www.owasp.org/index.php/Category:OWASP_Testing_Project.	3.7.2

2.1.8 Standards and schemes for IoT products

Standard / Scheme	Body	Country	Link	Ref.
IoT Security Testing Framework	ICSA Labs	USA / International	https://www.icsalabs.com/technology-program/iot-testing	3.8.1

2.1.9 Standards and schemes for other IT products

Standard / Scheme	Body	Country / Type	Link	Ref.
MIFARE Security Certification	NXP	International MIFARE products	https://www.mifare.net/en/about-mifare/certification/	3.9.1
ISO/IEC 19792 (Security evaluation of biometrics)	ISO/IEC	International Biometric systems	https://www.iso.org/standard/51521.html	3.9.2

2.2 Standards and schemes for cloud service providers (SWG 1.2)

Standard / Scheme	Body	Country	Link	Ref.
ANSSI SecNumCloud	ANSSI	France	https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/	4.1
Cloud Computing Compliance Controls Catalogue (C5)	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany	https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html	4.2
Cloud Security Alliance Cloud Controls Matrix	Cloud Security Alliance (CSA)	International	https://cloudsecurityalliance.org/group/cloud-controls-matrix/ https://cloudsecurityalliance.org/group/open-certification/#_downloads	4.3
Code of Practice for Cloud Service Providers	Cloud Industry Forum	International	https://www.cloudindustryforum.org/content/code-practice-cloud-service-providers	4.4
EuroCloud StarAudit Certification	EuroCloud	Europe (International)	https://staraudit.org/	4.5
ISO/IEC 27017 (Code of practice for information security controls	ISO/IEC	International	http://www.iso.org/iso/catalogue_detail?csnumber=43757	4.6

based on ISO/IEC 27002 for cloud services)				
ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)	ISO/IEC	International	http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498	4.7
TüV Rheinland Cloud Security Certification	TüV Rheinland	International	http://www.tuv.com/en/corporate/business_customers/information_security_cw/strategic_information_security/cloud_security_certification/cloud_security_certification.html	4.8

2.3 Standards and schemes for service providers and organisations (SWG 1.3)

2.3.1 Standards and schemes for generic organisations

Standard / Scheme	Body	Country	Link	Ref.
AEI Seal of Cybersecurity for Organisations	AEI	Spain	https://www.aeiciberseguridad.es/index.php/Sello_AEI	5.1.1
CIS Critical Security Controls	Center for Internet Security SANS Institute	International	https://www.cisecurity.org/critical-controls/Library.cfm https://www.sans.org/critical-security-controls/	5.1.2
Cyber Essentials / 10 steps to Cyber Security	CREST	UK	https://www.cyberessentials.org/	5.1.3

Cyber Resilience Review	US-CERT	US	https://www.us-cert.gov/ccubedvp/assessments	5.1.4
FINCSC – Finnish Cyber Security Certificate	JAMK University of Applied Sciences and partners	Finland	https://www.fincsc.fi/ (Finnish only)	5.1.5
ISF Standard of Good Practice for Information Security	Information Security Forum	International	https://www.securityforum.org/tool/the-isf-standardrmation-security/	5.1.6
IT Grundschutz	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany	https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html	5.1.7
ISO/IEC 27001 (Information Security Management Systems – Requirements)	ISO/IEC	International	http://www.iso.org/iso/iso27001 http://www.iso.org/iso/catalogue_detail?csnumber=54534	5.1.8
ISO/IEC 27032 (Guidelines for cybersecurity)	ISO/IEC	International	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375	5.1.10
ISO/IEC 27033 (Network security)	ISO/IEC	International	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63461	5.1.11
ISO/IEC 27034 (Application security)	ISO/IEC	International	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378	5.1.12
ISO/IEC 27035 (Information security incident management)	ISO/IEC	International	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62071	5.1.13

ISO/IEC 27036 (Information security for supplier relationships)	ISO/IEC	International	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59648	5.1.14
ISO/IEC 29100 (Privacy architecture framework) and related ISO standards	ISO/IEC	International	https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en	5.1.15
LEET Security Stamp	LEET Security	Spain	http://www.leetsecurity.com/	5.1.16
Open Trusted Technology Provider Standard (O-TTPS) **&** **ISO/IEC 20243 (O-TTPS -- Mitigating maliciously tainted and counterfeit products)**	Open Group ISO/IEC	International	https://www2.opengroup.org/ogsys/catalog/c139 http://www.opengroup.org/certifications/o-ttps http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394	5.1.17
Service Organisation Control (SOC)	AICPA	USA General	http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/ServiceOrganisation%27sManagement.aspx	5.1.18
Shared Assessments Program	Shared Assessment	International Vendor management	https://sharedassessments.org/about/	5.1.19
ULD Datenschutzaudit	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein	Germany (Schleswig-Holstein)	https://www.datenschutzzentrum.de/audit/ (German only)	5.1.20

2.3.2 Standards and schemes for Industry 4.0 and ICS (SWG 3.1)

Standard / Scheme	Body	Country / Industry	Link	Ref.
ANSSI Cybersecurity for Industrial Control Systems	ANSSI	France General ICS	https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_detailed_measures.pdf	5.2.1
API STD 1164 (Pipeline SCADA Security)	American Petroleum Institute (API)	USA Oil and Gas	https://global.ihs.com/doc_detail.cfm?document_name=API%20STD%201164	5.2.2
BSI ICS Security Compendium	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany General ICS	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.html	5.2.3
Catalog of Control Systems Security	Department of Homeland Security (DHS)	USA General ICS	https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf	5.2.4
ICS-CERT assessments: • **CSET** • **DAR** • **NAVV**	ICS-CERT	USA General ICS	https://ics-cert.us-cert.gov/Assessments	5.2.5
ISA/IEC 62433 (Security for Industrial Automation and Control Systems)	ISA/IEC	International General ICS	https://webstore.iec.ch/searchform&q=62443 http://www.isasecure.org/en-US/	5.2.6
NIST SP 800-82 (Guide to Industrial Control Systems (ICS) Security)	NIST	USA General ICS	http://dx.doi.org/10.6028/NIST.SP.800-82r2	5.2.7

Note: Apart from the standards listed above, a large number of other recommendations, guidelines and best practices for ICS security were published over the last decade by various public and private entities, both national and international. In 2011, ENISA published an overview called 'Protecting Industrial Control Systems - Annex III: ICS Security Related Standards, Guidelines and Policy Documents', ref. [17].

2.3.3 Standards for energy networks and smart grids (SWG 3.2)

Standard / Scheme	Body	Country / Industry	Link	Ref.
Cybersecurity Capability Maturity Model	US Department of Energy	US Energy, Electricity, Oil and Gas	https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program	5.3.1
ISO/IEC 27019 (Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry)	ISO/IEC	International General energy systems	https://www.iso.org/standard/43759.html	5.3.2
NERC Critical Infrastructures Protection (CIP) standards 002 - 009	NERC	USA Electrical Grid	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx	5.3.3
NIST IR 7628 (Guidelines for Smart Grid Cybersecurity)	NIST	USA Smart grids	https://www.nist.gov/node/562431	5.3.4

2.3.4 Standards and schemes for transportation (road, rail, air, sea) (SWG 3.3)

Standard / Scheme	Body	Country / Industry	Link	Ref.
RTCA DO-326A (Airworthiness Security Process Specification)	RTCA	International Aviation	http://www.rtca.org/store_product.asp?prodid=1173	5.4.1
ISO-SAE 21434 (Road Vehicles – Cybersecurity Engineering)	ISO / SAE	International Vehicles	https://www.iso.org/standard/70918.html	5.4.2
SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)	SAE	International Vehicles	http://webstore.ansi.org/RecordDetail.aspx?sku=SAE+J+3061-2016+(SAE+J3061-2016)	5.4.2
The Guidelines on Cyber Security onboard Ships	BIMCO et al.	International Shipping	http://www.srhmar.com/images/stories/pdf/Guidelines_on_cyber_security_onboard_ships.pdf	5.4.3

2.3.5 Standards and schemes for financial services and insurance (SWG3.4)

Standard / Scheme	Body	Country / Industry	Link	Ref.
BITS Software Assurance Framework	BITS	International Software development	http://fsroundtable.org/bits/about-bits/	5.5.1
CBEST	Bank of England	UK Financial service providers	http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx#	5.5.2
ISO/IEC 27015 (Information security management guidelines for financial services)	ISO/IEC	International Financial service providers	https://www.iso.org/standard/43755.html	5.5.3

2.3.6 Standards and schemes for public services / eGovernment / Digital Citizenship (SWG 3.5)

Standard / Scheme	Body	Country / Industry	Link	Ref.
Application Security and Development Security Technical Implementation Guide (STIG)	DISA	USA Federal IT systems	http://iase.disa.mil/stigs/app-security/app-security/Pages/index.aspx	5.6.1
National Security Framework (Esquema Nacional de Seguridad - ENS)	Entidad Nacional de Acreditación	Spain Public sector organisations and their service providers	https://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=ens&idioma=en#.WNpAE7u7r4Z	5.6.2
NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organisations)	NIST	USA Federal IT systems	https://web.nvd.nist.gov/view/800-53/Rev4/home	5.6.3

2.3.7 Standards and schemes for healthcare (SWG 3.6)

Standard / Scheme	Body	Country / Industry	Link	Ref.
ISO/IEC 27799 (Health informatics - Information security management in health using ISO/IEC 27002)	ISO/IEC	International	https://www.iso.org/standard/62777.html	5.7.1
ISO/IEC 62304 (Medical device software – Software life cycle processes)	ISO/IEC	International Medical software development	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=71604	5.7.2
IT Health CHECK Service (CHECK)	National Centre for Cyber Security (NCSC)	UK Healthcare providers	https://www.ncsc.gov.uk/articles/check-fundamental-principles	5.7.3

2.3.8 Standards and schemes for smart cities and smart buildings (SWG3.7)

Standard / Scheme	Body	Country / Industry	Link	Ref.
ISA/IEC 62433 (Security for Industrial Automation and Control Systems)	ISA/IEC	International General ICS	https://webstore.iec.ch/searchform&q=62443 http://www.isasecure.org/en-US/	5.8.1

2.3.9 Standards and schemes for telecom, media and content (SWG 3.8)

Standard / Scheme	Body	Country / Industry	Link	Ref.
GSMA Security Accreditation Scheme	GSMA	International UICC providers	http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme	5.9.1
ISO/IEC 27011 (Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations)	ISO/IEC	International	https://www.iso.org/standard/64143.html	5.9.2
TL 9000 Quality Management System	QuEST Forum	International ICT vendors	http://www.tl9000.org/	5.9.3

2.3.10 Standards and schemes for critical infrastructures

Standard / Scheme	Body	Country / Industry	Link	Ref.
AEI Seal of Cybersecurity for Organisations	AEI	Spain General	https://www.aeiciberseguridad.es/index.php/Sello_AEI	5.10.1
KRITIS	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Germany General	http://www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/publikationen_node.html	5.10.2
NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)	NIST	USA General	https://www.nist.gov/cyberframework	5.10.3
Référentiel Général de Sécurité (RGS)	ANSSI	France General	https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/ (French only)	5.10.4

2.3.11 Standards and schemes for general secure software development

Standard / Scheme	Body	Country	Link	Ref.
BSI PAS 754 (Software trustworthiness –Governance and management – Specification)	British Standards Institution (BSI)	UK	http://shop.bsigroup.com/ProductDetail/?pid=000000000030284608	5.11.1
Building Security in Maturity Model (BSIMM)	Gary McGraw, Sammy Migues, and Jacob West	International	https://www.bsimm.com/	5.11.2
ISO/IEC 21827 (Systems Security Engineering - Capability Maturity Model)	ISO/IEC	International	https://www.iso.org/standard/44716.html	5.11.3
Microsoft Security Development Lifecycle	Microsoft	International	https://www.microsoft.com/en-us/sdl/	5.11.4
OWASP Software Assurance Maturity Model	OWASP	International	https://www.owasp.org/index.php/OWASP_SAMM_Project http://www.opensamm.org/	5.11.5

2.3.12 Standards and schemes for cybersecurity service providers

Standard / Scheme	Body	Country / Industry	Link	Ref.
ANSSI requirements for security service providers (PDIS, PRIS, PASSI, PSCE, PSHE)	ANSSI	France Service providers for • Incident detection • Incident response • Information system security auditing • Electronic certificates • Electronic timestamping	https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/	5.12.1
CREST Simulated Targeted Attack and Response (STAR)	Council for Registered Ethical Security Testers (CREST)	UK Accreditation for CBEST, see section 5.5.2	http://www.crest-approved.org/uk/what-we-do/index.html	5.12.1

2.3.13 Standards and schemes for the payment industry

Standard / Scheme	Body	Country / Industry	Link	Ref.
PCI Data Security Standard	PCI SSC	International Card Payments	https://www.pcisecuritystandards.org/	5.13.1

2.3.14 Standards and schemes for IoT device vendors

Standard / Scheme	Body	Country / Industry	Link	Ref.
BITAG Internet of Things (IoT) Security and Privacy Recommendations	BITAG	International General	https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php	5.14.1
Future-proofing the Connected World	Cloud Security Alliance IoT Working Group	International General	https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/	5.14.1
GSMA IoT Security Guidelines	GSMA	Internal Telecom	http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/	5.14.2
Industrial Internet of Things Security Framework	Industrial Internet Consortium	International Industrial IoT systems	http://www.iiconsortium.org/IISF.htm	5.14.3
IoT Security Compliance Framework	IoT Security Foundation	International General	https://iotsecurityfoundation.org/best-practice-guidelines/	5.14.5
Online Trust Alliance IoT Trust Framework	Online Trust Alliance	USA General	https://otalliance.org/resources/iot-industry-resources	5.14.5
OWASP Internet of Things Project	OWASP	International General	https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project	5.14.7
Strategic Principles for Securing the Internet of Things (IoT)	Department of Homeland Security	USA General	https://www.dhs.gov/securingtheIoT	5.14.7

2.4 Standards and schemes for security professionals

Standard / Scheme	Body	Link	Ref.
CompTIA certifications (related to security)	CompTIA	https://certification.comptia.org/certifications	6.1
CREST certifications	CREST	http://www.crest-approved.org/uk/examinations/index.html	6.2
EC-Council certifications	EC-Council	https://www.eccouncil.org/programs/	6.3
GIAC certifications	GIAC	https://www.giac.org/certifications/	6.4
ISACA certifications	ISACA	http://www.isaca.org/Certification/Pages/default.aspx	6.5
ISA/IEC 62443 Cybersecurity Certificate Programs	ISA	https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/	6.6
(ISC)² certifications	(ISC)²	https://www.isc2.org/credentials/default.aspx	6.7
ISO/IEC 27021 (Competence requirements for information security management systems professionals)	ISO	http://www.iso.org/iso/catalogue_detail.htm?csnumber=61003	6.8
NCSC Certified Professional (CCP) certifications	NCSC	https://www.ncsc.gov.uk/scheme/certified-professional	6.9

3 Cybersecurity standards and schemes for products and components

3.1 Standards and schemes for generic IT products

3.1.1 Certification de Sécurité de Premier Niveau (CSPN)

3.1.1.1 Focus

The Certification de Sécurité de Premier Niveau (CSPN) scheme was set up by the French information security agency ANSSI in 2008. Under this scheme, the security of products is evaluated mainly by means of limited-time black box testing. CSPN aims to offer a high level of confidence on product security, while being less expensive or time-consuming than a Common Criteria evaluation.

3.1.1.2 Associated Evaluation Scheme and Governance

The governance of the certification scheme is handled by ANSSI. The evaluations are carried out by accredited 'Centres d'évaluation de la sécurité des technologies de l'information' (CESTI), which act as independent third parties. A list of CESTIs accredited by ANSSI can be found here: https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-centres-devaluation/

3.1.1.3 Process

The certification is based on criteria, a methodology and a process developed by ANSSI. The certification can be done digitally. The basic process is as follows:

1. The sponsor (the party that requests certification of a product from ANSSI and that finances the evaluation service) signs a contract with a CESTI.
2. The sponsor provides the product, its documentation and a Security Target (ST) to the CESTI. The Security Target describes the product's security functions that should be evaluated and the product's security requirements on the environment. In addition, the ST describes the product's rationale, its assets and the threats from which these assets should be protected. If the product makes use of cryptographic measures, these should be described as well, since the CSPN has specific requirements for the used algorithms, key lengths, key management procedures, random number generators etc.
3. The evaluator
    a. Checks the product's Security Target and other documentation
    b. Installs the product (if needed)
    c. Performs a high-level source code review, if source code is made available.
    d. Performs functional testing of the product's security functions and cryptographic mechanisms.

e. Performs testing of the resistance of these functions and mechanisms against targeted attacks aimed at finding and exploiting vulnerabilities. This analysis takes into account the time and resources spent and the attacker's assumed knowledge and expertise.
f. Analyses whether the product contains known vulnerabilities, e.g. those published in public databases.
g. Analyses how easily mistakes in the configuration or use of the product may lead to vulnerabilities.
h. Optionally, meets with the product's developers and assesses their capabilities.
i. Evaluates the product's use of cryptography and random number generators, if applicable, by means of various methods such as source code analysis, comparison to reference implementations and use of stubs and drivers.

4. The result of the evaluation is documented in an evaluation technical report (ETR) which is sent to the ANSSI for validation.
5. ANSSI validates the ETR drafted by the CESTI, and decides whether or not to certify the product. It drafts the certification report (an outtake of the ETR) and the certificate. With the sponsors' agreement, it publishes the security target and the certification report on the ANSSI website.

The CSPN processes distinguishes a so-called Observer role. The observer is an actor who is concerned by the results of the evaluation. In general, this is a client of a user of the evaluated product. The observer is kept informed of the start of the evaluation and the results obtained.They may ask to receive the evaluation technical report.

In case a certified product is changed, a re-certification may be necessary.

A more detailed description of the process and methodology can be found here: https://www.ssi.gouv.fr/administration/produits-certifies/cspn/les-procedures-formulaires-et-methodologies/

3.1.1.4 Practice

As of 1 December 2016, 189 products had been evaluated. Of these, 75 have been certified[3]. These products are divided into different categories, among which:

- Secure storage devices / software
- Operating systems
- Firewalls
- Intrusion detection systems
- Antivirus software
- Systems / software for identification, authentication and access control
- Systems / software for secure communication or secure messaging

[3] It is not entirely clear to the authors what the status of the evaluated but non-certified products is.

Eleven CESTIs have been accredited, all of them in France.

One of the CESTI estimates that the typical CSPN evaluation consists of 25 days dedicated to software security (protocol fuzzing, port scanning, etc.) and 10 days dedicated to the cryptographic analysis (algorithm choices and key sizes, protocol analysis, etc.). It furthers claims that a CSPN evaluation takes about half the time, and costs about one third, of a Common Criteria certification.

3.1.1.5 Formal Status

Authors are not fully clear about whether or not the French government requires a CSPN certification for products it buys or uses.

3.1.1.6 Relation to other standards / schemes

Although there is no formal relationship, the ANSSI website explicitly positions the CSPN as an alternative for Common Criteria in product security. Parts of the process and terminology is clearly based on CC.

3.1.2 Commercial Product Assurance (CPA)

3.1.2.1 Focus

The Commercial Product Assurance (CPA) scheme is a UK scheme aiming to evaluate commercial off-the-shelf products, and their developers, against published security and development standards. A security product that passes assessment is awarded a so-called 'Foundation Grade' certification. This means the product is proven to demonstrate good commercial security practice and is suitable for lower-threat environments.

3.1.2.2 Associated Evaluation Scheme and Governance

The CPA certification scheme is governed by the NCSC (National Cyber Security Centre) in the United Kingdom (formerly called the CESG). The 'Foundation Grade' assessment is carried out by independent NCSC-approved CPA test labs. A list of such test labs can be found at https://www.ncsc.gov.uk/search?keyword=CPA&f[0]=type%3Atest_lab.

3.1.2.3 Process

A vendor should first contact one of the approved CPA test labs to agree on the terms and initiate testing of their product. The lab will then liaise with the NCSC to confirm the suitability of the product for the assessment.

The following requirements apply:

- only products which perform a security-enforcing function, such as firewalls, virtualisation products and cryptography, are eligible to be certified.
- vendors are expected to provide technical assistance to labs during evaluation to ensure a good understanding of the product undergoing assessment.

- evaluation involves mostly ‘black box’ testing so it doesn’t require access to vendors’ commercially sensitive information, although this type of information may speed up the assessment.

Products are tested against the so-called CPA Security Characteristics. Product developers need these to fully understand which security enforcing functions will be assessed by the test labs. Purchasers can use these to know more about what functionality has and has not been assessed in a product. Specific security characteristics have been drawn up for the following product categories:

- Data-at-rest encryption products
- Data sanitisation products
- Email encryption products
- Software Execution Control products
- Mobile Device Management solutions
- Remote Desktop products
- Firewalls
- Secure real-time communication solutions
- Virtualisation platforms
- Virtual Private Network (VPN) solutions
- Smart Meters

All CPA Security Characteristics can be found at https://www.ncsc.gov.uk/document/security-characteristics-collection.

CPA certification is valid for two years and allows products to be updated during the lifetime of certification as updates may be required to solve new vulnerabilities. Costs and duration not known.

3.1.2.4 Practice

A list of certified products can be found through this link: https://www.ncsc.gov.uk/searchtype/product?f[0]=field_product_certifications%253Afield_assurance%3A226

Currently, 129 different products have been certified.

3.1.2.5 Formal Status

UK government information assets may be classified into three types: OFFICIAL, SECRET and TOP SECRET. A Foundation Grade CPA evaluation directly maps to the threat model for OFFICIAL, which means that products that obtain CPA evaluation may be used to process and store such information. Security-enforcing products used by UK governments or UK Critical National Infrastructure and for which CPA Security Characteristics are in place (see above) must obtain CPA certification.

3.1.2.6 Relation to other standards / schemes

In some cases, commercial products can gain CPA Foundation Grade certification not only through the CPA scheme, but also through Common Criteria (CC) certification. This is the case if a so-called 'CPA mapping' exists for the Protection Profile that was used in the product's CC evaluation.

3.1.3 Common Criteria (CC)

3.1.3.1 Focus

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently at version 3.1 revision 4. The standard comprises catalogues of functional and assurance requirements, together with instructions on how to construct security specifications and conduct independent security evaluations based on these requirements.

Common Criteria is a framework in which product users can specify their security functional and assurance requirements through the use of Protection Profiles (PPs). Product manufacturers may then implement and make claims about the security attributes of their products in a Security Target, which may match one or more specific PPs. Testing laboratories can then evaluate the product against its Security Target to determine whether it actually meets the claims. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standard, and repeatable manner at a level that is appropriate to the target environment.

Apart from stating the Security Functional Requirements of a class or products, a Protection Profile or Security Target also establishes the level of confidence that may be attributed to the product's security features through the security assurance processes:

- Security Assurance Requirements (SARs) that are descriptions of measures taken during development and/or evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, that full functional testing is performed, or that a certain level of vulnerability analysis (penetrating testing) is reached.
- The Evaluation Assurance Level (EAL) is a numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive). Higher EALs do not necessarily imply 'better security', they only mean that the claimed security assurance of the target of evaluation (TOE) has been more extensively verified. However, for lower EALs the bar to pass vulnerability analysis can be lower. Therefore, in practice there is a correlation. EALs may be augmented with additional assurance activities from Part 3 of the CC, resulting in a EAL level such as EAL4+.

3.1.3.2 Associated Evaluation Scheme and Governance

The Common Criteria Recognition Arrangement (CCRA) is an arrangement between participating evaluation schemes and other interested organisations. The participating schemes ensure that products are evaluated by competent and independent licensed laboratories to common standards, so as to determine the fulfilment of particular security properties, to a certain extent or assurance. The resulting certificates are then recognised by all the signatories of the CCRA.

Note that certificate recognition means that CCRA participants recognize that the evaluation scheme in the certificate authorizing nation correctly performed all of the activities involved in CC and CCRA processes. This does not imply that the certified IT product met the security requirements of another CCRA participant nation. To achieve the latter purpose, collaborative Protection Profiles (cPP) are developed by International Technical Communities consisting of vendors, test laboratories, CCRA nations, and academia. cPPs are developed with strong engagement and endorsement of all CCRA participant nations.

Within the CCRA only evaluations using collaborative protection profiles, up to Evaluation Assurance Level 2 (EAL 2) are mutually recognised (including augmentation with flaw remediation). In parallel with the CCRA, the European countries within the former ITSEC scheme recognise higher EALs under the so-called SOG-IS European Mutual Recognition Agreement (SOG-IS MRA). Most but not all SOG-IS members are also CCRA members. The SOG-IS MRA covers two technical domains: Smartcards and Similar Devices and Hardware Devices with Security Boxes.

The overall governance of the Common Criteria scheme is similar under both agreements. Certificates can be independently issued by any of the Certificate Authorizing Schemes. Each of these Schemes has recognized a number of evaluation laboratories, which carry out the actual product evaluations.

3.1.3.3 Process

The evaluation serves to validate claims made about a product. To be of practical use, the evaluation must verify the product's security features. This is done as follows:

1. A Protection Profile may be created by a user community, which identifies security requirements for a class of products (for example, smart cards used to provide digital signatures or network firewalls). These Security Functional Requirements are taken (and adapted) from Part 2 of the Common Criteria standard (ISO/IEC 15408).
2. The Protection Profile is certified by an independent test laboratory to make sure that it complies with all applicable CC requirements.
3. A product vendor chooses to create a product complying with one or more PPs and writes a Security Target explaining how the security requirements in these PPs are met by the product. If a PP does not exist for the product type the vendor may prepare their own Security Target directly.
4. A recognized evaluation laboratory selected by the vendor evaluates the product (Target of Evaluation, ToE) against the Security Target to make sure that the claims made by the vendor in the ST are actually valid.
5. Based on the evaluation report, the Certificate Authorizing Scheme that recognized the laboratory issues a Common Criteria certificate for the product.

Note that Common Criteria describes the set of general actions the evaluator is to carry out., but does not specify procedures to be followed in carrying out those actions. Supporting documentation (https://www.commoncriteriaportal.org/files/operatingprocedures/2006-09-003.pdf) defines how the criteria and evaluation methods are applied when certifying specific technologies. They replace multiple individual interpretations, and hence provide clarity for developers, evaluators, and users. Their relevance and use for particular technologies is approved by the CC Management Committee following submission of a suitable rationale. Their subsequent maintenance is a responsibility of the CC Development Board. There are two classes of CC supporting documentation:

- Those that are termed 'Mandatory Supporting Documents', and are required to have been applied when a product involving the particular technology is certified to support mutual recognition.
- Those that are termed 'Guidance Supporting Documents' contain more general advice.

Additionally, for evaluations under the SOG-IS agreement additional guidance applies; see http://www.sogisportal.eu/uk/supporting_doc_en.html. Examples of this include:

- The SOG-IS Crypto Evaluation Scheme, which recognises agreed cryptographic mechanisms, in particular with regard to their security strength, and offers guidance on conformance testing and the evaluation of the security architecture and implementation of the cryptographic measures implemented in an IT product.
- The SOG-IS Joint Interpretation Working Group (JWIG) Minimum Site Requirements, which defines a set of minimum requirements for the security of the site where a product is developed. These requirements are applicable from EAL3 upwards, but especially for EAL4+ and higher. They are mandatory for Common Criteria evaluations of smartcards and similar devices, including related software development, but can be verified during any type of Common Criteria evaluation.
- The guidance document ‘Application of Attack Potential to Smartcards’ explains the so-called JHAS rating methodology for attacks on the security of a smart card. For more information, see Appendix 1.

3.1.3.4 Practice

A typical evaluation can take anywhere from six to fourteen months. Consequently, evaluation is costly; the exact amount depends on the complexity of the product and the desired Evaluation Assurance Level. Note that this is only for the evaluation of a specific TOE against an existing Protection Profile or using no Protection Profile. In case a new Protection Profile is necessary, the process of certification of such a PP may again take a year.

3.1.3.4.1 CCRA

The CCRA covers mutual recognition between evaluation schemes for evaluations against collaborative protection profiles up to EAL1-2.

A list of Certificate Authorizing Schemes under the CCRA can be found at http://www.commoncriteriaportal.org/ccra/schemes/; it lists 17 nations. An additional 10 countries are listed as Certificate Consuming Members, meaning they accept Common Criteria certificates but do not issue them.

A list of certified Protection Profiles can be found at http://www.commoncriteriaportal.org/pps/. Currently over 130 PPs are listed, 6 of which are cPPs.

A list of licensed laboratories can be found at http://www.commoncriteriaportal.org/labs/; it lists 69 labs. However, there is some overlap in this list, as some laboratories are licensed under multiple Authorizing Schemes.

A list of certified products can be found at https://www.commoncriteriaportal.org/rss/certified_products.xml. As of March 2017, the list contained over 2800 products.

3.1.3.4.2 SOG-IS MRA

The number of European countries participating in the SOG-IS MRA is 11. Each of these countries has qualified a number of IT Security Evaluation Facilities (ITSEFs) that carry out the actual evaluations. An ITSEF may be qualified for 'All Products' on EAL 1-4, for 'Smartcards and similar devices' on EAL1-7, and/or for 'Hardware Devices with Security Boxes' on EAL1-7. So there is some overlap in the list. The full list of ITSEFs can be found at http://www.sogis.org/uk/status_participant_en.html.

3.1.3.5 Formal Status

Common Criteria is often used as the basis for a government-driven certification scheme, and typically evaluations are conducted for the use of government agencies and critical infrastructure.

3.1.3.6 Relation to other standards / schemes

Common Criteria is adopted as the ISO/IEC 15408 standard. Several companion standards exist:

- ISO/IEC 18045 (Common Evaluation Methodology) defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation. Note that this standard does not define evaluator actions for certain high-assurance Common Criteria components, where there is no generally agreed guidance.
- ISO/IEC TR 20004 refines the AVA_VAN assurance family activities defined in ISO/IEC 18045, and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation.
- ISO/IEC NP 19896-3 contains competence requirements for the knowledge, skills and effectiveness of Common Criteria evaluators.

Several other schemes for product security evaluation have been based on or greatly influenced by Common Criteria. Often, these schemes aim to strike a balance with the thoroughness of a full Common Criteria evaluation and the costs and throughput time of such an evaluation. Such schemes include:

- the CSPN scheme (section 3.1.1)
- the CAP scheme (section 3.6.2)
- the CPA scheme (section 3.1.2)
- the NITES scheme (section 3.1.5)
- the EMVCo Security Evaluation scheme (section 3.5.1)

- the MIFARE Security Evaluation scheme (section 3.9.1)

An ASD Cryptographic Security Evaluation (section 3.6.1) is only possible for products that already have been CC-certified.

3.1.4 European Privacy Seal

3.1.4.1 Focus

The European Privacy Seal certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection and taking into account the legislation in the EU Member States. The privacy certificate aims to facilitate an increase of market transparency for privacy relevant products and an enlargement of the market for Privacy Enhancing Technologies and finally an increase of trust in IT.

The scope can be either an IT product or an IT service.

IT products or services suitable for certification are products or services which are meant to be used by a multitude of users and will results in the IT-based processing of personal data. Basically, the following types of IT products are to be distinguished:

- Hardware products such as a hardware firewall or an external hard disk which provides for proper encryption of data
- Software products such as database applications, a software module for the obfuscation of video data or an age verification module to be used with cigarette vending machines. The meaning of the notion software products includes mobile apps. However, software that is provided as software as a service (SaaS) qualifies as an IT based service rather than as an IT product.

The Target of Evaluation (ToE) is the concrete object of an evaluation. It may be either one or several part(s) of an IT product, a complete product or even a combination of several products.

Manufacturers and vendors of IT products and providers of IT-based services can apply for a seal even if they are not subject to EU data protection law, but want to prove the compliance of their processing operations with EU law nevertheless. This may cover, but is not limited to the subject matter of Article 46(2) (f) of the GDPR, ref. [2].

3.1.4.2 Associated Evaluation Scheme and Governance

EuroPriSe governs the European Privacy Seal, its criteria, and the acting certification authority. The procedure consists of an evaluation of the IT product or IT service by admitted legal and IT experts and a validation of the evaluation report by the certification authority.

Find a list of registered experts bellow: https://www.european-privacy-seal.eu/EPS-en/register-of-experts

3.1.4.3 Process

EuroPriSe criteria translates the regulatory requirements into questions that can be answered in the context of an audit or certification. The EuroPriSe criteria and requirements for the certification of IT products and IT-based services can be found here:

https://www.european-privacy-seal.eu/AppFile/GetFile/e5ed7122-74b1-4f75-a5af-fb0c317bd20b

Not each and every question will be applicable to each and every product or service. The certification authority shall ensure that in any certification procedure the relevant criteria are applied and that all related questions are answered in a plausible manner, the appropriate granularity, and at a uniform and comparable level. Together with a transparent certification procedure conducted by a financially independent and impartial third party they build the foundation for confidence and trust.

The process looks as follows:

- Choose and contact a legal and a technical expert from the expert register
- Discuss evaluation with experts
- Contact the certification authority and schedule a preparatory first meeting
- Agree on evaluation with experts
- Apply for certification and conclude a Certification Agreement with the Certification Authority
- Experts conduct evaluation
- Manufacturer/Service provider hands in
    - Evaluation Report (confidential) compiled by legal and technical expert and approved by manufacturer
    - Short Public Report (public) compiled by legal and technical expert and approved by manufacturer

The costs: evaluations by experts are subject to remuneration; fees are individually negotiated by the parties.

The effort: certification efforts (validation by certification authority) are subject to remuneration. EuroPriSe certification fees are available on request.

3.1.4.4 Practice

Find below and overview of the certified (awarded seals) products and services: https://www.european-privacy-seal.eu/EPS-en/Awarded-seals

3.1.4.5 Formal Status

The European Privacy Seal is not formally required by any government or public authority. However, the European Privacy Seal could help to show compliance to applicable laws and regulations, e.g. the General Data Protection Regulation (see ref. [2]).

3.1.4.6 Relation to other standards / schemes

The latest version of the EuroPriSe criteria incorporates the new legal requirements that are introduced by the General Data Protection Regulation (GDPR, ref. [2]) which will be applicable from late May 2018 in all of the EU. Its predecessor is built on the requirements of the General Data Protection Directive (Directive 95/46/EC). Both versions integrate also other important EU regulations in relation to data protection, such as the ePrivacy Directive (ref. [4] and [5]).

EuroPriSe offers applicants the possibility to conduct combined certification projects together with ULD to receive the ULD Gütesiegel; see section 3.1.8.6.

3.1.5 National IT Evaluation Scheme (NITES)

3.1.5.1 Focus

The Singaporean National IT Evaluation Scheme (NITES) was setup by the Security Accreditation Committee (SAC). The NITES scheme specifications and requirements were not made public by CSA. There are four categories of products that can be evaluated under NITES: secure portable storage, network related devices (i.e. VPN), file/folder encryption, and key management solutions (i.e. HSM).

3.1.5.2 Associated Evaluation Scheme and Governance

The Cyber Security Agency (CSA) is acting as the Validation Body on behalf of SAC.

Currently, there is only one active accredited test laboratory.

3.1.5.3 Process

NITES evaluation are performed according to the NITES Evaluation Methodology, which is approximately equivalent to the EAL4+ package in Common Criteria.

Evaluation is to be performed by an accredited test lab.

3.1.5.4 Practice

The NITES scheme is active. Prospective vendors to government agencies are told to get equipment NITES evaluated and are directed to a test lab and/or CSA for advice on evaluation.

Products that pass evaluation are listed on the Government Evaluated Security Product List (GESPL). Unfortunately, this list is not publicly accessible.

3.1.5.5 Formal Status

Ministries, Agencies and Statutory Boards of the Singapore Government must utilise the GESPL to identify suitable IT products for their sensitive deployments.an

CSA is in the process of being accredited by Common Criteria as an issuing Certification Body. Once this is complete, the NITES scheme would lose its relevance.

3.1.5.6 Relation to other standards / schemes

NITES is an adaptation of Common Criteria v3.1, approximately EAL4+ with additions mainly on ATE_IND-2 (Independent Testing) and AVA_VAN-5 (Vulnerability Analysis). NITES has a provision to recognise EAL4 CC-certified products (with some conditions or additional tests performed).

3.1.6 Software Improvement Group (SIG) Software Quality Model for Security

3.1.6.1 Focus

The Software Improvement Group (SIG) Software Quality Model for Security is based on ISO 25010 and describes five quality characteristics of software security and their relation to nine system properties. The model describes the generic controls that need to be in place and describes specific controls that are needed depending on the situation. This way, the model offers a technology and context-independent frame of reference to evaluate controls.

3.1.6.2 Associated Evaluation Scheme and Governance

The Software Improvement Group is headquartered in Amsterdam, with regional offices in the Nordics, Belgium, Germany and Greece. Its mission is to give organisations the detailed insight they need to achieve better code quality and productivity.

A SIG software security evaluation involves a combination of systematic expert code review and the application of commercial and open source tooling. Each system property (e.g. data transport) represents a view of the system, and for each property a number of sub-properties are described that represent controls (best practices) that need to be in place. The criteria are in the relevant standards. Scoring the sub-properties with ‘weak’, ‘normal’ or ‘strong’ leads to a score between one and five stars for each system property. Each system property has relations to one or more software security characteristics (e.g. confidentiality), leading to a score for each of these characteristics. This eventually leads to a final system score between one and five stars.

3.1.6.3 Process

Companies wishing to have a SIG Security Evaluation of their software should start by contacting SIG.

3.1.6.4 Practice

The ISO 17025-certified SIG evaluation lab has applied the Quality model for Security more than 100 times.

3.1.6.5 Formal Status

None.

3.1.6.6 Relation to other standards / schemes

The SIG Security Evaluation is partly based in ISO 25010 (System and Software Quality Model) and binds leading standards into one framework to evaluate and measure the quality of security in software.

The SIG model contains a library of mappings to relevant standards (e.g. OWASP ASVS, see section 3.7.1).

3.1.7 UL Cybersecurity Assurance Program (UL 2900-1 / 2)

3.1.7.1 Focus

As cyber-attacks become more sophisticated, harder to protect against, and costlier than ever, security precautions are critical. It is estimated that by 2018, 66% of networks will have an IoT security breach. Product manufacturers worldwide are asking for support in their organisations to bring safer and more secure products and systems to market. Purchasers wanted to address security in their supply chain by having an independent trusted third party perform assessments on connected products and on the vendors that manufacture, install, operate, and maintain those products.

The aim of the UL Cybersecurity Assurance Program (UL CAP) is to mitigate safety and performance risks that are inherent to the use of connected products. By using the UL 2900 series of cybersecurity standards, UL CAP offers testable cybersecurity criteria for network-connectable products.

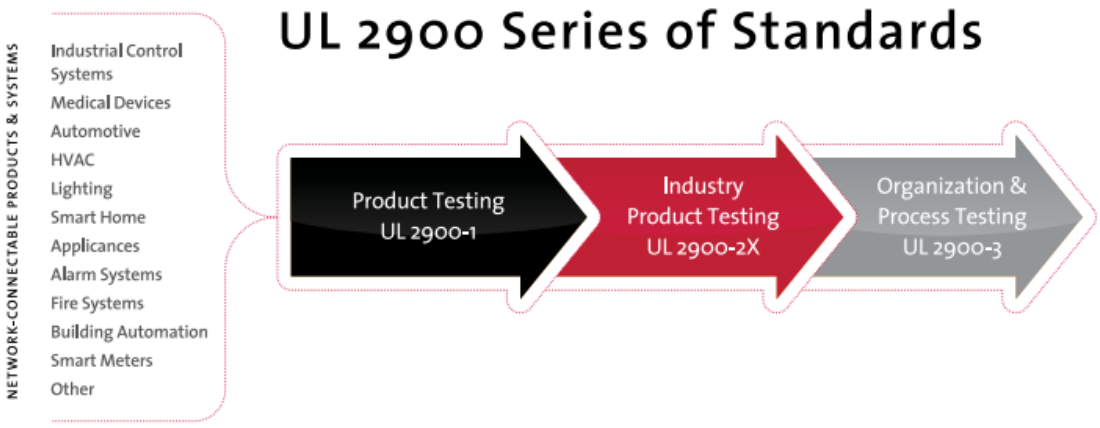
The UL 2900 series was developed with input from major stakeholders representing the U.S. Federal government, academia and industry. The series consists of the following standards:

- UL 2900-1 (Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements)
- UL 2900-2-1 (Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems)
- UL 2900-2-2 (Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems)

3.1.7.2 Associated Evaluation Scheme and Governance

The evaluation scheme and governance is performed by UL. The testing lab that tests against the UL 2900 standard for network-connectable devices is separated (within UL) with the Evaluation Scheme that approves and hands-out the actual certificate.

3.1.7.3 Process



The UL 2900 series of standards contains the ability to test and evaluate based on the following criteria:

- Fuzz testing of products to identify zero day vulnerabilities over all interfaces
- Evaluation of known vulnerabilities on products that have not been patched using the Common Vulnerability Enumerations (CVE) scheme
- Identification of known malware on products
- Static source code analysis for software weaknesses identified by Common Weakness Enumerations (CWE)
- Static binary analysis for software weaknesses identified by Common Weakness Enumerations (CWE), open source software and third party libraries
- Specific security controls identified for use in products that reduce the security risk associated with:
    - Access control and authentication on products
    - Cryptography used in products
    - Remote communications to products
    - Software updates on products
    - Decommissioning of products
- Structured penetration testing of products based on flaws identified in other tests
- Risk assessment of product security mitigation designed into products.

The price and duration of the UL CAP depends on the scope of the product.

3.1.7.4 Practice

UL 2900 was released on April 2016. To date (22-Feb-2017) two products have been certified against UL CAP.

3.1.7.5 Formal Status

None. However, the UL CAP services and software security efforts are recognised within the U.S. White House Cybersecurity National Action Plan (CNAP) as a way to test and certify network-connectable devices within the IoT supply chain.

3.1.7.6 Relation to other standards / schemes

A UL CAP assessment for network-connectable devices (based on UL 2900-1 or one of the part of UL 2900-2) may or may not be done together with an assessment of the organisation, based on UL 2900-3. Certification of the product is only possible if the organisation is assessed as well; otherwise, only a Product Evaluation Report Summary will be issued.

3.1.8 ULD Datenschutz-Gütesiegel

3.1.8.1 Focus

The scope of the ULD Datenschutz-Gütesiegel (Data Protection Seal of Quality) encompasses IT products in general, i.e. hardware, software, automated processes and services. A prerequisite is that they are suitable for use by public authorities.

A Gütesiegel certifies that the compatibility of a product with the rules on data protection and data security has been established in a formal procedure. On this basis, the ULD recommends the use of the product by the public authorities in the federal state of Schleswig-Holstein.

The ULD provides a regularly updated catalogue stating the requirements for IT products with regard to privacy protection, which can be found at https://www.datenschutzzentrum.de/uploads/guetesiegel/guetesiegel-anforderungskatalog.pdf (in German).

3.1.8.2 Associated Evaluation Scheme and Governance

The goals of the 'Unabhängiges Landeszentrum für Datenschutz' (ULD, Independent State Centre for Data Protection) are:

- Following up all alleged data protection violations and sending the concerned parties a written final assessment.
- Monitoring the processing of data by Schleswig-Holstein authorities; objecting to violations of the data protection law and demanding rectification of defects.
- Advising authorities, corporations and citizens on all data protection issues, for example when setting up new computer systems or when questions arise on the interpretation of data protection law or legislation.

3.1.8.3 Process

Manufacturers or vendors commission a specialist or test centre of their choosing, accredited by the ULD. The test centre then carries out legal and technical checks on the product. The product is checked for compatibility with the provisions on privacy protection and data security. Particular attention is paid to data avoidance and minimization, to data security and revisability and to ensuring the rights of those concerned.

The results are documented in a specialist report. This report and the application for certification are then submitted to the ULD. If the ULD approves the product as legally and technically correct, then a privacy protection seal is awarded for two years.

The seal of approval is awarded for a precisely described program version. If a modified version is to be distributed, manufacturers, experts and the ULD jointly check in a simplified procedure whether the modified product can bear the seal of approval. For fundamental changes, a new certification must be carried out.

3.1.8.4 Practice

Over 80 accredited test centres (or experts) are listed on the ULD Gütesiegel website. The number of approved products (since 2007) is over 50.

The European Union currently partly funds the ULD Datenschutz-Gütesiegel programme as part of its "e-region Schleswig-Holstein" programme. Thanks to this financial support, small and medium-sized enterprises (SME) in the region are being offered an incentive to obtain a ULD Datenschutz-Gütesiegel for their information technology products, whether software, hardware or automated processes. Companies meeting the funding criteria under the "eRegion Schleswig-Holstein" initiative receive a fixed sum to partially offset the costs of the certification. The ULD also provides its standard chargeable services in the certification process free of charge in these cases.

3.1.8.5 Formal Status

There is no legal obligation for the ULD Gütesiegel. However, public authorities in Schleswig-Holstein are legally bound to give preference to products that meet the data protection requirements when procuring IT products.

3.1.8.6 Relation to other standards / schemes

The ULD offers applicants the possibility to conduct combined certification projects together with EuroPriSe, see section 3.1.4

In case of a combined certification project, EuroPriSe and ULD collaborate closely. Privacy professionals who are accredited as legal and technical experts for both certification schemes may hand in a single evaluation report dealing with the requirements of both schemes. Either the EuroPriSe certification authority or ULD takes the lead in the certification project and is primarily responsible for the validation of the evaluation report. The competent employees of the other certification scheme build on the findings of the employees of the leading scheme and focus on verifying that requirements resulting from the particularities of their certification scheme (e.g., specific legal provisions of German or Schleswig-Holstein law) are met. This approach comes with synergetic effects that may lead to a reduction of the overall certification costs. In order to collaborate in a combined certification project, the EuroPriSe and ULD must be permitted by the applicant to exchange information that is relevant for the conduct of the certification project.

Successful finalisation of a combined certification project results in the award of both the European Privacy Seal and the ULD-Gütesiegel.

3.2 Standards and schemes for products used in Industry 4.0 and ICS (SWG 3.1)

3.2.1 ISA/IEC 62443 (Security for Industrial Automation and Control Systems)

3.2.1.1 Focus

See section 5.2.6.1.

3.2.1.2 Associated Evaluation Scheme and Governance

The ISA Security Compliance Institute (ISCI), a not-for-profit automation controls industry consortium, manages the ISASecure™ conformance certification program. ISASecure independently certifies industrial automation and control (IAC) products and systems to ensure that they are robust against network attacks and free from known vulnerabilities.

ISASecure does not offer assessments for integrator site engineering practices or asset owner operations and maintenance practices. ISASecure certifies off-the-shelf systems; not the site engineered / deployed systems.

ISCI offers three certifications in alignment with ISA/IEC 62443, see http://www.isasecure.org/en-US/Certification:

- ISASecure Embedded Device Security Assurance (EDSA) Certification, which is primarily based on IEC 62443-4-1 and IEC 62443-4-2.
- ISASecure System Security Assurance (SSA) Certification, which is primarily based on IEC 62443-3-3.
- ISASecure Security Development Lifecycle Assurance (SDLA) Certification

The first two certifications take into account both functional security and secure software development, and are available in different rigor levels. A supplier that holds an ISASecure SDLA certification thereby meets the SDLA evaluation element required to achieve ISASecure certification for their products or control systems. A supplier applying for a product certification that does not hold an SDLA process certification at the appropriate level, will undergo an SDLA evaluation at this level as a part of the ISASecure product evaluation itself.

Note: the IECEE is establishing the IECEE System Industrial Cyber Security Program, see section 5.2.6.2. From the published guidance documentation, it appears that the scope of this program will also include products. This certification is therefore an alternative to ISASecure certification.

3.2.1.3 Process

ISCI does not operate an internal testing lab, but instead partners with qualified labs to perform industrial automation and control systems (IACS) cybersecurity assessments. A list of accredited

ISASecure Certification Bodies can be found at http://isasecure.org/en-US/Certification-Bodies/Accredited-ISASecure-Certification-Bodies. As per February 2017, two companies were listed.

The product certification process is not specified in detail on the ISASecure website. Instead, suppliers are directed to contact one of the accredited Certification Bodies.

ISCI has also qualified a number of test tools for automated security testing. A list of such tools can also be found on the website.

3.2.1.4 Practice

A list of ISASecure EDSA-certified devices can be found at http://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Devices. As per February 2017, around 15 devices were listed, mostly DCS controllers.

3.2.1.5 Formal Status

The government of Japan has adopted ISASecure as part of their critical infrastructure protection scheme and has set up an accredited test lab to process certifications locally in Japan. Japanese-language translations of ISASecure certification specifications are available on the Japanese ISASecure Certification Scheme web pages.

3.2.1.6 Relation to other standards / schemes

See section 5.2.6.6.

3.2.2 IACS Cybersecurity Certification Framework

3.2.2.1 Focus

The European Reference Network for Critical Infrastructure Protection (ERNCIP) project aims to foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities.

One of the Thematic Groups within ERNCIP deals with Industrial Automated Controls Systems (IACS) cybersecurity certification. This group's goal is to encourage the provision of certified components as a contribution to improving IACS' in-depth cyber-defence. The work of this group has led to an elaborate proposal for a European IACS components Cybersecurity

Certification Framework (ICCF). The ICCF focuses on the security of IACS components, rather than subsystems or even complete IACSs.

The ICCF Framework proposes a IACS Compliance & Certification Scheme (ICCS), which consists of four levels:

- ICCS-A1 (Self-declaration of compliance) - intended for common, non-critical products.
- ICCS-A2 (Third-party compliance assessment) - also intended for common, non-critical products, but offers an enhanced level of evaluation.

- ICCS-B (Cyber resilience certification) – intended for products used in critical infrastructures
- ICCS-C (Full cyber resilience certification) – intended for products used in the most critical environments, such as defence systems and nuclear industries.

3.2.2.2 Associated Evaluation Scheme and Governance

The evaluation scheme for the European ICCF scheme and the governance of this scheme are still under discussion. The following parties are proposed to have a role:

- The European Commission
- International standardisation bodies
- The Thematic Group of the European Joint Research Centre (JRC)
- National cybersecurity agencies
- Corporate stakeholders (vendors, buyers, certifiers, laboratories).

3.2.2.3 Process

The proposed evaluation process bears similarities to Common Criteria, see section 3.1.3. It uses Protection Profiles for generic 'classes' of devices, and a Security Profile for each individual device implementation.

3.2.2.4 Practice

None yet. Trials have been scheduled for 2017; the scheme is planned to go live in 2018.

3.2.2.5 Formal Status

None.

3.2.2.6 Relation to other standards / schemes

The ICCF scheme takes into account especially the work done in the ISA/EC 62443 standards; see section 3.2.1. For example, the IEC 62443-4-2 standard was adopted as the basic set of

cybersecurity requirements. Moreover, the proposed evaluation scheme is heavily influenced by Common Criteria.

3.3 Standards and schemes for products used in energy networks and smart grids (SWG 3.2)

3.3.1 IEEE 1686 (Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities)

3.3.1.1 Focus

This standard defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection programs. Security regarding the access, operation, configuration, firmware revision and data retrieval from an IED are addressed.

More info: https://standards.ieee.org/findstds/standard/1686-2013.html

3.3.1.2 Associated Evaluation Scheme and Governance

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard.

The IEE 1686 standard is sponsored by the IEE PES Power & Energy Society (http://www.ieee-pes.org/) that provides the world's largest forum for sharing the latest in technological developments in the electric power industry.

NIST (the National Institute of Standards and Technologies) has been tasked with laying out a plan for the transformation of the U.S.'s aging energy infrastructure into interoperable Smart Grid. As part of their task, they've put together an open forum for members to collaborate on standards development called the Smart Grid Interoperability Panel (SGIP). NIST and the SGIP are selecting a framework of standards which are being used as the backbone of the new Smart Grid. The IEEE 1686 standard is one of these.

3.3.1.3 Process

Not applicable.

3.3.1.4 Practice

Not known.

3.3.1.5 Formal Status

None.

3.3.1.6 Relation to other standards / schemes

This standard is designed to provide the tools and features for a user to implement an IED security effort in response to NERC CIP requirements; see section 5.3.3.

This standard references:

- IEEE 1711 Trial-use standard for a cryptographic protocol for cyber security of substation serial links.

Other standards that reference this standard:

- IEEE 1815 Electric Power Systems Communications-Distributed Network Protocol (DNP3).
- ETSI - TR 103 118 Machine-to-machine communications (M2M); smart energy infrastructures security; review of existing security measures and convergence investigations.
- IEC/TR 62351-10: Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 10: Security Architecture Guidelines.
- IEC TR 62351-13: Power systems management and associated information exchange - data and communications security - part 13: guidelines on security topics to be covered in standards and specifications.

3.3.2 IEEE C37.240 (Cybersecurity Requirements for Substation Automation, Protection, and Control Systems)

3.3.2.1 Focus

This document provides technical requirements for substation cybersecurity. It presents sound engineering practices that can be applied to achieve high levels of cybersecurity of automation, protection, and control systems independent of voltage class or criticality of cyber assets. Cybersecurity includes trust and assurance of data in motion, data at rest, and incident response.

These requirements are categorized as follows:

- High level requirements and priorities for interface categories
- System communications components
- Functional Requirements
- User authentication and authorization
- Data-in-motion protection
- Configuration management
- Security event auditing and analysis/incident response
- Security testing

3.3.2.2 Associated Evaluation Scheme and Governance

There is no official evaluation scheme regarding this standard.

The Institute of Electrical and Electronics Engineers (IEEE) is a member based organization. Its activities include developing standards dedicated to advance technology for the benefit of humanity.

3.3.2.3 Process

None.

3.3.2.4 Practice

Not publicly known.

3.3.2.5 Formal Status

None.

3.3.2.6 Relation to other standards / schemes

Related standards include:

- IEC 62351-8, Power systems management and associated information exchange—Data and communications security—Part 8: Role-based access control)

3.4 Standards and schemes for products used in the telecom industry (SWG3.8)

3.4.1 GSMA Network Equipment Security Assurance Scheme

3.4.1.1 Focus

The Network Equipment Security Assurance Scheme (NESAS) of the GSMA is focused on Product Security Assurance for network equipment defined by the 3GPP standardisation organisation. So in essence all 2G/3G/4G/5G mobile telephony equipment for the mobile/telco communications infrastructure comes under the remit of the scheme. The 3GPP SA3 security standards development group develop the security requirements and associated test cases for the different networks elements.

3.4.1.2 Associated Evaluation Scheme and Governance

The GSMA SECAG (Security Assurance Group) has defined and developed the scheme. The GSMA NESAS Accreditation Board accredit vendors' development processes. Security evaluations are carried out by ISO17025 certified security test labs.

3.4.1.3 Process

Firstly, to be NESAS-compliant, vendors must submit their product development and product lifecycle processes for accreditation by GSMA. Audits are carried out on these processes by a 3rd party audit company appointed and overseen by the GSMA NESAS Accreditation Board consisting of Network Operators.

Secondly, vendors submit their product to undergo an evaluation by an ISO17025 certified test lab. The test lab checks that the product has been developed according to the processes that have been accredited by GSMA. The product is then tested by the test lab against the requirements defined by the 3GPP SA3 group.

Testing consists of security functional tests and security non-functional tests such as vulnerability scans, robustness tests, penetration test.

An evaluation report is provided to the vendor by the test lab. Operators may then request vendors to share their report with them to prove compliance to NESAS.

3.4.1.4 Practice

The NESAS scheme is currently being piloted by the GSMA and is expected to be launched in the second quarter of 2017.

3.4.1.5 Formal Status

The India DoT have stated that they intend to use the security requirements and test cases defined by 3GPP SA3 as part of their in-country security certification program.

3.4.1.6 Relation to other standards / schemes

3GPP defines the security requirements and test cases, while GSMA defines the scheme process, test lab requirements etc.

The following documents are in preparation by 3GPP:

- 3GPP TR 33.916 (Security Assurance Methodology (SCAS) for 3GPP network products)
- 3GPP TR 33.926 (Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes)
- 3GPP TS 33.117 (Catalogue of general security assurance requirements
- 3GPP TS 33.116 (Security Assurance Specification (SCAS) for the MME network product class)

The following documents are in preparation by the GSMA:

- GSMA FS.13 (Network Equipment Security Assurance Scheme – Overview)
- GSMA FS.14 (Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation Requirements and Process)
- GSMA FS.15 (Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process)
- GSMA FS.16 (Network Equipment Security Assurance Scheme – Dispute Resolution Process)

3.5 Standards and schemes for products used in the payment industry

3.5.1 EMVCo Security Evaluation

3.5.1.1 Focus

EMVCo is an organisation of the major payment schemes. Its goal is to develop and maintain a set of specifications, most prominently the contact and contactless EMV specifications, that define requirements to ensure worldwide interoperability and acceptance of secure payment transactions.

All contact and contactless payment cards used for making an EMV payment worldwide must undergo a security evaluation. EMVCo manages and evolves the security requirements and related testing processes.

The EMVCo Security Evaluation Process is based on a complete set of published EMVCo documents (specifications, requirements, and security guidelines) made available to product providers and security evaluation laboratories for the development and security evaluation of their products. There are three different Security Evaluations:

- The **Integrated Circuit (IC) Security Evaluation** considers the security of the IC product, and is intended to provide a high level of assurance in the security functions that are designed to effectively deal with known attack methods. Attack methods include threats such as reverse engineering, information leakage, and fault injection.
- In EMVCo terminology, a Platform is the collective name for the IC hardware with its dedicated software, Operating System, Run Time Environment, and Platform environment on which one or more applications can be executed. EMVCo's **Platform Security Evaluation** considers how the Platform developed by the product provider follows relevant security guidelines. An important factor is how the product provider builds upon the security of the IC to provide security for the complete Platform product.
- The **Integrated Circuit Card (ICC) Security Evaluation** considers how the payment applications developed by the product provider follow the relevant security guidelines. An important factor is how the product provider builds upon the security of the IC and the OS or the underlying approved Platform to provide overall security for a payment application on the ICC.

3.5.1.2 Associated Evaluation Scheme and Governance

EMVCo consists of six members, namely American Express, Discover, JCB, MasterCard, UnionPay, and Visa. They are supported by dozens of banks, merchants, processors, vendors and other industry stakeholders who participate as EMVCo Associates. EMVCo is managed by the Board of Managers, which is comprised of two representatives from each of the member payment systems. The EMVCo Executive Committee, also managed by payment system representatives, provides guidance on EMVCo's long-term strategy. Various Working Groups complete EMVCo's work, and decisions are made on a consensus bases to ensure card infrastructure uniformity.

3.5.1.3 Process

1. Sign EMVCo Agreement
    - EMVCo and the product provider sign an EMVCo agreement covering the EMVCo Security Evaluation Process, including confidentiality and other aspects.
2. Complete EMVCo Registration Questionnaire
    - The product provider completes an EMVCo questionnaire defining details of the product intended for evaluation and related administrative information.
3. Initial Discussion
    - Initial discussions between the product provider and the EMVCo Security Evaluation Secretariat are conducted to develop a common understanding of the evaluation process and of the underlying information required.
4. Product Design
    - The product provider finalises the design of the product (if not completed prior to initiation of the EMVCo Security Evaluation Process) or updates the product in response to the requirements derived from the relevant security guidelines.
5. Select Laboratory and Decide Evaluation Details
    - After the EMVCo Security Evaluation Secretariat reviews any security evaluations of the product performed by the product provider or a third party, the product provider and the EMVCo Security Evaluation Secretariat agree on precise details of the EMVCo evaluation.
6. Assess Product and Product Provider Infrastructure
    - The evaluation of the IC, Platform, or ICC product includes a threat and vulnerability assessment of identified security assets.
7. Submit Reports to EMVCo Security Evaluation Secretariat
    - The laboratory prepares an evaluation report package.
8. Validate Laboratory Evaluation Reports
    - The EMVCo Security Evaluation Secretariat reviews the EMVCo Evaluation Report from the security evaluation laboratory.
9. Risk Analysis
    - Based on the evaluation results provided by the laboratories the product provider and the EMVCo Security Evaluation Secretariat together – typically during a meeting – perform an assessment of the risks resulting from the vulnerabilities discovered.
10. Issue EMVCo Compliance Certificate
    - If the EMVCo Summary Report prepared by the EMVCo Security Evaluation Secretariat concludes that sufficient assurance has been demonstrated, and is approved by the SEWG, EMVCo will issue the product provider an EMVCo Compliance Certificate for that product.

Unless the certificate is withdrawn or the product is superseded by newer products from the product provider, products with an EMVCo Compliance Certificate are removed from the EMVCo Approved Products list after one year for IC and Platform products and after three years for ICC products, unless approval is renewed. Products that reach the six-year limit will be removed from the list.

3.5.1.4 Practice

A total of 11 laboratories have been fully or provisionally recognised by EMVCo for IC, Platform and/or ICC evaluations. An overview is given here: http://www.emvco.com/approvals.aspx?id=99

An overview of the approvals and certificates can be found on the following website:

https://www.emvco.com/approvals.aspx?id=31

3.5.1.5 Formal Status

EMVCo acts as the security certification entity for all approvals relating to the security of IC, Platform, and ICC products intended for use in payment cards issued by EMVCo members.

3.5.1.6 Relation to other standards / schemes

For EMVCo IC and Platform approvals, the same assessment is used as for a Common Criteria (see section 3.1.3) evaluation of a smart cards at EAL4+ (AVA-VAN.5) or a MIFARE Security Certification (see section 3.9.1). All of these schemes use the same attack rating method, called JHAS. All of them use the same set of attacks (side channel, fault, etc.) and require the same number of points for all attacks paths to achieve.

As a consequence, all payment schemes (MasterCard, Visa etc.) allow the use either a EMVCo IC and Platform approval or a CC approval using a suitable Protection Profile as a basis for their payment cards. A Platform approved under either of these schemes still need to be combined with a payment application and undergo an ICC Security Evaluation in case of a CCD/CPA card or a scheme-specific security evaluation in case the application complies with another payment application specification.

For more information on the JHAS attack rating method, see Appendix 1.

3.5.2 PCI PTS HSM Security Requirements

3.5.2.1 Focus

The PCI Council has set requirements to ensure the security around Hardware Security Modules (HSM). Applications and processes concerning payments and cardholder verification may be supported by HSMs. Such processes include:

- PIN Processing
- 3-D Secure
- Card Verification
- Card Production and Personalisation
- EFTPOS (Electronic Funds Transfer at Point of Sale)
- ATM Interchange
- Cash Card Reloading
- Data Integrity
- Chip Card Transaction Processing

3.5.2.2 Associated Evaluation Scheme and Governance

Similar as described in section 3.5.3.2 for PCI PA DSS.

3.5.2.3 Process

The security assessment consists of physical security requirements, logical security requirements, and device security requirements. The assessments are performed by third-party testing laboratories.

3.5.2.4 Practice

Not known.

3.5.2.5 Formal Status

All aspects relating to compliance, enforcement, and adoption of these standards, including all issues relating to risk, are the responsibility of the individual payment card brands. As of April 2016, the card schemes have not yet published any mandates regarding the deployment of PCI HSM compliant devices.

3.5.2.6 Relation to other standards / schemes

The HSM security requirements are based on existing standards like ISO, ANSI, Federal standards, and other good practices recognised by the financial industry. Some requirements of PCI HSM are similar to those in FIPS 140-2, see section 3.6.3.

3.5.3 PCI Payment Application Data Security Standard (PCI PA-DSS)

3.5.3.1 Focus

The PCI Payment Application Data Security Standard (PA-DSS) is developed specifically for software vendors that develop payment application. PA-DSS helps in securing cardholder data that is shared, stored, and processed by merchants and financial institutions and entities in payment applications. PA-DSS compliant applications help merchants and agents mitigate compromises, prevent storage of sensitive cardholder data and support overall compliance with the PCI DSS.

3.5.3.2 Associated Evaluation Scheme and Governance

The PCI Security Standards Council maintains, evolves, and promotes the Payment Card Industry Security Standards. PCI was found by five global payment brands (American Express, Discover Financial Services, JCB International, MasterCard, and Visa) along with Strategic Members that share equally in the Council's governance, have equal input into the PCI Security Standards Council, and share responsibility for carrying out the work of the organisation. Other Participating Organisations may include merchants, banks, processors, hardware and software developers, and point-of-sale vendors.

Payment Application Qualified Security Assessors (PA-QSAs) are parties selected by the PCI Council that are allowed to perform the PCI PA DSS assessment on payment applications. Find a list of all the PA-QSAs accredited by PCI:

https://www.pcisecuritystandards.org/assessors_and_solutions/payment_application_assessors

3.5.3.3 Process

Validation of payment applications occurs though an assessment by Payment Application Qualified Security Assessors based on the Payment Application Data Security Standard. Their evaluation of the application and their documentation of such compliance is provided in a corresponding Report on Validation.

Price and duration are not publicly disclosed.

3.5.3.4 Practice

Find a list of certified products below:
https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agree=true

Currently 551 products have been certified under PA DSS (3rd February 2017).

3.5.3.5 Formal Status

All aspects relating to compliance, enforcement, and adoption of these standards, including all issues relating to risk, are the responsibility of the individual payment card brands. For example, MasterCard mandates PA-DSS as per 1st of July 2012, however, Visa Europe 'only' strongly encourages payment application vendors to ensure their products undergo PA-DSS validation but do not mandate. However, the council urges merchants to use approved payment applications in their payment environment.

3.5.3.6 Relation to other standards / schemes

Using PA-DSS compliant payment applications is not required for PCI DSS compliance (see section 5.13.1). However, it greatly simplifies the PCI DSS compliance process. PA-DSS works hand-in-hand with PCI DSS and simplifies a PCI DSS assessment as the approved payment application does not need to be re-assessment during the PCI DSS assessment.

3.5.4 PCI PIN Transaction Security Point of Interaction Security (PCI PTS POI)

3.5.4.1 Focus

Throughout the processing of online and offline payment card transactions at Automated Teller Machines (ATMs) and Point of Sales (POS) terminals, the management, processing and transmission of personal identification number (PIN) data must meet certain security requirements as explicitly instructed by the PCI Council. This particular set of requirements is

relevant to acquiring institutions and agents that are in-charge of PIN transaction processing to have their ATM and POS products evaluated.

Card issuers rely on acquiring banks and processors to ensure cardholder PINs are handled securely during processing. As a consequence, all acquiring banks, their processing agents and any other third parties involved in the processing of PIN-based transactions and the associated cryptographic keys must participate in the program.

3.5.4.2 Associated Evaluation Scheme and Governance

Similar as described in section 3.5.3.2 for PCI PA DSS.

3.5.4.3 Process

A PIN entry device manufacturer may contact a PCI-recognised laboratory directly to obtain

- Guidance on designing POIs to PCI security requirements.
- Review of the vendor's POI design, answer questions via email or phone, participate in conference calls to clarify requirements and perform a preliminary physical security assessment on a vendor's hardware.
- Guidance on bringing a vendor's POI into compliance with the PCI requirements if areas of non-compliance are identified during the evaluation.
- Test fees
- Test dates

A list of PCI-recognised laboratories can be found at https://www.pcisecuritystandards.org/assessors_and_solutions/pci_recognized_laboratories. Currently eight labs are listed here.

Note that the payment schemes all have their own set of rules regarding the compliance certification process, enforcement, etc.

3.5.4.4 Practice

A list of PCI PTS (PIN Transaction Security) accepted devices can be found at https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices. Currently 821 devices are listed here.

3.5.4.5 Formal Status

All aspects relating to compliance, enforcement, and adoption of these standards, including all issues relating to risk, are the responsibility of the individual payment card brands. However, the processing of online and offline payment card transactions at ATMs and POS terminals, the management, processing and transmission of personal identification number (PIN) data must meet certain security requirements as explicitly instructed by the PCI Council.

3.5.4.6 Relation to other standards / schemes

The PCI TS POI standard refers to ISO and ANSI specifications in the requirements. For example, for key-management techniques PCI PTS POI requires conformance to ISO 11568 and ANSI X9.24. For PIN-encryption techniques ISO 9564 is referred.

3.6 Standards and schemes for cryptographic modules

3.6.1 ASD Cryptographic Evaluation

3.6.1.1 Focus

The Australian Signals Directorate (ASD) Cryptographic Evaluation is an unconstrained search and test for cryptographic vulnerabilities. The focus are ICT security products containing cryptographic functionality. The purpose of the evaluation is to achieve a higher level of confidence in the implementation and architecture of the cryptographic security.

Depending on the type and technology of ICT security product undergoing an ASD Cryptographic Evaluation, areas of testing may include packet sniffing, black box testing, source code review, key management analysis and Random Number Generation (RNG) evaluation.

3.6.1.2 Associated Evaluation Scheme and Governance

The certification scheme is called ASD Cryptographic Evaluation, the Australasian Certification Authority (ACA), oversees Australasian Information Security Evaluation Program (AISEP) product testing by licensed commercial evaluation facilities. The certification scheme owner is the Australian Signals Directorate. The ASD produces the Australian Government Information Security Manual (ISM). The manual is the standard which governs the security of government ICT systems.

3.6.1.3 Process

An Australian government agency must request and require that an ICT security product undergo an ASD Cryptographic Evaluation.

The ASD Cryptographic Evaluation process generally takes several months. The result of an ASD Cryptographic Evaluation is a published consumer guide on the Evaluated Product List (EPL).

3.6.1.4 Practice

Evaluated products can be found on the EPL: https://www.asd.gov.au/infosec/epl/index.php

3.6.1.5 Formal Status

An ASD Cryptographic Evaluation is legally required by the Australian and New Zealand governments for ICT security product containing cryptographic functionality that will be used to reduce the encryption requirements of information.

3.6.1.6 Relation to other standards / schemes

Only products that have successfully undergone a Common Criteria evaluation, or are in the process of being evaluated for CC in the Australasian Information Security Evaluation Program (AISEP) are eligible for an ASD Cryptographic Evaluation.

Similar cryptographic evaluations are conducted in other nations, such as the UK's CAPS scheme (see section 3.6.2) and the USA's and Canada's Cryptographic Module Validation Program (CMVP) (see section 3.6.3). The results and certification/validation of these cryptographic evaluations are not a replacement for an ASD Cryptographic Evaluation for Australian government agencies. However, providing all relevant documentation drawn up for such an evaluation may assist the ASD Cryptographic Evaluation process.

3.6.2 CESG Assisted Products Scheme (CAPS)

3.6.2.1 Focus

CAPS (CESG Assisted Products Service) is a certification scheme exclusive to the UK Government market. CAPS evaluations are an involved and technical process that is best defined as a partnership between the developer and NCSC. CAPS combines the cryptographic knowledge of the NCSC (formerly CESG) with the private sector's expertise and resources to accelerate the development of High Grade products.

Cryptographic products use encryption to provide security. Such products include disk encryptors, link and network encryptors, secure radios and access control devices. CAPS also evaluates products that control data flow between domains of differing classifications (cross-domain solutions). Her Majesty's Government (HMG) policy sets out approved standards to be employed where encryption is used to safeguard government classified data; CAPS verifies that products have met these standards.

3.6.2.2 Associated Evaluation Scheme and Governance

Similar governance as found in CPA under section 3.1.2.2.

3.6.2.3 Process

Developers or manufacturers may incorporate appropriate the NCSC's (formerly CESG) cryptographic or public domain algorithms in their products and submit them for evaluation by CAPS. Discussions between CAPS and the developer, a Consultancy and Advice contract gives companies access to the NCSC's knowledge, skills and experience in the field of Information Assurance, supplemented by a range of guidance documentation before products enter full

evaluation. Once approved, products are issued with a certificate and/or approval letter detailing the level of cryptographic protection they offer and are listed on this website.

Service pre-requisites

- HMG sponsor: The developer is normally required to be sponsored by a UK Government department to support their business case for the NCSC to evaluate the product.
- UK presence: Any developer wishing to have a product evaluated under CAPS must have an operational UK business presence.
- Site security: The company must also have been accredited under the UK Government's List X scheme.
- Personnel security: Stringent security procedures, possibly including the need for some staff to hold Developed Vetting (DV) clearance, are required.
- Access to source code: A CAPS evaluation depends on full and unfettered access to design documentation, source code, schematics, physical layout and other information normally treated as "company confidential". We require access to this material on our premises, without any restrictions on which evaluators may view it or when it may be viewed. It should be noted in particular that this requirement may also apply to third party intellectual property (IP) used in the product.

3.6.2.4 Practice

A list of certified products can be found here: https://www.ncsc.gov.uk/index/certified-product?f[0]=field_assurance_scheme%3A225&f[1]=field_assurance_status%3AAssured

To date (February 2017) 69 products have been evaluated.

3.6.2.5 Formal Status

Not known.

3.6.2.6 Relation to other standards / schemes

Not known.

3.6.3 FIPS 140-2

3.6.3.1 Focus

The FIPS140-2 standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against this standard. The adoption and use of this standard is available to private and commercial organisations.

The Cryptographic Module Validation Program (CMVP) is a joint American and Canadian security accreditation program for cryptographic modules. The program is available to any vendors that seeks to have their products certified for use by the U.S. Government and regulated industries (such as financial and health-care institutions) that collect, store, transfer, share and disseminate "sensitive, but not classified" information. Product certifications under the CMVP are performed in accordance with the requirements of FIPS 140-2. The CMVP was established by the U.S. National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada in July 1995. The Cryptographic Algorithm Validation Program (CAVP), which provides guidelines for validation testing for FIPS approved and NIST recommended cryptographic algorithms and components of algorithms, is a prerequisite for CMVP.

The Cryptographic Algorithm Validation Program (CAVP) provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components. Cryptographic algorithm validation is a prerequisite of cryptographic module validation (CMVP).

3.6.3.2 Associated Evaluation Scheme and Governance

The NIST's Computer Security Division (CSD) and Communications Security Establishment Canada (CSEC) jointly serve as the Validation Authorities (VAs) validating the test results and issuing certificates for both CMVP and CAVP.

All conformance testing against FIPS 140-2 is handled by third-party laboratories that are accredited as Cryptographic Module Testing Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP) or Cryptographic and Security Testing (CST) laboratories.

3.6.3.3 Process

CMVP cryptographic modules are tested independently by accredited Cryptographic and Security Testing (CST) laboratories or NVLAP-accredited laboratories. The cryptographic modules are tested against the Security Requirements for Cryptographic Modules found in FIPS 140-2. These security requirements cover 11 areas related to the design and implementation of a cryptographic module. For each area, the cryptographic module receives a security level rating (1-4, from lowest to highest) depending on what requirements are met. An overall rating is issued for the cryptographic module, which indicates (1) the minimum of the independent ratings received in the areas, and (2) fulfilment of all the requirements in the other areas. On the validation certificate the individual ratings and the overall rating is listed. It is important to realise that the overall rating of a cryptographic module is not necessarily the most important rating. In fact, the rating of an individual area may be more important than the overall rating, depending on the environment in which the cryptographic module will be implemented (this includes understanding what risks the cryptographic module is intended to address).

Price and duration are unknown.

3.6.3.4 Practice

Find below a list of validated cryptographic modules under CMVP:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2017.htm

Find an overview of validation lists under CAVP:
http://csrc.nist.gov/groups/STM/cavp/validation.html

3.6.3.5 Formal Status

FIPS 140-1 became a mandatory standard for the protection of sensitive data when the Secretary of Commerce signed the standard on January 11, 1994. FIPS 140-2 supersedes FIPS 140-1 and the standard was signed on May 25, 2001.

3.6.3.6 Relation to other standards / schemes

The operator of a cryptographic module is responsible for ensuring that the algorithms and key lengths are in compliance with the requirements of NIST SP 800-131A.

3.6.4 ISO/IEC 19790 (Security requirements for cryptographic modules)

3.6.4.1 Focus

ISO/IEC 19790 defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million-dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location).

This International Standard specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level. The following requirement areas have been defined:

- Cryptographic Module Specification
- Cryptographic Module Interfaces
- Roles, Services, and Authentication
- Software / Firmware Security
- Operational Environment
- Physical Security
- Non-Invasive Security
- Sensitive Security Parameter Management
- Self-Tests
- Life-Cycle Assurance
- Mitigation of Other Attacks

These eleven security requirements are divided into a set of assertions (i.e., statements that have to be true for the module to satisfy the requirement of a given area at a given level). Each assertion has a set of requirements set to the vendor. These requirements describe the type of documentation or explicit information that the vendor shall provide in order for the tester to verify the conformity to the given assertion.

The standard specifies four security levels, where each level adds requirements to the previous one. Security level 2 is the highest security level attainable by a pure software module.

3.6.4.2 Associated Evaluation Scheme and Governance

There is no official evaluation scheme for ISO/IEC 19790. However,

- In Japan, IPA operates a cryptographic module validation program known as the JCMVP, with ISO/IEC 19790 as a basis.
- In South Korea, the Korean Cryptographic Module Validation Program (KCMVP) was established in 2005 and uses ISO/IEC 19790 as a basis for their program specifying the Korean approved set of cryptographic algorithms and security functions.
- A validation program in Spain for cryptographic modules is based on the ISO standards
- A validation program in Turkey for cryptographic modules is based on the ISO standards
- Other national programs are under consideration

3.6.4.3 Process

The evaluation process is defined by the respective national evaluation scheme.

3.6.4.4 Practice

Not known.

3.6.4.5 Formal Status

None.

3.6.4.6 Relation to other standards / schemes

ISO/IEC 19790 is related to FIPS 140-2 (see section 3.6.3). In fact, the first edition of this standard was technically almost identical. However, a second revision of ISO/IEC 19790 was published in August of 2012 to cope with evolving technologies and input from the many experts and nations represented in ISO.

Further related standards are:

- ISO/IEC CD 19896-2 (Competence requirements for information security testers and evaluators -- Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers)
- ISO/IEC 20543 Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
- ISO/IEC 18367 Cryptographic algorithms and security mechanisms conformance testing,
- ISO/IEC 17825 Non-invasive attack mitigation test metrics for cryptographic modules

3.7 Standards and schemes for web applications

3.7.1 OWASP Application Security Verification Standard (incl. OWASP Top 10)

3.7.1.1 Focus

The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls. Controls may be present both in the application itself and in the environment in which the application is used. Applications may rely on these controls to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. The ASVS project is a superset of the more commonly known OWASP Top 10.

The ASVS also provides developers with a list of requirements for secure development.

The ASVS defines three security verification levels, each consisting of a list of security requirements. These requirements can be mapped to security-specific features that can be implemented by developers. Based on how critical the application is and the sensitivity of the data it is processing, additional or more in-depth requirements must be met:

- ASVS Level 1 is meant for all software.
- ASVS Level 2 is for applications that contain sensitive data, which requires protection.
- ASVS Level 3 is for the most critical applications.

3.7.1.2 Associated Evaluation Scheme and Governance

The OWASP Application Security Verification Standard is maintained by the Open Web Application Security Project (OWASP), a not-for-profit organisation focused on improving the security of software by empowering both organisations and individuals to make informed decisions regarding security. All material released by OWASP is available under a free and open software license, including the OWASP Application Security Verification Standard.

There is no official associated evaluation scheme for testing and certifying compliance of web applications to the ASVS. In fact, to ensure vendor-neutrality, OWASP does not endorse or recommend any commercial products or services. This should not inhibit organisations from offering such assurance services, as long as they do not claim official OWASP certification.

3.7.1.3 Process

The ASVS requirements were developed with the following objectives in mind:

- **Use as a metric** - Provide application developers and application owners with a yardstick with which to assess the degree of trust that can be placed in their web applications.
- **Use as guidance** - Provide guidance to security control developers as to what to build into security controls in order to satisfy application security requirements. Organisations may use the ASVS as a blueprint to create a Secure Coding Checklist specific to an application, platform or organisation.

- **Use during procurement** - Provide a basis for specifying application security verification requirements in contracts.

The manner in which the ASVS is used varies per organisation. The standard itself provides two case studies which demonstrate example usages.

3.7.1.4 Practice

A broad range of companies and agencies around the globe have added ASVS to their software assurance tool boxes, as listed here: https://www.owasp.org/index.php/Category%3AOWASP_Application_Security_Verification_Standard_Project#tab=ASVS_Users

3.7.1.5 Formal Status

None

3.7.1.6 Relation to other standards / schemes

The OWASP Top 10 2010 is a subset of the ASVS 3.0. This means that ASVS contains 144 additional items compared to the OWASP Top 10.

The ASVS also includes a reference mapping between the ASVS v3.0 and section 6.5 of the PCI DSS v3.0 standard (see section 5.13.1). This section of PCI DSS in turn was derived from the OWASP Top 10 2004/2007.

A mobile application version of the ASVS, called MASVS, is currently in development and can be found at https://github.com/OWASP/owasp-masvs.

3.7.2 OWASP Testing Guide

3.7.2.1 Focus

The aim of the OWASP Testing Guide is to help testers and organisations understand the what, why, when, where, and how of testing web applications. This project has been in development for more than ten years by community participation and industry feedback. It is a complete testing framework, not merely a simple checklist or prescription of issues that should be addressed.

The Testing Guide describes in detail both the general testing framework and the techniques required to implement the framework in practice.

3.7.2.2 Associated Evaluation Scheme and Governance

The OWASP Testing Project is maintained by the Open Web Application Security Project (OWASP), a not-for-profit organisation focused on improving the security of software by empowering both organisations and individuals to make informed decisions regarding security. All material released by OWASP is available under a free and open software license, including the OWASP Testing Project.

To ensure vendor-neutrality, OWASP does not endorse or recommend any commercial products or services. This should not inhibit organisations from offering such assurance services, as long as they do not claim official OWASP certification.

3.7.2.3 Process

The OWASP Testing Guide includes a section describing a typical testing framework that can be developed within an organisation. It can be seen as a reference framework that comprises techniques and tasks that are appropriate at various phases of the software development life cycle (SDLC).

As the guide points out, security testing will never be an exact science where a complete list of all possible issues that should be tested can be defined. Indeed, security testing is only an appropriate technique for testing the security of web applications under certain circumstances. The goal of the OWASP Testing Project is to collect all the possible testing techniques, explain these techniques, and keep the guide updated. The method is based on the black box approach where the tester knows nothing or has very little information about the application to be tested.

3.7.2.4 Practice

Not applicable.

3.7.2.5 Formal Status

None

3.7.2.6 Relation to other standards / schemes

No formal relation between the OWASP Testing Project and other standards and schemes has been defined. In particular, there is no direct link between OWASP ASVS (see section 3.7.1) and the OWASP Testing Guide. However, in practice the Testing Guide describes many methods on how to test for each the categories of vulnerabilities described in the OWASP ASVS.

3.8 Standards and schemes for IoT products

3.8.1 ICSA Labs IoT Security Testing Framework

3.8.1.1 Focus

The term “Internet of Things” or IoT is a very broad term referring to many kinds and types of devices and sensors that heretofore had not been network-connected. Therefore, the ICSA Labs Internet of Things (IoT) Security Testing Framework is not a stand-alone set of criteria for any particular type of device or sensor. Instead, it is focused on specifying security testing requirements for distinct classes of IoT device types. The intent of the document is to be a starting point for developing a more specific set of testable, security-related requirements for a unique class of IoT devices and their component parts.

Testing requirements in the Framework are based on six categories: alerting/logging, authentication, communications, cryptography, physical security, and platform security.

3.8.1.2 Associated Evaluation Scheme and Governance

ICSA Labs is an ISO-accredited, independent, third-party testing lab with 25 years of computer and network security testing experience.

3.8.1.3 Process

ICSA Labs works with prospective IoT testing customers by first building a unique set of requirements from the framework prior to testing the customer's IoT device or sensor and its component parts. Once the criteria requirements are set, ICSA Labs performs recurring security testing. IoT devices and sensors that meet the security requirements following successful testing of the device and its component parts are awarded ICSA Labs IoT Certification.

3.8.1.4 Practice

As of April 2017, one product was listed by ICSA Labs as being certified against the ICSA Labs Internet of Things (IoT) Security Testing Framework.

3.8.1.5 Formal Status

None.

3.8.1.6 Relation to other standards / schemes

When creating the Framework, ICSA Labs compared the categories and resulting requirements to other emerging guidelines, including the OWASP Internet of Things Top 10 (see section 5.14.7), the Industrial Internet Consortium Reference Architecture (see section 5.14.4), and the Online Trust Alliance's IoT Trust Framework (see section 5.14.6).

3.9 Standards and schemes for other IT products

3.9.1 MIFARE Security Certification

3.9.1.1 Focus

The MIFARE Security Certification focusses on the implementation of security features in MIFARE Plus and MIFARE DESFire products. Correct implementation of these features is crucial to providing a secure environment for system providers and end users.

requirements for a MIFARE product to get the MIFARE Security Certification are not fixed. Penetration tests are performed on the product, but what tests are performed differs between products. The closest to a list of requirements is the description of the Vulnerability Assessment of Common Criteria level 5, which essentially requires the evaluator to perform a methodical

vulnerability analysis and to perform penetrating testing. This is because the MIFARE Security Certification is developed based upon the Common Criteria (CC).

3.9.1.2 Associated Evaluation Scheme and Governance

Certification of a MIFARE Plus or MIFARE DESFire product may be achieved in one of two ways:

- in the form of a Common Criteria evaluation (see section 3.1.3) against the Protection Profile BSI-CC-PP-0084-2014.
- via MIFARE Security Certification offered by NXP

The MIFARE Security Certification has an elaborate governance. External laboratories do the testing. In this scheme there are two different laboratories: a certification lab and an evaluation lab. The evaluation lab conducts the action vulnerability analysis, whilst the certification lab checks whether the evaluation lab's work is in line with the standard, whilst NXP acts as an administrator and observer of the process.

3.9.1.3 Process

1. Manufacturer (= MIFARE licensee) submits forms to NXP.
2. NXP approves request and provides list of accredited evaluation labs.
3. Manufacturer chooses an accredited evaluation lab and provides product and documentation.
4. Evaluation lab prepares test plan and submits it to accredited certification lab.
5. Certification lab approves test plan.
6. Evaluation lab evaluates the product and delivers 'Test Report Lite' to certification lab.
7. Certification lab examines report; if OK, issues Approval Letter and notifies NXP.

An evaluation takes around 16 weeks in total.

3.9.1.4 Practice

A list of the issued security certificates can be found on: https://www.mifare.net/en/about-mifare/certification/security-certificates/

3.9.1.5 Formal Status

NXP requires a MIFARE Security Evaluation (or equivalent CC certification at EAL4+) from licensees for all MIFARE Plus and MIFARE DESFire products, including firmware implementations, emulations, native ASICs, applets etc.

3.9.1.6 Relation to other standards / schemes

Hardware, cryptographic libraries and Java Card Open Platforms must have a valid Common Criteria certificate against an EAL4+ Protection Profile (see section 3.1.3) or a valid EMVCo IC and Platform Certificate (see section 3.5.1) before final approval can be issued.

The MIFARE security evaluation is basically a subset of the Common Criteria, where it focusses on class 7, the Assurance Vulnerability Assessment. This because the other classes, focusing on

areas such as governance and management, are not necessary for the correct functioning of MIFARE products.

The MIFARE Security Certification scheme requires the same level of security vulnerability analysis and testing as the Common Criteria scheme for smart cards, as it is based on the same JHAS testing requirements. For more information, see Appendix 1.

3.9.2 ISO/IEC 19792 (Security evaluation of biometrics)

3.9.2.1 Focus

ISO/IEC 19792 specifies the subjects to be addressed during a security evaluation of a biometric system. It covers the biometric-specific aspects and principles to be considered during the security evaluation of such a system, but does not address the non-biometric aspects which might form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels).

ISO/IEC 19792 does not aim to define any concrete methodology for the security evaluation of biometric systems but instead focuses on the principal requirements. As such, the requirements in ISO/IEC 19792 are independent of any evaluation or certification scheme and will need to be incorporated into and adapted before being used in the context of a concrete scheme.

3.9.2.2 Associated Evaluation Scheme and Governance

None. ISO/IEC 19792 is independent of any specific evaluation scheme. This standard could serve as a framework for the development of concrete evaluation and testing methodologies to integrate the requirements for biometric evaluations into existing evaluation and certification schemes. However, no information could be found on any scheme that actually uses ISO/IEC 19792.

3.9.2.3 Process

None.

3.9.2.4 Practice

Not known.

3.9.2.5 Formal Status

None.

3.9.2.6 Relation to other standards / schemes

None.

4 Cybersecurity standards and schemes for ICT services

4.1 ANSSI SecNumCloud

4.1.1 Focus

The Référentiel Général de Sécurité (RGS) scheme (see section 5.10.4) defines a set of security rules that are imposed on French administrative authorities to ensure the security of their information systems. It also proposes good practices in the security of information systems that the administrative authorities are free to apply.

The RGS allows the qualification of new types of providers. The SecNumCloud framework covers the provision of secure cloud services and aims to qualify RGS providers offering a service in the cloud. The qualification framework for cloud service providers covers three types of activity: Software as a Service (SaaS), (PaaS) and Infrastructure as a Service (IaaS). The requirements pertain to access control and identity management, cryptography, operational security and information security incident management.

The SecNumCloud Requirements are divided into two different levels: Essential and Advanced. Currently, only the Essential requirements have been published.

4.1.2 Associated Evaluation Scheme and Governance

See section 5.10.4.2.

4.1.3 Process

The requirements will be verified by a documentary, organisational, physical and technical evaluation of the processes, infrastructures and locations targeted by the qualification.

4.1.4 Practice

At the moment, no service providers have been qualified yet. Three service providers are in the process of being qualified.

4.1.5 Formal Status

Not known.

4.1.6 Relation to other standards / schemes

This scheme is an extension of the Référentiel Général de Sécurité (RGS) scheme; see section 5.10.4.

4.2 Cloud Computing Compliance Controls Catalogue (C5)

4.2.1 Focus

The C5 is a German Government-backed attestation scheme introduced in Germany by the Federal Office for Information Security (BSI) to help organisations demonstrate operational security against common cyber-attacks. The C5 fits within the context of the "Security Recommendations for Cloud Providers", an assessment made by BSI defining a set of minimum requirements of security for Cloud Service Providers (CSP).

The C5 is intended primarily for professional cloud service providers, their auditors and customers of the cloud service providers. It defines which requirements (also referred to as controls) the cloud providers have to comply with or which minimum requirements the cloud providers should be obliged to meet.

Compared to other security standards, the so-called surrounding parameters for transparency are a novelty. They provide information on the data location, provision of services, place of jurisdiction, certifications and duties of investigation and disclosure towards government agencies and contain a system description. The resulting transparency makes it possible for potential cloud customers to decide whether legal regulations (such as data protection), the customers' own policies or also the threat scenario regarding economic espionage make the usage of the respective cloud service seem appropriate.

The C5 is subdivided into 17 sections (e.g. 'security policies and work instructions', 'cryptography and key management', and 'mobile device management') and an objective is assigned to each section (e.g. for 'mobile device management' this is 'Guaranteeing security when using mobile terminal devices in the cloud provider's area of responsibility for the access to IT systems in order to develop and operate the cloud service'). The objective provides the cloud provider a summarised target which they have to fulfil in the related section through corresponding organisational and operational measures and (procedural) organisation. Individual requirements are assigned to each objective which specify general principles, procedures and measures for fulfilling the objective.

The requirements were, wherever possible, taken from known security standards (see section 4.2.6). They were supplemented by the BSI's own requirements only to the extent needed.

4.2.2 Associated Evaluation Scheme and Governance

The C5 is not a certification which is issued by the BSI or any other certification body, instead, third party auditors may audit a CSP and verify whether it complies with the C5 requirements. The validity of such an attestation is dependent on the quality of the auditor, and the C5 therefore provides the requirements of such an auditor.

4.2.3 Process

There are two different types of audits which can be performed. With the first type the auditor focusses upon whether the design of the CSP's cyber security system follows the C5 requirements. With the second type the auditor will perform, additionally to the first type, functional tests on the effectiveness of these systems.

For a BSI-conform attestation of a cloud service, the report must include the following information:

- Detailed system description of the cloud service
- Qualification of the auditor
- Any identified deviations from the requirements
- Information on the limitation of liability

The CSP and the auditor make an agreement on how long the audit is valid, although the BSI usually recommends an audit period of twelve months.

4.2.4 Practice

In December 2016 Amazon Web Services was the first C5-certified Cloud Service Provider. No other certified CSPs have been found.

4.2.5 Formal Status

The C5 scheme is not mandatory. It is up to a CSP to be audited or not.

4.2.6 Relation to other standards / schemes

The requirements in the C5 are referenced to other standards, which provides a quick overview of where the requirements of the catalogue can be found in other standards and whether the requirements go beyond the standards or not. This reference document can be found at the website of the BSI: https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/FAQ/FAQ_relations_node.html

4.3 Cloud Security Alliance Cloud Controls Matrix

4.3.1 Focus

The Cloud Controls Matrix (CCM) is a list of requirements for security assurance in the cloud, developed by the Cloud Security Alliance (CSA). The CSA is a member-driven organisation, chartered with promoting the use of best practices for providing security assurance within Cloud Computing, and providing education on the uses of Cloud Computing.

The CCM is the CSA's royalty-free cloud security control objectives catalogue, designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security stance of a cloud provider. It covers fundamental security principles across 16 domains (e.g. Datacentre Security Asset Management, Mobile Security and Anti Malware, and Security Incident Management, E-discovery & Cloud forensics, and Incident Reporting) to help cloud customers assess the overall security risk of a Cloud Service Providers (CSP).

4.3.2 Associated Evaluation Scheme and Governance

The STAR program is intended to be a trust mark for cloud security and offers a flexible, incremental and multi-layered certification scheme to cloud service providers. The program offers three different levels of meeting security assurance requirements as listed in the CCM. The first level is a 'self-assessment' for organisations with a low/moderate risk profile. The second and third levels are intended for organisations with increased risk profiles, through 3rd party assessment-based certification and continuous monitoring based certification respectively.

4.3.3 Process

As stated above, a STAR audit can be performed at different levels, depending on the requirements of the CSP:

- Level 1 (self-assessment): Cloud providers either submit a completed Consensus Assessments Initiative Questionnaire (CAIQ), a set of more than 140 questions based on the CCM, or a report documenting compliance with Cloud Controls Matrix (CCM).
- Level 2 (attestation): A report is made by a third party on whether or not the CSP is compliant with the CCM. STAR attestation is based on type-2 SOC (see section 5.1.18) attestations supplemented by the criteria in the CCM.
  See also https://cloudsecurityalliance.org/star/attestation/.
- Level 2 (certification): A CSP is certified after a rigorous third-party assessment on the CSP's compliance with the ISO/IEC 27001 information management system standard (see section 5.1.8) together with the CSA Cloud Controls Matrix.
  See also https://cloudsecurityalliance.org/star/certification/.
- Level 3 (continuous monitoring): High-risk cloud stakeholders require certifications schemes that provide high assurance and high transparency. The STARWatch software is a Software as a Service (SaaS) application to help organisations manage compliance with CSA STAR requirements. STARWatch delivers the content of the Cloud Controls Matrix (CCM) and

Consensus Assessments Initiative Questionnaire (CAIQ) in a database format, enabling users to manage compliance of cloud services with CSA practices.

Note: the difference between a (Level-2) attestation and a certification is that the certificate is valid for 3 years, whereas the attestation merely serves as a snapshot in time whether the CSP is compliant with the CSM at that point.

4.3.4 Practice

The full list of STAR-registered companies can be found at:
https://cloudsecurityalliance.org/star/#_registry

4.3.5 Formal Status

The CSA CCM scheme is not mandatory. It is up to a CSP to be audited or not.

4.3.6 Relation to other standards / schemes

As stated above, a STAR attestation proves compliance with SOC type-2, see section 5.1.18. A STAR certification also proves compliance with ISO/IEC 27001 (see section 5.1.8).

ENISA listed several levels of the CSA CCM scheme on its Cloud Certification Schemes List (CCSL) – see https://resilience.enisa.europa.eu/cloud-computing-certification.

4.4 Code of Practice for Cloud Service Providers

4.4.1 Focus

This Code of Practice for Cloud Service Providers from the Cloud Industry Forum ('CIF') is for organisations offering to customers remotely hosted IT services of any type. These services include, but are not limited to, multi-tenanted services accessed via the Internet.

The Code of Practice for Cloud Service Providers focusses on Transparency, Capability and Accountability:

- Transparency: Organisations must show the ability to perform essential management functions, as demonstrated by having in place auditable documented management systems.
- Capability: Organisations must ensure a reasonable and consistent level of transparency about businesses and their operational practices throughout the Cloud Industry
- Accountability: Organisations which assert that they are complying with the Code shall be accountable for their compliance with the Code and for their behavior with customers.

Thus, the focus is more on good management practices, which indirectly should improve the cybersecurity stance of Cloud Service Providers, than on assessing cybersecurity directly. More

details can be found on the website of the Cloud Industry Forum: https://www.cloudindustryforum.org/content/cop-detailed-overview.

4.4.2 Associated Evaluation Scheme and Governance

When an organisation follows the Code of Practice, it can acquire the labels CIF Certified or CIF Certified+.

CIF is a membership-based not-for-profit organisation answerable to its members. It has two separate governance streams: one for business activity (the Management Board responsible for administration, development, finance and similar) and one for governance of the CIF Code of Practice scheme (the Code Governance Board). This sheet is primarily concerned with governance issues related to the Code of Practice

4.4.3 Process

The Certification can be acquired through two different processes:

- Self-Certification (CIF Certified)
  - The CIF will spot check and randomly audit Self-Certifications as well as investigate any formal complaint of non-compliance against an organisation claiming compliance with the Code.
- Independent Certification (CIF Certified+)
  - An organisation may opt for Independent Certification performed by a Certification body approved by the CIF.

The certification is valid for one year

4.4.4 Practice

See https://selfcert.cloudindustryforum.org/certification/.

4.4.5 Formal Status

The CIF Certified or CIF Certified+ Certification is not mandatory. It is up to a CSP to be audited or not.

ENISA listed the Code of Practice of Cloud Infrastructure Providers on its Cloud Certification Schemes List (CCSL) – see https://resilience.enisa.europa.eu/cloud-computing-certification.

4.4.6 Relation to other standards / schemes

Not known.

4.5 EuroCloud StarAudit Certification

4.5.1 Focus

The EuroCloud StarAudit (ECSA) program is a certification scheme to establish trust in cloud services both on the customer and the user side. The purpose of the StarAudit scheme is to provide accountable quality assessment of cloud services through a transparent and reliable certification process. If a Cloud Service Providers (CSP) matches the StarAudit requirements, the StarAudit certificate is granted. These requirements are in different categories: Facilities (hardware, cooling, etc.), Platform as a Service (PaaS), Infrastructure as a Service, Software as a Service (SaaS), and Organisation (processes, policies)

4.5.2 Associated Evaluation Scheme and Governance

EuroCloud Europe is a non-profit organisation, as is the ECSA program. This program is not funded by any industry sponsor nor does it receive any financial means from other organisations or government bodies.

A CSP can be rated at different levels, with every level adding more requirements to the audit: a CSP can be considered to be a 3, 4 or 5-star Trusted Cloud Service. This allows for a small CSP not having to meet the same level of requirements as a large CSP.

4.5.3 Process

There are four different steps in this scheme. It is not necessary to complete all the steps, dependent on the wishes of the CSP a self-assessment may be sufficient:

1. The first step is a self-assessment by the CSP at the level of requirements the CSP wants to commit to. After the CSP has shown that it is compliant with the requirements at the desired level, the CSP is considered a Trusted Cloud Service Provider.
2. The next step is for the CSP to register with the self-assessment as a StarAudit partner. As a partner, the CSP will be actively made visible by StarAudit (e.g. on their website, see the practice section)
3. The third step is to become certified after being audited by a StarAudit-AAO (Accredited Audit Organisation).
4. Finally, by following the guidelines and recommendations of StarAudit, the CSP will remain compliant with StarAudit's requirements.

As long as no changes are made to the cloud service profile and assessment areas, the certificate is valid for three years. An annual check-up is obligatory.

4.5.4 Practice

All CSPs with a valid StarAudit Certificate, a published Self-Assessment report or an approved datacentre can be found here: https://staraudit.org/all-certificates.html

4.5.5 Formal Status

The EuroCloud StarAudit Certification scheme is not mandatory. It is up to a CSP to be audited or not.

4.5.6 Relation to other standards / schemes

The requirements of this scheme make use of ISO 27001 (see section 5.1.8) and ISO 27018 (see section 4.7). However, since these standards are only used as input for the StarAudit, compliance with StarAudit does not imply full compliance with the ISO standards.

ENISA listed the EuroCloud StarAudit Certification scheme on its Cloud Certification Schemes List (CCSL) – see https://resilience.enisa.europa.eu/cloud-computing-certification.

4.6 ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services)

4.6.1 Focus

ISO 27017 generally focuses on the protection of the information in cloud services. This standard is built upon the existing security controls of ISO 27002. Specific guidance is provided for 37 of the existing ISO/IEC 27002 controls; separate but complementary guidance is given for the cloud service customer and the cloud service provider.

Moreover, ISO 27017 suggests seven additional security controls for the cloud, where ISO 27002 does not adequately cover this area. These controls address the following aspects:

- Shared roles and responsibilities within a cloud computing environment
- Removal and return of cloud service customer assets when a contract is terminated
- Segregation in virtual computing environments
- Virtual machine hardening
- Administrator's operational security associated with the cloud environment
- Monitoring of Cloud Services
- Alignment of security management for virtual and physical networks

4.6.2 Associated Evaluation Scheme and Governance

See section 5.1.8.2 on the governance of ISO 27001.

A number of ISO 27001 certification bodies offer certification against ISO 27017. Such a certification means that the ISMS in question obtained ISO 27001 certification and additionally

complies with the guidance for the existing security controls and with the new controls in ISO 27017.

4.6.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

4.6.4 Practice

The number of parties that have obtained certification seems to be limited still, perhaps because ISO 27017 was introduced only recently (2015). As the ISO survey (see section 5.1.8.4) does not give information on ISO 27017 separately, it is hard to get an overview. However, some big names are already certified, including Microsoft Azure, Amazon Web Services, Dropbox and Google Cloud Platform.

Certification for ISO 27001 is increasingly popular. As ISO 27017 is effectively an add-on for ISO 27001, and given the need for demonstrable security for cloud services, it seems likely that the number of ISO 27017 certificates will increase as well.

4.6.5 Formal Status

None.

4.6.6 Relation to other standards / schemes

Certification against ISO 27001 is a prerequisite for obtaining certification against ISO 27017.

4.7 ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)

4.7.1 Focus

ISO/IEC 27018, which was published in 2014, establishes controls and guidelines for measures to protect Personally Identifiable Information for the public cloud computing environment. The guidelines are based on those specified in ISO/IEC 27002 with controls objectives extended to include the requirements needed to satisfy privacy principles in ISO/IEC 29100.

ISO 27018 provides specific guidance is provided for 14 of the existing ISO/IEC 27002 controls and lists 24 new controls.

Whereas ISO 27017 is concerned with the general security of cloud services, ISO 27018 deals specifically with how PII is handled in the cloud.

4.7.2 Associated Evaluation Scheme and Governance

See section 5.1.8.2 on the governance of ISO 27001.

A number of ISO 27001 certification bodies offer certification against ISO 27018. Such a certification means that the ISMS in question obtained ISO 27001 certification and additionally complies with the guidance for the existing security controls and with the new controls in ISO 27018.

4.7.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

4.7.4 Practice

See for ISO 27017, section 4.6.4. Big companies that are certified against ISO 27018 include Amazon Web Services, a number of Microsoft services and Dropbox. The number of lesser-known companies advertising compliance on their websites seems to be larger than for ISO 27017, perhaps due the fact that the latter was published later.

4.7.5 Formal Status

None.

4.7.6 Relation to other standards / schemes

Certification against ISO 27001 is a prerequisite for obtaining certification against ISO 27018.

4.8 TüV Rheinland Cloud Security Certification

4.8.1 Focus

TüV Rheinland has developed an extensive catalogue of requirements and criteria for cloud services, which is based on standards, studies and on selected regulations and recommendations.

The focus of this catalogue includes, but is not limited to: hypervisor, virtualisation of data centers, systems, access concepts, networks, system interfaces, administrative processes, services, processes and compliance.

4.8.2 Associated Evaluation Scheme and Governance

The catalogue of requirements is the basis for the Cloud Security Certification. The audit checks how far the requirements have been implemented and check the quality and sustainability of processes.

The certification is custom fitted to the organisation, such that organisations with different standards can get the TUV Certification: a low-risk organisation does not have to have the same requirements as a high-risk organisation. TUV assesses this on a case-by-case basis.

4.8.3 Process

The auditing procedure for Cloud Service certification combines a variety of methods:

- Interviews during which auditors check how far the requirements have been implemented and check the quality and sustainability of processes.
- In contracts and SLAs the adherence to performance pledges is checked.
- The cloud service architecture is subjected to a stress test.
- Penetration tests are used to identify possible safety gaps.

Once acquired, cloud certification is valid for three year and can subsequently be renewed.

4.8.4 Practice

An analysis of the search request ‘cloud’ on www.certipedia.com indicates that there are 13 certified organisations, which include companies like Box, Deutsche Telekom and Vodafone.

4.8.5 Formal Status

The Cloud Service Certification scheme is not mandatory. It is up to a CSP to be audited or not.

ENISA listed the Cloud Security Certification scheme of TUV Rheinland on its Cloud Certification Schemes List (CCSL) – see https://resilience.enisa.europa.eu/cloud-computing-certification.

4.8.6 Relation to other standards / schemes

Not known.

5 Cybersecurity standards and schemes for service providers and organisations

5.1 Standards and schemes for generic organisations

5.1.1 AEI Seal of Cybersecurity for Organisations

5.1.1.1 Focus

The Seal of Cybersecurity certification is a certification scheme developed by the 'Spanish Cybersecurity Innovation Cluster' (AEI Ciberseguridad). It includes the technical and management security requirements that any organisation should comply with to demonstrate it has implemented in a secure way physical and logical systems and measures to protect their assets against cyber threats.

The AEI Seal of Cybersecurity distinguishes three different types of organisations (A, B and C) that can be certified, depending on the access level to the information systems of other organisations through their products or services. This ranges from software developers to general cleaning services, lawyers or system integrators. The Seal has a special category for Critical Infrastructure operators, for which several specific technical and management requirements are applicable.

The standard includes technical and management requirements in the following categories:

- Communication protocols: configurations and implementations
- Software development: web and desktop, distributed applications, etc.
- Data Protection: national regulations and European General Data Protection Regulation
- Infrastructure: both physical and logical
- Human Resources: experience and training
- Suppliers: SLAs, Cybersecurity awareness, etc.
- Services: digital signature, cryptography, key storage, etc.

The requirements are listed in the Seal of Cybersecurity Industry Standard. This document is available upon request to any interested organisation via AEI or any of the accredited consultant organisations (see below).

5.1.1.2 Associated Evaluation Scheme and Governance

The Seal of Cybersecurity is a third-party certification scheme.

It is owned by the Spanish Cluster of Cybersecurity (AEI Ciberseguridad Association), who is acting as the Accreditation Body and Certification Authority, guaranteeing the quality of the scheme and the different associated services. AEI Ciberseguridad is a national non-profit

Cybersecurity and advanced technologies association with more than 80 private and public members.

5.1.1.3 Process

Any organisation can freely implement the requirements of the certification scheme and ask for certification.

All information regarding the certification process is public available on the Association's website: https://www.aeiciberseguridad.es/index.php/Sello_AEI. This website also contains a list of (four) approved consultants delivering implementation services for the Seal of Cybersecurity, as well as a list of accredited audit/evaluation entities, for which currently (Feb 2017) only one organisation is listed.

The website also offers information on the expected number of working days an audit will take. Depending on the size and complexity of the organisation and its products/services, this may range from a couple of days to a few weeks. Estimates for maintenance evaluations and renewal evaluations are included as well.

5.1.1.4 Practice

AEI Ciberseguridad has grown from 40 members to +80 during the past 2 years.

The Seal of Cybersecurity was launched in June 2016. Since then, around 60 organisations – public or private- were certified or are in the process of being certified. This includes companies from Spain, Italy, Switzerland and France. The Seal has been implemented and certified in several sectors: financial, cloud providers, consultant companies, public sector contractors, datacentres, etc.

5.1.1.5 Formal Status

Currently there is no official mandate from the (Spanish) government that operators of critical infrastructure or other organisations must obtain the Cybersecurity Seal. However, some operators and companies are requesting the Seal to suppliers when issuing tenders.

5.1.1.6 Relation to other standards / schemes

No official relation.

5.1.2 CIS Critical Security Controls / SANS Critical Security Controls

5.1.2.1 Focus

The Center for Internet Security (CIS) is a US-based non-profit organisation, which maintains the CIS Critical Security Controls. This is a list of 20 security controls that an organisation could implement to thwart the most pervasive cybersecurity attacks. The list is the result of the consensus of a large number of cybersecurity experts, primarily from the US and Australia.

The list is prioritised, starting with the controls that an organisation should implement first. Every control consists of a number of ‘sub-controls’, which are concrete actions an organisations can take. These actions are marked as ‘foundational’ or ‘advanced’. The reasons for each control are explained, and procedures and tools that can help implementing the control are described.

5.1.2.2 Associated Evaluation Scheme and Governance.

There is no official evaluation scheme for the CIS Controls.

The CIS regularly publishes new versions of the list. A new version may add new controls (and deletes others to keep the total number at 20. Also, the priority of controls may change. These changes are made in response to observations made regarding new types of attack and defense methods and the actual effectiveness of a specific control.

The SANS Institute offers a number of trainings on implementing the CIS Controls; see www.sans.org/find-training. SANS is also hosting a series of events ("summits") that will bring the community together to share ideas and learn from each other. The CIS Controls are also part of the US National Cyber Hygiene Campaign, a multi-year effort that provides key recommendations for a low-cost program that any organisation can adopt to achieve immediate and effective defenses against cyberattacks.

5.1.2.3 Process

There is no official evaluation process for the CIS Controls.

To aid organisations in implementing the CIS Controls, the CIS maintains mappings, use cases, measurement tools and other documentation on its website. These include:

- CIS Controls Measurement Companion
- CIS Controls IoT Security Companion
- CIS Controls Mobile Security Companion
- CIS Controls Towards a Privacy Impact Assessment Companion[4]
- CIS Security Benchmarks,
- CIS Consensus Security Measures.

5.1.2.4 Practice

- The U.S. Department of State determined that among the 3,085 cyberattacks it had experienced over fiscal year 2009, the CIS Controls showed remarkable alignment with actual attacks.
- Subsequent implementation of the CIS Controls by every system administrator across 24 time zones in which the Department operates, achieved an 88% reduction in vulnerability-based risks across 85,000 systems.

[4] This document seems to be identical to Appendix F of v6.0 of the Security Controls themselves.

- In December of 2011, the Centre for the Protection of National Infrastructure (CPNI) announced that the government of the United Kingdom would be adopting the CIS Critical Security Controls as the framework for securing their critical infrastructure.
- In May of 2012, the NSA Director fully endorsed the adoption of the CIS Controls as a foundation for effective network security.
- The Australian Department of Defense tested the Top 4 Controls against 1700 types known malware and found that implementation of just the Top 4 Controls effectively stopped every one of the 1700 types of malware tested.
- Consumer Energy, a Fortune 500 combined Gas and Electric Utility, officially adopted the CIS Controls in June 2011. Consumer Energy started by using the CIS Controls as an assessment tool with a small team of cybersecurity and IT staff, conducting an internal assessment covering the corporate IT environment in less than a week.

5.1.2.5 Formal Status

None.

5.1.2.6 Relation to other standards / schemes

The GIAC Critical Controls Certification (GCCC) (see section 6.4) is a certification for security professional based on the Critical Security Controls.

Mappings of the CIS Controls to controls listed in other standards are available at the CIS and SANS websites.

The CIS Controls, plus the Companion documents listed above, have been standardised by ETSI as ETSI TR 103 305 (CYBER; Critical Security Controls for Effective Cyber Defence):

- ETSI TR 103 305-1 (The Critical Security Controls) is equivalent to version 6.0 of the CIS Security Controls[5].
- ETSI TR 103 305-2 (Measurement and auditing) is equivalent to the CIS Controls Measurement Companion.
- ETSI TR 103 305-3 (Service Sector Implementations) is equivalent to the CIS Controls IoT Security Companion and the CIS Controls Mobile Security Companion.
- ETSI TR 103 305-4 (Facilitation Mechanisms) is equivalent to the Appendices C, D, E and F of v6.0 of the CIS Security Controls.

[5] Note that the latest version of the CIS Controls, as of February 2017, is v6.1.

5.1.3 Cyber Essentials / 10 Steps to Cyber Security

5.1.3.1 Focus

The UK Government launched the 10 Steps to Cyber Security guide to encourage organisations to consider their cyber security measures, and to ascertain whether organisations thought they were managing their cyber risks sufficiently.

The Guide provides organisations with clear guidance on implementation as well as offering independent certification for those who want it. It can be found at https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

5.1.3.2 Associated Evaluation Scheme and Governance

The Cyber Essentials scheme is a cybersecurity standard which organisations can be assessed and certified against. It identifies the security controls that an organisation must have in place within their IT systems in order to have confidence that they are addressing cyber security effectively and mitigating the risk from Internet-based threats.

The scheme focuses on the following five essential mitigation strategies within the context of the 10 Steps to Cyber Security guide.

- Boundary Firewalls and Internet Gateways
- Secure Configuration
- Access Control
- Malware Protection
- Patch Management

Companies can be certified either at the Cyber Essentials or the Cyber Essentials Plus level, see the next section.

The Cyber Essentials scheme is set up by the UK Government which have appointed independent certification bodies to do the assessment. The list of Certified Bodies can be found here: http://www.cyberessentials.org/certifying-bodies/index.html

5.1.3.3 Process

Once an organisation has decided to proceed with a Cyber Essentials certification, a Certifying Body must be appointed to carry out the assessment.

Both Cyber Essentials and Cyber Essentials Plus include a questionnaire which relates to security controls and the secure configuration of an organisation's computing resources. CREST Certifying Bodies also conduct a remote technical assessment at Cyber Essentials aimed at validating elements of the questionnaire.

The key differentiator for Cyber Essentials Plus is the inclusion of a technical review of the organisation's workstations. This additional phase of testing increases the validity of certification considerably by providing evidence of compliance against the following scenarios:

- Can malicious files enter the organisation from the Internet through either web traffic or email messages?
- Should malicious content enter the organisation, how effective are the anti-virus and malware protection mechanisms?
- Should the organisation's protection mechanisms fail, how likely is it that the organisation will be compromised due to failings in the patching of the organisation's workstations?

5.1.3.4 Practice

A list with originations having the Cyber Essentials certificate can be found here: http://www.cyberessentials.org/list/

5.1.3.5 Formal Status

All suppliers bidding for government contracts which involve handling of sensitive and personal information and provision of certain technical products and services, are required to be compliant with the Cyber Essentials controls.

5.1.3.6 Relation to other standards / schemes

No official relationships. However, the technical controls within the scheme reflect those covered in well-established standards, such as the ISO/IEC 27000 series.

5.1.4 Cyber Resilience Review

5.1.4.1 Focus

The Cyber Resilience Review (CCR) is based upon ten domains, namely:

- Asset Management
- Controls Management
- Configuration and Change Management
- Vulnerability Management
- Incident Management
- Service Continuity Management
- Risk Management
- External Dependencies Management
- Training and Awareness
- Situational Awareness

5.1.4.2 Associated Evaluation Scheme and Governance

The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organisation's operational resilience and cybersecurity practices. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organisational resilience as well as provide a gap analysis for improvement based on recognised best practices.

The Department of Homeland Security (DHS) partnered with the Computer Emergency Response Team (CERT) Division of Carnegie Mellon University's Software Engineering Institute to create the CRR.

5.1.4.3 Process

Each domain is composed of a purpose statement, a set of specific goals and associated practice questions unique to the domain, and a standard set of Maturity Indicator Level (MIL) questions. The MIL questions examine the institutionalisation of practices within an organisation.

The CCR consists of three key phases:

1. The assessment. The CRR is typically delivered in a six-hour workshop led by facilitators from DHS. The facilitators elicit answers from the critical infrastructure organisation's personnel in cybersecurity, operations, physical security, and business continuity. However, the CRR Self-Assessment Package allows organisations to apply the same method without the participation of external facilitators. It contains the same questions, scoring mechanisms, and options for improvement as the externally facilitated CRR.
2. Interpreting the CRR Report. The results documented are interpreted within the context of the organisation.
3. Making Improvements. The organisation determines next steps for improving its cybersecurity practices.

5.1.4.4 Practice

There is no certification process affiliated with the CRR.

5.1.4.5 Formal Status

None.

5.1.4.6 Relation to other standards / schemes

A mapping of the CRR to the NIST Cybersecurity Framework is available here: https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf.

5.1.5 FINCSC – Finnish Cyber Security Certificate

5.1.5.1 Focus

The Finnish Cyber Security Certificate (FINCSC) is a cybersecurity certification for companies and organisations, especially Small and Medium Enterprises (SME). Its aim is to create an understanding of the cybersecurity needs of the organisation and using this knowledge to ensure business continuity. Holding a FINCSC certificate enables an organisation to maintain information security and data protection, as well as ensuring effective and reliable services for its customers and partners.

The FINCSC is suitable for all organisations, regardless of type, sise or sector. However, the scheme is especially aimed at SMEs, as the originators considered that existing schemes were too expensive for such companies.

5.1.5.2 Associated Evaluation Scheme and Governance

The scheme was created and is governed by the JAMK University of Applied Sciences, in collaboration with the Confederation of Finnish Industries, the Federation of Finnish Enterprises, Telia Company Ltd and the Finnish Communications Regulatory Authority.

5.1.5.3 Process

The evaluation scheme is based on a self-assessment, using a questionnaire that contains question in 11 different categories. The questionnaire is then assessed by an accredited Assessor Body.

The fee for certification is 350€.

After the certificate expires, the organisation must take part in a renewal process.

5.1.5.4 Practice

A pilot was carried out in 2015 and 2016. Since the official start of the scheme in December 2016, about 30 SMEs have obtained the certificate and the number grows continually. Five companies have a license to act as an Assessor Body.

5.1.5.5 Formal Status

None.

5.1.5.6 Relation to other standards / schemes

There are no official relationships to other standards or schemes.

5.1.6 ISF Standard of Good Practice for Information Security

5.1.6.1 Focus

The Standard of Good Practice for Information Security 2016 provides comprehensive controls and guidance on current and emerging information security topics enabling organisations to respond to the rapid pace at which threats, technology and risks evolve. Implementing the Standard helps organisations to:

- Identify how regulatory and compliance requirements can be met
- Respond to rapidly evolving threats, including sophisticated cyber security attacks by using threat intelligence to increase cyber resilience
- Be agile and exploit new opportunities – while ensuring that associated information risks are managed to acceptable levels.

The 2016 version includes the introduction of topics such as:

- Threat Intelligence
- Cyber Attack Protection
- Industrial Control Systems

- Information Risk Assessment
- Security Architecture
- Enterprise Mobility Management

5.1.6.2 Associated Evaluation Scheme and Governance

There is no evaluation scheme or certification. The standard serves as a guideline.

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by developing best practice methodologies, processes and solutions that meet the business needs of its Members.

5.1.6.3 Process

None.

5.1.6.4 Practice

Members of the ISF have free access to the Standard. It is unclear to what extent these members have implemented the Standard.

Some of the members are listed on the following page: https://www.securityforum.org/about/our-members/

5.1.6.5 Formal Status

None.

5.1.6.6 Relation to other standards / schemes

The Standard, along with the ISF Benchmark; a comprehensive security control assessment tool, provide complete coverage of the topics set out in ISO/IEC 27002:2013, COBIT 5 for Information Security, NIST Cybersecurity Framework, SANS Top 20 Critical Security Controls for Effective Cyber Defense and Payment Card Industry Data Security Standard (PCI DSS) version 3.1.

5.1.7 IT Grundschutz

5.1.7.1 Focus

The IT-Grundschutz Catalogues contain recommendations for standard security safeguards for typical business processes, applications, and IT systems. The objective of IT-Grundschutz is to achieve an adequate level of protection for all information available in an organisation.

Central in the IT-Grundschutz catalogue are the modules. Each of the modules of the IT-Grundschutz Catalogues contains a short description of the applicable components, approaches, and IT systems, as well as an overview of the threat scenario and the recommended safeguards.

The modules are grouped into the following catalogues according to the IT-Grundschutz layer model:

- Generic aspects: This includes modules such as security management (not WHAT needs to be done, but concretises the HOW), as well as topics such as patch and change management or outsourcing.
- Infrastructure: This layer presents recommendation on, among other things, the protection of buildings, data centres, office spaces, mobile workplaces and cabling.
- IT systems: This is a collection of instructions on securing various operating systems, as well as mobile telephones, multifunctional devices, or routers and switches.
- Networks: This layer covers security requirements for heterogeneous networks, network management, WLAN (wireless networks), VoIP (Voice over IP – computer telephony), Bluetooth and other networks.
- IT applications: This final layer presents measures for SAP, Exchange Server, Active Directory and internet use, for example.

Next to the module section, the threat and the safeguard sections of the IT-Grundschutz Catalogue contain detailed descriptions of 1) the threats referred to as the threat scenarios in the individual modules and 2) the security safeguards mentioned in the modules.

In order to achieve an appropriate level of security, the BSI Standard 100-2 “The IT-Grundschutz Methodology” describes how an efficient management system for information security can be set up and how the IT-Grundschutz Catalogues can be used for this purpose. A systematic approach is required to design the security process, and the security process is comprised of the following phases in the context of IT-Grundschutz:

- 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
    - Structure analysis
    - Determination of the protection requirements
    - Selection and adaptation of safeguards
    - Basic security check
    - Supplementary security analysis
- Implementation of the security concept
- Maintenance of information security during live operations and implementation of continuous improvement process

5.1.7.2 Associated Evaluation Scheme and Governance

In order to make the successful implementation of IT-Grundschutz clear to the outside world, the BSI has developed a certification scheme for information security. This scheme takes the requirements on management systems for information security found in ISO/IEC 27001 into

account. Unlike the original ISO 27001 certification, the “ISO 27001 certificate based on IT-Grundschutz” not only covers the information security management system, but also the concrete technical implementation.

The Bundesamt für Sicherheit in der Informationstechnik (BSI) is the German Upper-level Federal agency in charge of managing computer and communication security for the German government. Its areas of expertise and responsibility include the security of computer applications, critical infrastructure protection, Internet security, cryptography, counter eavesdropping, certification of security products and the accreditation of security test laboratories.

5.1.7.3 Process

The basis for awarding an ISO 27001 certificate on the basis of IT-Grundschutz is the audit performed by an external auditor who is certified with the BSI. The result of the audit is an audit report that is then presented to the certification department, which decides if the ISO-27001 certificate based on IT-Grundschutz should be awarded. Sets of criteria for the procedure are, in addition to the ISO 27001 standard, the IT-Grundschutz methodology.

The auditors audit the submitted information security management system (ISMS) documents and verify their correctness against spot checks in an on-site audit. This audit does not focus merely on the concrete implementation of the catalogues of safeguards for technical systems. Rather, it addresses the question of to what extent the management exercises its responsibility. The audit asks, for example, whether the management has allocated sufficient resources to permanently establish the information security management system. Once the ISMS has been established and the measures have been implemented, the actual certification is relatively effortless.

Because the process of fully implementing IT-Grundschutz is frequently long, there are two preliminary stages, the initiation stage and the expansion stage, marked by so-called auditor’s certificates which can already be issued once certain subsets of the safeguards defined in the catalogues have been implemented.

An ISO 27001 certificate is issued for three years. A brief, routine auditing visit is made once a year to ensure the level of security is being maintained.

5.1.7.4 Practice

No central database of issued certificates is available.

5.1.7.5 Formal Status

None. However, an IT Grundschutz-based evaluation is mandatory (or will become mandatory) for critical infrastructures in Germany in the context of KRITIS (see section 5.10.2).

5.1.7.6 Relation to other standards / schemes

The IT-Grundschutz is strongly related to ISO 27001, however it is significantly deeper and more specific. Put simply, the controls (requirements) of ISO 27001 describe WHAT needs to be done, while IT-Grundschutz additionally describes HOW it can be done.

5.1.8 ISO/IEC 27001 (Information Security Management Systems — Requirements)

5.1.8.1 Focus

ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). ISO describes an ISMS as 'a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.' The standard describes how an organisation must set its security objectives and determine the risks that threaten these objectives. The organisation can respond to the identified risks with a risk treatment plan. An important part of this plan is choosing appropriate controls. ISO 27001 contains a list of controls for each security objective, although it is not mandatory to implement all of these controls and other controls may be used as well.

ISO 27001 (together with other standards in the family) also provides the framework for 3rd party audits and certification of an organisation's ISMS.

The ISO 27001 family of standards has been growing quickly over the last years, and now includes some 40 standards. The table below gives an overview of the most relevant of these within the context of this document. Some of these standards are discussed in separate sections of this document, as referenced.

ISO/IEC number	Focus	Reference
ISO/IEC 27002	Gives a more detailed description of the controls described in Annex A of ISO 27001	-
ISO/IEC 27003	Gives implementation guidance for ISO 27001	-
ISO/IEC 27004	Gives guidance on monitoring, measurement, analysis and evaluation of an ISMS	-
ISO/IEC 27005	Provides guidelines for information security risk management	-
ISO/IEC 27011	Adds requirements, guidance and controls specific for telecommunications organisations	5.9.2

ISO/IEC 27015	Adds requirements, guidance and controls specific for financial services organisations	5.5.3
ISO/IEC 27017	Adds requirements, guidance and controls specific for cloud services	4.5
ISO/IEC 27018	Adds requirements, guidance and controls specific for public cloud services acting as Personally Identifiable Information (PII) processors	4.7
ISO/IEC 27019	Adds requirements, guidance and controls specific for the energy industry	5.3.2
ISO/IEC 27032	Adds requirements, guidance and controls for improving cybersecurity	5.1.10
ISO/IEC 27033	Adds requirements, guidance and controls for network security	5.1.11
ISO/IEC 27034	Adds requirements, guidance and controls for application security	5.1.12
ISO/IEC 27035	Adds requirements, guidance and controls for incident management	5.1.13
ISO/IEC 27036	Adds requirements, guidance and controls for supplier management	5.1.13
ISO/IEC 27799	Health informatics - Information security management in health using ISO/IEC 27002	5.7.1

5.1.8.2 Associated Evaluation Scheme and Governance

Organisations can have their information security management system certified against ISO 27001 by independent certification bodies. To ensure sufficient quality of these certifications, certification bodies can be accredited by a national accreditation body. The International Accreditation Forum keeps a list of all accreditation bodies per country, see http://www.iaf.nu/articles/IAF_Members__Signatories/4.

Each accreditation body keeps a list of accredited certification bodies, such that interested organisations can easily find a reputable party to work with.

5.1.8.3 Process

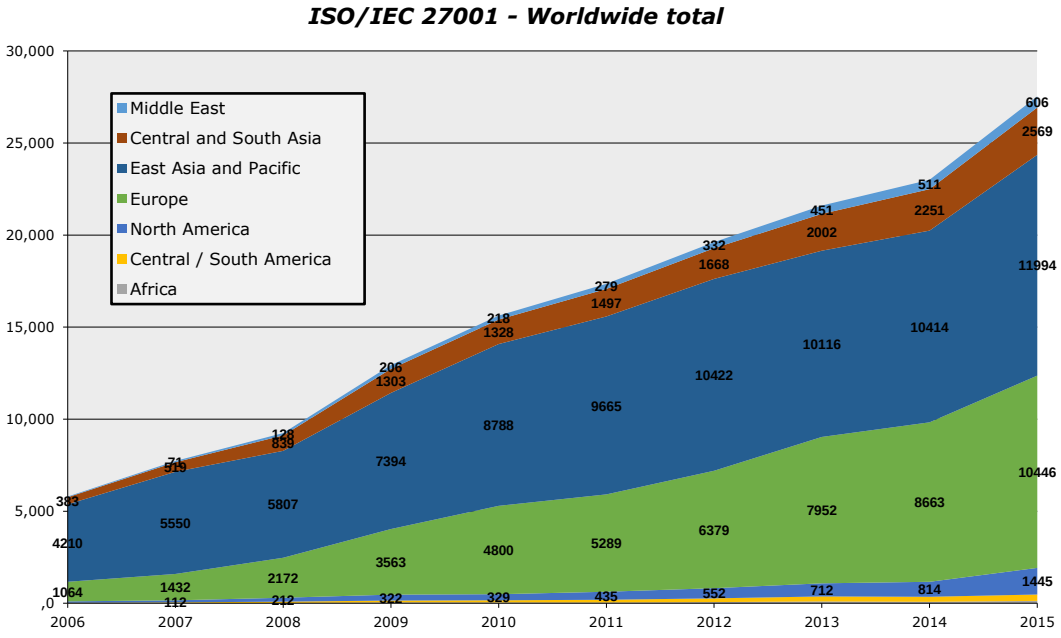
When creating an ISMS that is able to be certified against ISO 27001, an organisation should start by developing and documenting the necessary ISO 27001 procedures and controls. These procedures and controls should then be implemented according to these documents. Regular internal audits and management reviews of these documents and their implementing is part of the requirements of ISO 27001 and follows from the requirement that the ISMS should not just be (and remain) compliant, but should be continually improved. All non-compliancies found during an internal audit or management review should be mitigated by corrective and preventive actions. In other words, not only should the error be corrected, but measures should be taken to prevent the error from happening again.

Once all of this is in place, the certification process can start. This is divided in two steps: a Stage 1 audit and Stage 2 audit. In the Stage 1 audit (Documentation review) the auditor checks whether the organisation's documentation is compliant with ISO 27001. During Stage 2 audit (Main audit) the auditor checks whether all organisation activities are compliant with both ISO 27001 and their documentation.

Any non-compliancies found by the auditor that prevent certification must corrected within a certain time period. Once a certificate is granted, it is valid for three years, after which another Stage 1 audit and Stage 2 audit must take place before the certificate can be renewed.

5.1.8.4 Practice

ISO regularly publishes the 'ISO Survey of Certifications', which shows the number of valid certificates to ISO management system standards (including ISO 9001, 14001, 20001 and 27001) worldwide. The latest edition of this survey is from 2015 and shows particularly quick growth for ISO 27001 with a 20% increase to 27,536 certificates worldwide. With 10,446 issued certificates, European organisations account for almost 40% of the total. The figure below is taken from the survey.



The survey also makes clear that ISO 27001-certified organisations come from all sectors of the economy, ranging from agriculture to education. The number of European countries in which such organisations can be found is 47.

These numbers make clear that ISO 27001 is the IT-security related certification with the most uptake in this survey, apart from some certifications for security professionals.

5.1.8.5 Formal Status

None.

5.1.8.6 Relation to other standards / schemes

ISO 27001 forms the basis for other standards in the ISO 270xx family.

ENISA listed ISO 27001 certification on its Cloud Certification Schemes List (CCSL) – see https://resilience.enisa.europa.eu/cloud-computing-certification.

ISO/IEC 21827 (see section 5.11.3) is an International Standard based on the Systems Security Engineering Capability Maturity Model (SSE-CMM) that can measure the maturity of the implementation of ISO 27001 / ISO 27002 security controls.

5.1.9 ISO/IEC 27002 (Code of practice for information security controls)

5.1.9.1 Focus

ISO/IEC 27002 is a code of practice - a generic, advisory document; not a formal specification such as ISO/IEC 27001. It recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information. The same information security controls are also discussed in ISO

Management should define a set of policies to clarify their direction of, and support for, information security. At the top level, there should be an overall “information security policy”. Within this policy, the following controls should be considered:

- Organization 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
- Compliance

5.1.9.2 Associated Evaluation Scheme and Governance

Organizations that adopt ISO/IEC 27002 must assess their own information risks, clarify their control objectives and apply suitable controls (or indeed other forms of risk treatment) using the standard for guidance.

5.1.9.3 Process

None

5.1.9.4 Practice

Because of the relationship between ISO 27002 and ISO 27001, the numbers given in section 5.1.8.4 also apply for ISO 27002.

5.1.9.5 Formal Status

None

5.1.9.6 Relation to other standards / schemes

None

5.1.10 ISO/IEC 27032 (Guidelines for cybersecurity)

5.1.10.1 Focus

ISO/IEC 27032 provides guidance for improving the state of cybersecurity, drawing out its unique aspects and its dependencies on other security domains. It covers the baseline security practices for stakeholders in cyberspace. This standard provides:

- an overview of cybersecurity,
- an explanation of the relationship between cybersecurity and other types of security,
- a definition of stakeholders and a description of their roles in cybersecurity,
- guidance and controls (over and above those in ISO/IEC 27001) for addressing common cybersecurity risks,
- a framework to enable stakeholders to collaborate on resolving cybersecurity issues.

5.1.10.2 Associated Evaluation Scheme and Governance

See section 5.1.8.2 on the governance of ISO 27001.

At least some ISO 27001 certification bodies offer certification against ISO 27032, even though it officially is a guideline and not a certification standard. Such a certification means that the ISMS in question obtained ISO 27001 certification and additionally complies with the guidance for the existing security controls and with the new controls in ISO 27032.

5.1.10.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

5.1.10.4 Practice

As the ISO survey (see section 5.1.8.4) does not give information on ISO 27032 separately, it is hard to get an overview. A number of companies claiming certification against ISO 27032 were found, however this number seems to be quite limited.

5.1.10.5 Formal Status

None.

5.1.10.6 Relation to other standards / schemes

Given the broad scope of this standard, the controls provided are at a high level. The standard does refer to a number of other standards to provide more detail.

PECB offers basic and more advanced courses (including exams and certificates) on ISO 27032, including courses for auditors.

5.1.11 ISO/IEC 27033 (Network Security)

5.1.11.1 Focus

ISO/IEC 27033-1:2015 includes the following:

- An overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security
- Guidance on how network security risks are identified and analysed, and the definition of network security requirements based on that analysis.
- An overview of the controls that support network technical security architectures and related technical controls, as well as those non-technical controls and technical controls that are applicable not just to networks
- An introduction to good quality network technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network "technology" areas, and briefly addresses the issues associated with implementing and operating network security controls, and the on-going monitoring and reviewing of their implementation.

5.1.11.2 Associated Evaluation Scheme and Governance

See section 5.1.8.2 on the governance of ISO 27001.

At least some ISO 27001 certification bodies offer certification against ISO 27033, even though it officially is a guideline and not a certification standard. Such a certification means that the ISMS in question obtained ISO 27001 certification and additionally complies with the guidance for the existing security controls and with the new controls in ISO 27033.

5.1.11.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

5.1.11.4 Practice

As the ISO survey (see section 5.1.8.4) does not give information on ISO 27033 separately, it is hard to get an overview. A number of companies claiming certification against ISO 27033 were found, however this number seems to be quite limited.

5.1.11.5 Formal Status

None

5.1.11.6 Relation to other standards / schemes

ISO/IEC 27033 is part of the ISO 27000 family.

5.1.12 ISO/IEC 27034 (Application Security)

5.1.12.1 Focus

ISO/IEC 27034 offers guidance on information security to those specifying, creating or procuring, implementing and using application systems. The aim is to ensure that computer applications deliver the necessary level of security in support of the organisation's Information Security Management System. ISO 27034 consists of six parts, some of which are still drafts:

- Part 1: Overview and concepts – published 2011
- Part 2: Organisation normative framework – published 2015
- Part 3: Application security management process – expected publication May 2017
- Part 4: Application security validation – expected publication 2019
- Part 5: Protocols and application security control data structure - expected publication May 2017
- Part 5-1: Protocols and application security control data structure – XML schemas – under development
- Part 6: Case studies – published 2016 (informative)

ISO/IEC 27034 is aimed at architects, analysts, programmers, testers, IT Team, DBA, Admins, etc., who need to know what and when Application Security Controls should be applied, integrate Application Security Controls in their activities, meet the requirements of the Application Security Controls associated measurements, get access to tools and best practices and facilitate peer review.

It can also be used by auditors, in order to know the scope and process of verification measurements for the corresponding Application Security Controls, make audit results repeatable, identify a list of verification measurements which can generate supporting evidence to demonstrate that the application has reached the required level of trust authorised by the management and standardise the application security verification.

5.1.12.2 Associated Evaluation Scheme and Governance

See section 5.1.8.2 on the governance of ISO 27001.

It does not seem currently possible (yet) to be evaluated by an independent certification body against ISO 27034 specifically.

5.1.12.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

5.1.12.4 Practice

A number of companies (including Microsoft) have issued self-declarations for conformance against ISO 27034-1.

Several companies offer basic and more advanced courses (including exams and certificates) on ISO 27034, including courses for auditors.

5.1.12.5 Formal Status

None.

5.1.12.6 Relation to other standards / schemes

ISO/IEC 27034 does not propose any Application Security Controls by itself, nor any coding or testing best practices, although Part 6 discusses some possibilities. A possible source of best practices and technical details that can be used to create ASCs is the OWASP Top 10, see section 3.7.2. OWASP has started a project to convert the latest OWASP Top 10 into ASCs suitable for use with ISO 27034; see https://www.owasp.org/index.php/OWASP_ISO_IEC_27034_Application_Security_Controls_Project.

5.1.13 ISO/IEC 27035 (Information security incident management)

5.1.13.1 Focus

ISO/IEC 27035 consists of two parts: 27035-1 and 27035-2:

- Part 1 outlines the concepts and principles underpinning information security incident management and introduces the remaining part(s) of the standard. It describes an information security incident management process consisting of five phases, and says how to improve incident management.
- Part 2 concerns assurance that the organisation is in fact ready to respond appropriately to information security incidents that may yet occur. It addresses the rhetorical question “Are we ready to respond to an incident?” and promotes learning from incidents to improve things for the future. It covers the Plan and Prepare and Lessons Learned phases of the process laid out in part 1.

5.1.13.2 Associated Evaluation Scheme and Governance

See section 5.1.8.2 on the governance of ISO 27001.

At least some ISO 27001 certification bodies offer certification against ISO 27035, even though it officially is a guideline and not a certification standard. Such a certification means that the ISMS in question obtained ISO 27001 certification and additionally complies with the guidance for the existing security controls and with the new controls in ISO 27035.

5.1.13.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

5.1.13.4 Practice

As the ISO survey (see section 5.1.8.4) does not give information on ISO 27035 separately, it is hard to get an overview. A number of companies claiming certification against ISO 27035 were found, however this number seems to be quite limited.

5.1.13.5 Formal Status

None

5.1.13.6 Relation to other standards / schemes

ISO/IEC 27035 is part of the ISO 27000 family.

The ETSI standards on Information Security Indicators (see http://www.etsi.org/technologies-clusters/technologies/information-security-indicators) form a specific reference framework for information security incident management, providing:

- A full set of operational indicators for organisations to use to benchmark their security posture,
- A guide to select operational indicators from the full set,
- A security event classification model and taxonomy,
- Guidelines for security event detection testing and assessment of detection effectiveness,
- Key Performance Security Indicators (KPSI) to evaluate the maturity of security event detection

5.1.14 ISO/IEC 27036 (Information security for supplier relationships)

5.1.14.1 Focus

ISO/IEC 27036 consists of four parts:

- Part 1 provides overview and concepts of information security in supplier relationships.

- Part 2 provides a high level framework for establishing information security requirements and expectations in supplier relationships. This framework includes governance, life cycle processes, and relevant high-level requirements statements.

Based upon part 1 and part 2, the other two parts focus upon guidelines for ICT supply chain security and guidelines for security of cloud services.

- Part 3 provides guidelines to acquirers and suppliers for managing information security risks associated with the ICT products and services supply chain. It builds on the requirements in Part 2 and provides additional practices that augment high-level requirements from Part 2. A wide range of information security controls are noted in part 3.
- Part 4 provides guidelines for information security of cloud computing services which are often provided through supply chain from the perspective of both the acquirer and supplier of such services. Specifically, it involves managing the information security risks associated with cloud computing services throughout the supplier relationship life cycle. It builds on the requirements in Part 2 and provides additional practices that can augment high-level requirements from Part 2 and guidance from Part 3.

5.1.14.2 Associated Evaluation Scheme and Governance

There is no related evaluation scheme. Moreover, part 2 explicitly states that ISO/IEC 27036 Part 2 is not intended for certification purposes.

However, see section 5.1.8.2 on the governance of ISO 27001.

5.1.14.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

5.1.14.4 Practice

The ISO survey (see section 5.1.8.4) does not give information on ISO 27036 separately, and an exact number therefore cannot be given.

5.1.14.5 Formal Status

None

5.1.14.6 Relation to other standards / schemes

ISO/IEC 27036 is part of the ISO/IEC 27001 family (see section 5.1.8).

Part 3: Most of the controls mentioned in this part are covered in general terms by ISO/IEC 27002, however, this part provides additional guidance in the specific context of ICT supplies. An annex includes a breakdown of comparable clauses in ISO/IEC 15288 and ISO/IEC 12207, and another identifies relevant clauses from ISO/IEC 27002.

Part 4: This part does not include business continuity management/resiliency issues involved with the cloud service. ISO/IEC 27031 addresses business continuity. This part does not provide

guidance on how a cloud service provider should implement, manage and operate information security. Guidance on those can be found in ISO/IEC 27002 and ISO/IEC 27017 (see section 4.6).

5.1.15 ISO/IEC 29100 (Privacy architecture framework) and related ISO standards

5.1.15.1 Focus

ISO issued a set of guidelines and frameworks on privacy protection. Other standards are in preparation

The main standards already published are:

- ISO/IEC 29100 (Privacy framework):
  - This document provides a privacy framework which:
    - specifies a common privacy terminology;
    - defines the actors and their roles in processing personally identifiable information (PII);
    - describes privacy safeguarding considerations; and
    - provides references to known privacy principles for information technology.
- ISO/IEC 29101 (Privacy architecture framework):
  - This document defines a privacy architecture framework that
    - specifies concerns for information and communication technology (ICT) systems that process personally identifiable information (PII);
    - lists components for the implementation of such systems; and
    - provides architectural views contextualizing these components.
- ISO/IEC 29190 (Privacy capability assessment model):
  - This document provides organisations with high-level guidance about how to assess their capability to manage privacy-related processes. In particular, it
    - 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.

Privacy standards under development include:

- ISO/IEC 29134 (Guidelines for privacy impact assessment):
  - This document gives guidelines for:
    - a process on privacy impact assessments; and
    - a structure and content of a PIA report.
- ISO/IEC 27550 (Privacy engineering):
  - For this standard no further information could be found.
- ISO/IEC 27551 (Requirements for attribute-based unlinkable entity authentication)

    - For this standard no further information could be found.
- ISO/IEC 27552 (Enhancement to ISO/IEC 27001 for privacy management - Requirements)
    - For this standard no further information could be found.
- ISO/IEC 29151 (Code of practice for personally identifiable information protection)
    - For this standard no further information could be found.
- ISO/IEC 20547-4 (Big data reference architecture -Security and privacy fabric)
    - For this standard no further information could be found.

5.1.15.2 Associated Evaluation Scheme and Governance

None.

5.1.15.3 Process

None.

5.1.15.4 Practice

None.

5.1.15.5 Formal Status

None.

5.1.15.6 Relation to other standards / schemes

Another ISO standard related to privacy is ISO / IEC 27018, see section 4.7.

5.1.16 LEET Security Stamp

5.1.16.1 Focus

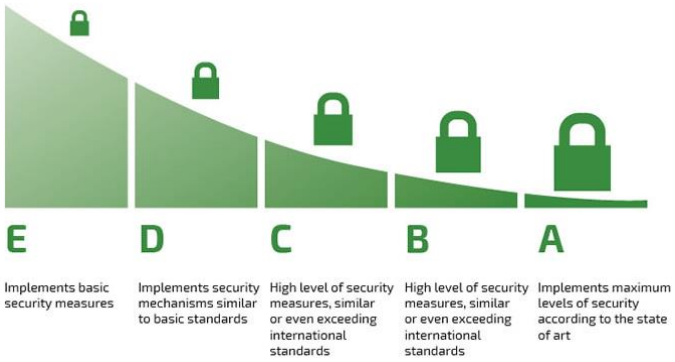
The LEET Security Stamp is based upon a rating guide containing over 850 controls with the focus upon Confidentiality, Integrity and Availability. These controls are subdivided into 14 categories:

- Information Security Management Program
- Systems Operation
- Personnel Security
- Facility Security
- Third-party processing
- Resilience
- Compliance
- Malware protection
- Network controls
- Monitoring
- Access control

- Secure development
- Incident handling
- Cryptography

5.1.16.2 Associated Evaluation Scheme and Governance

The organisation is rated using the rating guide, and the score will be displayed within three dimensions: Confidentiality, Integrity and Availability. The LEET stamp shows the score for the qualified service achieved on each of them, depending on the security and service continuity implemented measures.



The guide was developed by Leet Security after receiving feedback from interested parties (people / organisations commenting are listed in the acknowledgments section). The rating agency LEET Security is an independent entity, formed for the sole purpose of developing and managing a labeling system to qualify reliably the levels of information security offered by ICT service providers, particularly -but not solely- in cloud environments.

Customers / providers will provide feedback during the next review period (every 2 years). Leet Security is responsible for keeping the guide up to date, updating it with addressing emerging technologies and new threats. Leet Security is also responsible for maintain the list of current labelled / rated services and assuring the continuous adherence of those services to the level published. Customers have free access to a safe channel to express any divergence between current situation in the service provided and the level of security rated. Leet Security is responsible for investigating all the issues raised. In order to assure that security labels / ratings correspond to the current situation, Leet Security is also responsible for auditing service providers periodically.

5.1.16.3 Process

- The first step to get a service rated is to complete an application through the website or offline. Once the application has been processed, the following step is signing the contract that establishes the use conditions of our rating system and defines the scope and characteristics of the service/s being rated.
- The next step, the registration process, has different activities:
  1. Training. Each service provider needs to have a minimum of people with enough knowledge of rating methodology and criteria.

2. Presentation of memorandum. The service provider should present a memorandum where it explains and justifies how and why it considers that its service should have a particular rating level.
3. Validation. Based on the previous documentation, the rating agency will carry out an on-site evaluation within the following 20 days, and approve the service rating application, require further information or clarification, or to propose and alternative level.

- The follow-up to ensure that the required conditions are maintained during the period of validity, is performed based on three additional control mechanisms:
  1. Perform random audits.
  2. Digital surveillance, including incident/compain notification channel for users of rated services.
  3. Obligation for the provider to notify LEET Security about any circumstance or modification that may affect the rating.

- In either case, LEET Security would proceed with a reassessment in order to determine whether maintenance or modification of the rating levels granted to the service.
  - The rating has a period of validity of 12 months starting in the date when it is formally approved.

5.1.16.4 Practice

ENISA listed the LEET Security Rating Guide on its Cloud Certification Schemes List (CCSL) – see https://resilience.enisa.europa.eu/cloud-computing-certification.

5.1.16.5 Relation to other standards / schemes

None.

5.1.17 Open Trusted Technology Provider Standard (O-TTPS)

5.1.17.1 Focus

The O-TTPS is an open standard containing a set of organisational guidelines, requirements, and recommendations for integrators, providers, and component suppliers to enhance the security of the global supply chain and the integrity of Commercial Off The Shelf (COTS) Information and Communication Technology (ICT). This standard if properly adhered to will help assure against maliciously tainted and counterfeit products throughout the COTS ICT product life cycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

5.1.17.2 Associated Evaluation Scheme and Governance

The Open Group Trusted Technology Forum (OTTF) offers a program which grants organisation with a certification if they comply with the O-TTPS.

The OTTF is a global initiative that invites industry, government, and other interested participants to work together to evolve this document and other OTTF deliverables.

The OTTF has a large number of members. The platinum members are Capgemini, Fujitsu, HP, Huawei, IBM, Oracle and Philips. Notable gold members are American Express, Boeing, Microsoft and NASA. The full list can be accessed at https://reports.opengroup.org/membership_report_all.pdf.

5.1.17.3 Process

Organisations can get the certification either through a self-assessment or by third party assessment. The certification is valid for three years.

The Third-Party Assessed tier requires the applicant to use an O-TTPS Recognized Assessor to assess evidence of conformance that is supplied by the applicant. For the Self-Assessed tier, the applicant completes the assessment independently and is not required to use an O-TTPS Recognized Assessor, though may choose to utilise the assistance of a third-party assessor in determining conformance.

The list of recognised assessors can be found on http://certification.opengroup.org/ottps-recognized-assessors.

5.1.17.4 Practice

At this point only two organisations are certified with the O-TTPS: IBM and Huawei. The list can be found on https://certification.opengroup.org/register/ottps-certification

5.1.17.5 Formal Status

None.

5.1.17.6 Relation to other standards / schemes

None.

5.1.18 Service Organisation Controls (SOC)

5.1.18.1 Focus

The Assurance Services Executive Committee (ASEC) of the American Institute of CPAs (AICPA) has developed the Trust Services Principles and Criteria (TSPC) which address the risks and opportunities of IT-enabled systems and privacy programs. The following principles and related criteria are used by practitioners in the performance of Trust Services engagements:

- Security. The system is protected against unauthorised access, use, or modification to meet the entity's commitments and system requirements.
- Availability. The system is available for operation and use to meet the entity's commitments and system requirements.
- Processing integrity. System processing is complete, valid, accurate, timely, and authorised to meet the entity's commitments and system requirements.
- Confidentiality. Information designated as confidential is protected to meet the entity's commitments and system requirements.

- Privacy. Personal information is collected, used, retained, disclosed and disposed to meet the entity's commitments and system requirements.

5.1.18.2 Associated Evaluation Scheme and Governance

AICPA has developed three different kind of Service Organisation Controls (SOC) of which type 2 and 3 specifically focus upon the TSPC. The SOC are designed to help service organisations, organisations that operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant (CPA).

Each type of SOC report is designed to help service organisations meet specific user needs:

- SOC1: Report on Controls at a Service Organisation Relevant to User Entities' Internal Control over Financial Reporting
- These reports are intended to meet the needs of entities that use service organisations and the service auditors who audit the user entities' financial statements when evaluating the effect of controls at the service organisation on the user entities' financial statements.
  - SOC2: Report on Controls at a Service Organisation Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
- These reports are intended to meet the needs of a broad range of users who need information and assurance about controls at a service organisation that affect the security, availability, or processing integrity of the systems that the service organisation uses to process users' data or the confidentiality or privacy of the information processed by these systems.
  - SOC3: Trust Services Report for Service Organisations
- These reports are designed to meet the needs of a wider range of users who need assurance about controls at a service organisation that affect the security, availability, or processing integrity of the systems used by a service organisation to process users' information, or the confidentiality or privacy of that information, but do not have the need for or knowledge necessary to effectively use a SOC2 report.

Unlike a SOC 1 report, which is only an auditor-to-auditor communication, SOC 2 Reports are generally restricted use report (at the discretion of the auditor using the guidance in the standard) and SOC 3 Report (in all cases) will enable the service organisation to share a general use report that would be relevant to current and prospective customers or as a marketing tool to demonstrate that they have appropriate controls in place to mitigate risks related to security, privacy, etc.

The American Institute of CPAs is active in 143 countries. AICPA members represent many areas of practice, including business and industry, public practice, government, education and consulting.

The AICPA sets ethical standards for the profession and U.S. auditing standards for private companies, nonprofit organisations, federal, state and local governments. It develops and grades the Uniform CPA Examination, and offers specialty credentials for CPAs who concentrate on personal financial planning; forensic accounting; business valuation; and information management and technology assurance.

5.1.18.3 Process

1. Choosing what SOC suits the organisation:

Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC 1 Report
Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?	Yes	SOC 1 Report
Will the report be used by your customers or stakeholders to gain confidence and place trust in a service organisation's systems?	Yes	SOC 2 or 3 Report
Do you need to make the report generally available or seal?	Yes	SOC 3 Report
Do your customers have the need for and ability to understand the details of the processing and controls at a service organisation, the tests performed by the service auditor and results of those tests?	Yes	SOC 2 Report
	No	SOC 3 Report

2. Choose a CPA that will take the SOC audit from the following list: http://www.aicpa.org/InterestAreas/GovernmentalAuditQuality/Membership/Pages/Findamemberfirm.aspx

   It is not clear whether all these members offer SOC audits, but some notable CPAs that do are Deloitte, Ernst & Young and Price Waterhouse Coopers

3. The auditing process is not predefined and can therefore differ between CPAs.

5.1.18.4 Practice

The following list includes but is not limited to:

- Amazon web services
- Microsoft Azure

Between October and December of 2015, EY surveyed 49 global financial services organisations with third-party risk functions in the retail and commercial banking, investment banking, insurance, and wealth and asset management sectors. The purpose of the survey was to address the distinctive nature of managing third-party risk in the financial services industry.

71% of organisations find that a service organisation controls (SOC) 2 report is useful (neutral or above) in reducing or removing the need to perform a review on a third party, up from 52% last year.

5.1.18.5 Formal Status

None.

ENISA listed the SOC 1, 2 and 3 on its Cloud Certification Schemes List (CCSL) – see https://resilience.enisa.europa.eu/cloud-computing-certification.

5.1.18.6 Relation to other standards / schemes

None.

5.1.19 Shared Assessments Program

5.1.19.1 Focus

For most top-tier organisations, outsourcing key functions has become a necessary component to creating efficiencies in today's complex economy. Organisations must develop comprehensive programs managing third party risk in areas such as security, cybersecurity, technology, privacy, and business resiliency risk.

The standard focusses upon key controls in the following domains of third party risk management:

- Risk assessment and treatment
- Security policy
- Organisational security
- Asset and information management
- Human resources security
- Physical and environmental security
- Operations management
- Access control
- Application security
- Incident event and communications management
- Business resiliency
- Compliance
- Network security
- Privacy
- Treatment management.
- Server security
- Cloud security

5.1.19.2 Associated Evaluation Scheme and Governance

The Shared Assessments Program consists of two schemes in order to evaluate the key controls: the Standardized Information Gathering (SIG) questionnaire and the Agreed Upon Procedures (AUP). The two can be used separately, but the AUP can also be used as a verification of the SIG.

- The SIG questionnaire allows an issuer/outsourcer to obtain all of the information necessary to conduct an initial assessment of a service provider's cybersecurity, IT, privacy, data security and business resiliency controls. Questions within the SIG are filtered by the user to apply to the specific type of service outsourced to the third party.
- The AUP is a tool for performing standardised onsite risk management assessments, including assessments of cybersecurity, IT, privacy, data security, and business resiliency. The AUP provides several vital functions:
    - First it allows an outsourcer to validate the answers provided by a third party using the SIG questionnaire.
    - Secondly, it sets forth the risk control areas to be assessed as part of an onsite assessment, as well as the procedures to be followed while conducting the assessment and the sampling procedures to be used.

Shared Assessments is a member-driven, industry-standard body with tools and best practices. Shared Assessments Program members work together to eliminate redundancies and create efficiencies, giving all parties a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments. The list of members can be found on the following website: https://sharedassessments.org/assessment-firms/.

5.1.19.3 Process

Organisations can use the SIG and the AUP both to evaluate their own controls, as well as evaluating that of third party services providers.

The SIG questionnaire requires answering a large number of questions. However, questions that are not related with the activities of the organisation can be omitted. The AUP focusses on an onsite assessment collecting and reporting results.

5.1.19.4 Practice

Organisations having applied the Shared Assessment Program include, but are not limited to, financial institutions, healthcare organisations, energy/utility, retailers, and telecommunications companies.

Between October and December of 2015, EY surveyed 49 global financial services organisations with third-party risk functions in the retail and commercial banking, investment banking, insurance, and wealth and asset management sectors. The purpose of the survey was to address the distinctive nature of managing third-party risk in the financial services industry.

28% of respondents adopted the Shared Assessments program as a framework, up from 24% the year prior. There was a strong correlation between organisations that used Shared Assessments and those that accept a SIG or AUP to reduce or replace assessment efforts.

5.1.19.5 Formal Status

None

5.1.19.6 Relation to other standards / schemes

The controls are annually updated, and are based on referenced industry regulations, guidelines and standards.

5.1.20 ULD Datenschutzaudit

5.1.20.1 Focus

Authorities in Schleswig-Holstein can have their privacy protection system checked and audited in a formal procedure by the ULD. If the process is successful, the authority is awarded an 'ULD Datenschutzaudit' (ULD Data Protection Audit) label. Private companies can be audited too, provided they are part of the data processing system in a public office.

5.1.20.2 Associated Evaluation Scheme and Governance

The goals of the 'Unabhängiges Landeszentrum für Datenschutz' (ULD, Independent State Centre for Data Protection) are:

- Following up all alleged data protection violations and sending the concerned parties a written final assessment.
- Monitoring the processing of data by Schleswig-Holstein authorities; objecting to violations of the data protection law and demanding rectification of defects.
- Advising authorities, corporations and citizens on all data protection issues, for example when setting up new computer systems or when questions arise on the interpretation of data protection law or legislation.

5.1.20.3 Process

The audit is based on a written agreement between the relevant authority and the ULD. This is followed by stocktaking, defining the privacy protection targets, setting up a privacy protection management system and drawing up a privacy policy. If the report from the ULD is successful, a privacy protection audit label is finally awarded for three years.

The costs for the audit are based on the expected personnel expenses. An hourly rate of € 80 per employee is used. Personnel expenses shall be determined before completion of the agreement between the respective authority and the ULD.

5.1.20.4 Practice

In total 32 authorities are listed on the ULD Datenschutzaudit as having obtained the label since 2007.

The European Union currently partly funds the ULD Datenschutzaudit programme as part of its "e-region Schleswig-Holstein" programme. Thanks to this financial support, small and medium-sized enterprises (SME) in the region are being offered an incentive to obtain a Datenschutzaudit. Companies meeting the funding criteria under the "eRegion Schleswig-Holstein" initiative receive a fixed sum to partially offset the costs of the audit. The ULD also provides its standard chargeable services in the certification process free of charge in these cases.

5.1.20.5 Formal Status

None.

5.1.20.6 Relation to other standards / schemes

Although there is no official requirement, using IT products that have obtained an ULD Datenschutz-Gütesiegel (see section 3.1.8) simplifies the process for authorities to obtain an 'ULD Datenschutzaudit' label.

5.2 Standards and schemes for Industry 4.0 and ICS (SWG 3.1)

5.2.1 ANSSI Cybersecurity for Industrial Control Systems

5.2.1.1 Focus

Industrial Control Systems (ICS) today are highly computerised and interconnected with IT systems or the Internet. As such, they are exposed to the same threats, with potentially more serious consequences. The objective is to subject all new critical ICSs to an approval process, thus ensuring that their cybersecurity level is acceptable according to their current threat status and its potential developments.

According to ANSSI, the objective of cybersecurity is to analyse system vulnerabilities (hardware, software, procedures, and human factors) in order to implement measures to limit and be in a position to safeguard the continuity of core business functions to an acceptable extent. Based on this vision ANSSI published guides on Cybersecurity for ICS. The working group on cybersecurity in Industrial Control Systems is composed with actors in the field of automated industrial process control systems and specialists in IT3 Security, and has drafted a set of measures to improve the cybersecurity of ICS4. These guides are pragmatic to help all the stakeholder of the industry to take into account the cybersecurity related issues. They offer a simple and appropriated methodology, illustrated by real situations.

The guides can be found here in English and French: https://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels/

5.2.1.2 Associated Evaluation Scheme and Governance

ANSSI is the national authority in the area of cyber defense and network and information security (NIS) body for France. The mission of ANSSI consists of a broad range of regulatory and operational activities, from issuing regulations and verifying their application, to monitoring, alert and rapid response – particularly on government networks.

Whether ANSSI certifies and / or approves specifically against the ICS guidelines and how is not clear.

5.2.1.3 Process

As the General Security Guidelines (French acronym "RGS") indicate, the guidelines are built upon four pillars that are essential for the good functioning of ICSs:

- Availability: within a context of high productivity, any degradation in availability results directly in financial losses and dissatisfied customers (delivery delays, increased production costs, production down-time, etc.);
- Integrity: compliance in this regard certifies that the products and services provide meet customer or regulatory requirements. For Safety Instrumented Systems (SIS) that protect assets and individuals (for example, safety shutdown systems), this is imperative. Integrity concerns all ICS components, for example PLC programmes, data exchange and SCADA software databases;
- Confidentiality: this is sometimes minimised, but the divulging of a company's information assets can have a very tangible impact on its profits and its future (loss of customers). ICSs contain sensitive parameters and data such a manufacturing formulae, quantities of substances used, system plans, maintenance plans, PLC programs and devices address lists. These can be exploited by competitors or malicious groups to direct targeted attacks or simply to collect data enabling company know-how to be copied;
- Traceability: this is a regulatory requirement in many activity sectors (e.g. food, transport and nuclear industries). Not being able to provide proof of the traceability of operations carried out, materials used and origin of materials, and non-compliance with regulatory requirements may result in legal action being taken against a company.

Under the guidelines all ICSs are classified according to the method described in the Classification Method and Key Measures Guide: https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf

Each class systematically includes the measures of the class below it. Below is a brief description of the three cybersecurity classes for ICSs.

- Class 1: ICSs for which the risk or impact of an attack is low. The measures recommended for this class must be able to be applied in complete autonomy. This class mainly corresponds to rules provided in the ANSSI Healthy Network Guide.
- Class 2: ICSs for which the risk or impact of an attack is significant. There is no state control over this class of ICS, but in the event of inspection or incident, the responsible entity must be able to provide evidence that adequate measures have been implemented.
- Class 3: ICSs for which the risk or impact of an attack is critical. In this class, the obligations are heightened and the conformity of ICSs is verified by the state authority or an accredited body.

For each Class different methods have to be implemented on areas, such as: training, responsibility, and risk analysis (not exhaustive). Find the full list of required methods in the document mentioned above.

Price and duration not found.

5.2.1.4 Practice

Not found.

5.2.1.5 Formal Status

The guidance documents are used to define the methods for applying the measures set out within the framework of French law No. 2013-1168 of 18 December 2013, known as the Military programming law (LPM). The enforcement mechanics around this law are unclear.

5.2.1.6 Relation to other standards / schemes

Technical terms in the guidelines relating to information system security are based on the ISO 27000 standards series and the IGI 1300 (French government standard on classified information). Furthermore, Cybersecurity classes and asset determination is performed according to a level of impact and likelihood. This method is based on terms and concepts found in risk analysis methods such as the EBIOS method.

5.2.2 API STD 1164 (Pipeline SCADA Security)

5.2.2.1 Focus

This API (American Petroleum Institute) standard on SCADA security provides guidance to the operators of oil and gas liquids pipeline systems for managing SCADA system integrity and security.

The API STD 1164 standard is an industry voluntary standard specifically designed to provide the operators with a description of industry practices in SCADA security, and to provide the framework needed to develop sound security practices within the operator's individual companies. Therefore, the use of this standard is not limited to pipelines but should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system. As a voluntary standard, each operator has the liberty to utilise, or not, any and all of the standard within their SCADA system.

The standard provides a means to improve the security of the pipeline SCADA operation by:

- analyzing vulnerabilities of the SCADA system that can be exploited by unauthorised entities,
- listing the processes used to identify and analyze the SCADA system vulnerabilities to unauthorised attacks,
- providing a comprehensive list of practices to harden the core architecture, and
- providing examples of industry best practices.

API 1164 addresses access control, communication security (including encryption), information distribution classification, physical issues (including disaster recovery and business continuity plans), operating systems, network design, data interchange between enterprise and third-party support/customers, management systems, and field devices configuration and local access.

Appendix A in API 1164 contains a checklist guide for evaluating SCADA system security and Appendix B illustrates an example of a security plan for a SCADA control system.

The Appendix A checklist addresses the following areas:

- Authentication
- Change and problem management
- Network connectivity
- Application and database
- Personnel security
- System security audit and review
- Physical security
- Computer, telephone, and network usage
- Information retention/archive/backup
- Information classification and application criticality
- Contractors, vendors, consultants, and third parties.

The security plan in Appendix B comprises sections on identification, documentation, risk analysis, preventive action, oversight, and security management.

5.2.2.2 Associated Evaluation Scheme and Governance

None. The Framework is meant to provide best practices for organisations to implement advance supervisory control and data acquisition (SCADA) cyber security. The standard is maintained by API Standards Department (standards@api.org).

5.2.2.3 Process

Implementation of this standard, to advance supervisory control and data acquisition (SCADA) cyber security, is not a simple process or one-time event, but a continuous process. The overall process could take years to implement correctly depending on the complexity of the SCADA system. Additionally, the process would optimally be started as part of a SCADA upgrade project and use this standard to “design in” security as an element of the new system.

A SCADA security program for the organisation shall be designed to ensure the organisation’s ongoing implementation of industry best practices in cyber security and compliance with all relevant standards. The SCADA security program will identify accountability for all aspects of SCADA security at every organisational level at it scope should include the operator’s organisation, business partners, vendors, and external suppliers of SCADA products and services for the SCADA system.

The SCADA security program should document the SCADA security plan, identify the roles and responsibilities of security professionals and practitioners who will implement policies and procedures, and provide for the coordination of security efforts in the SCADA domain with the cyber security activities of the entire organisation.

5.2.2.4 Practice

Not known.

5.2.2.5 Formal Status

Not known.

5.2.2.6 Relation to other standards / schemes

Not known.

5.2.3 BSI ICS Security Compendium

5.2.3.1 Focus

The Industrial Control Systems (ICSs) Security Compendium provides an overview of several architectural, technical and organisational best practices for the asset owners of ICS. These best practices are a collection of reasonable measures which have proven to be successful in practice on the one hand and, on the other, can be derived from existing standards. Within the following areas best practices are included:

- Security-specific processes / policies
- Selection of the used systems and components as well as of the assigned service providers and integrators
- Constructional and physical securing
- Technical measures

5.2.3.2 Associated Evaluation Scheme and Governance

The ICS Security Compendium also describes a methodology for performing audits in ICS installations. There is, however, no ICS Security Compendium evaluation scheme. The closest to an evaluation scheme is TÜViT providing security checks and penetration tests in order to reduce security vulnerabilities in production infrastructure. TÜViT designed and formulated the ICS Security Compendium upon request from the German Federal Office for Information Security (BSI).

5.2.3.3 Process

The audit process as described by the ICS Security Compendium consists of the following steps:

- Kick-off
- Familiarisation
- Coordination workshop
- Creation of the audit plan
- Checking of documents
- On-site review
- Follow-up of the on-site review
- Creation of the audit report, final presentation

5.2.3.4 Practice

Since there is no official ICS Security Compendium audit, the practice of this standard is not known.

5.2.3.5 Formal Status

None

5.2.3.6 Relation to other standards / schemes

The ICS Security Compendium provides an overview of how the best practices relate to:

- IEC 62443 (see section 3.2.1)
- VDI/ VDE 2182
- NERC CIP (see section 5.3.3)
- DHS Best Practices
- IT-Grundschutz (see section 5.1.7)
- ISO 27001 (see section 5.1.8)

The ICS Security Compendium also refers to ISO 62351 (Power systems management and associated information exchange - Data and communications security), a multi-part specification of security measures for communication protocols in the ICS industry, as developed by IEC.

5.2.4 Catalog of Control Systems Security

5.2.4.1 Focus

The Catalog of Control Systems Security - Recommendations for Standards Developers presents a wide sampling of best practice, guidelines, and security controls for control systems used in many industries. Because this document is not limited to a specific industry sector, it should, therefore, be viewed as a master listing of reference information to be used when reviewing and developing standards for control systems.

The Catalog contains 22 security controls. Examples include: Security policy, Physical and environmental security, Monitoring and reviewing control systems security policy and Risk management and assessment. For each of these security controls, a number of high-level requirements are discussed, including implementation guidance for each requirement.

The recommended controls are designed specifically to provide standards bodies of industry sectors the basic security framework needed to develop sound security standards within each individual industry sector. The recommendations presented in this document are designed to assist in creating the appropriate security program for control system networks with awareness to the threats and vulnerabilities of the enterprise.

5.2.4.2 Associated Evaluation Scheme and Governance

None.

The Catalog of Control Systems Security was developed by the U.S. Department of Homeland Security (DHS).

5.2.4.3 Process

None.

5.2.4.4 Practice

Not publicly accessible.

5.2.4.5 Formal Status

None.

5.2.4.6 Relation to other standards / schemes

The document provides an overview of how all the controls relate to the following standards:

- FIPS 140-2 (see section 3.6.3)
- API 1164 (see section 5.2.2)
- ISO 27001 (see section 5.1.8)
- ISA/IEC 62443 (see section 5.2.6)
- NERC CIP 002 to 009 (see section 5.3.3)
- NIST SP 800-53 (see section 5.2.7)

5.2.5 ICS-CERT assessments

5.2.5.1 Focus

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The following sectors are considered to be critical:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector

- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Sector-Specific Agencies
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

The ICS-CERT Assessments are focused on two different areas:

- Design Architecture: focusing on the underlying ICS network architecture, integration of Information Technology (IT) and Operational Technology teams, vendor support, monitoring, cyber security controls, and all internal and external connections.
- Network Architecture: focusing on the underlying ICS network architecture, integration of Information Technology (IT) and Operational Technology teams, vendor support, monitoring, cyber security controls, and all internal and external connections.

5.2.5.2 Associated Evaluation Scheme and Governance

ICS-CERT offers two different evaluation schemes:

- ICS-CERT's Design Architecture Review (DAR) provides critical infrastructure asset owners and operators with a comprehensive technical review and cyber evaluation of the architecture and components that comprise their industrial control systems (ICS) operations.
- ICS-CERT's Network Architecture Verification and Vali-dation (NAVV) is a passive analysis of network traffic occurring within the ICS network.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates within the National Cybersecurity and Integration Center (NCCIC), a division of the Department of Homeland Security's Office of Cybersecurity and Communications (DHS CS&C). NCCIC/ICS-CERT is a key component of the DHS Strategy for Securing Control Systems. The primary goal of the Strategy is to build a long-term common vision where effective risk management of control systems security can be realised through successful coordination efforts.

5.2.5.3 Process

- Design Architecture Review (DAR)
- During this 2-3 day review the ICS-CERT assessment team evaluate the architecture and processes, with a focus on three key areas:
    - ICS Network Architecture
    - Asset Inventory
    - Protective and Detective Controls
- Network Architecture Verification and Validation (NAVV)

- Using a combination of both open-source and commercially available tools, ICS-CERT presents a strategic visualisation of the network traffic and device-to-device communications that are occur-ring within ICS network segments.
- The ICS-CERT's assessment team evaluates network traffic, reviewing:
    - Protocol hierarchy and organisation of network traffic;
    - Device to Device communications—including iden-tification of "top-talkers" and the devices generating the most traffic;
    - Communications traversing (or attempting to traverse) the ICS network boundary—for verification that the perimeter protections are functioning as intended;
    - Potentially misconfigured devices—or those exhib-iting suspicious or anomalous behavior;
    - ICS protocol analysis—including an in-depth review of function codes and control parameters that are observed within the captured traffic.

Upon completion of the assessment process, ICS-CERT will compile an in-depth report for the asset owner, including a prioritised analysis of key discoveries and practical mitigations for enhancing the organisation's cybersecurity posture.

Because ICS-CERT's DAR and NAVV services are based on Con-gressional funding, they are available as an onsite facilitated assessment for critical infrastruc-ture asset owners and operators at no cost. Upon completion of the process, ICS-CERT will compile an in-depth report for the asset owner, including a prioritised analysis of key discoveries and practical mitigations for enhancing the organisation's cyber security posture.

5.2.5.4 Practice

Not available.

5.2.5.5 Formal Status

None.

5.2.5.6 Relation to other standards / schemes

None.

5.2.6 ISA/IEC 62443 (Security for Industrial Automation and Control Systems)

5.2.6.1 Focus

The ISA/IEC 62443 standard is an international standard for security of the industrial automation and control systems in the operational technology domain. The standard was initiated by the International Society of Automation (ISA) and is carried worldwide and being further developed by the IEC.

The standard applies all types of plants, facilities and systems in all industries, including:

- Hardware and software systems such as Distributed Control Systems (DCS), Programmable Logic Controllers (PLC) and Supervisory Control And Data Acquisition (SCADA) systems.
- Associated interfaces, APIs or HMIs used to provide control, safety and manufacturing operations.
- Continuous, batch and discrete processing systems.

The ISA/IEC 62433 standard consists of a number of parts, which are arranged in four groups, corresponding to the primary focus and intended audience:

- General – This group includes parts that address topics that are common to the entire series.
- Policies and Procedures – Parts in this group focus on the policies and procedures associated with IACS security.
- System Requirements – The parts in this group address requirements at the system level.
- Component Requirements – The fourth and final group includes elements that provide information about the more specific and detailed requirements associated with the development of IACS products.

The overview in Figure 1 provides more information on the topic and current status of each part of ISA/IEC 62443.

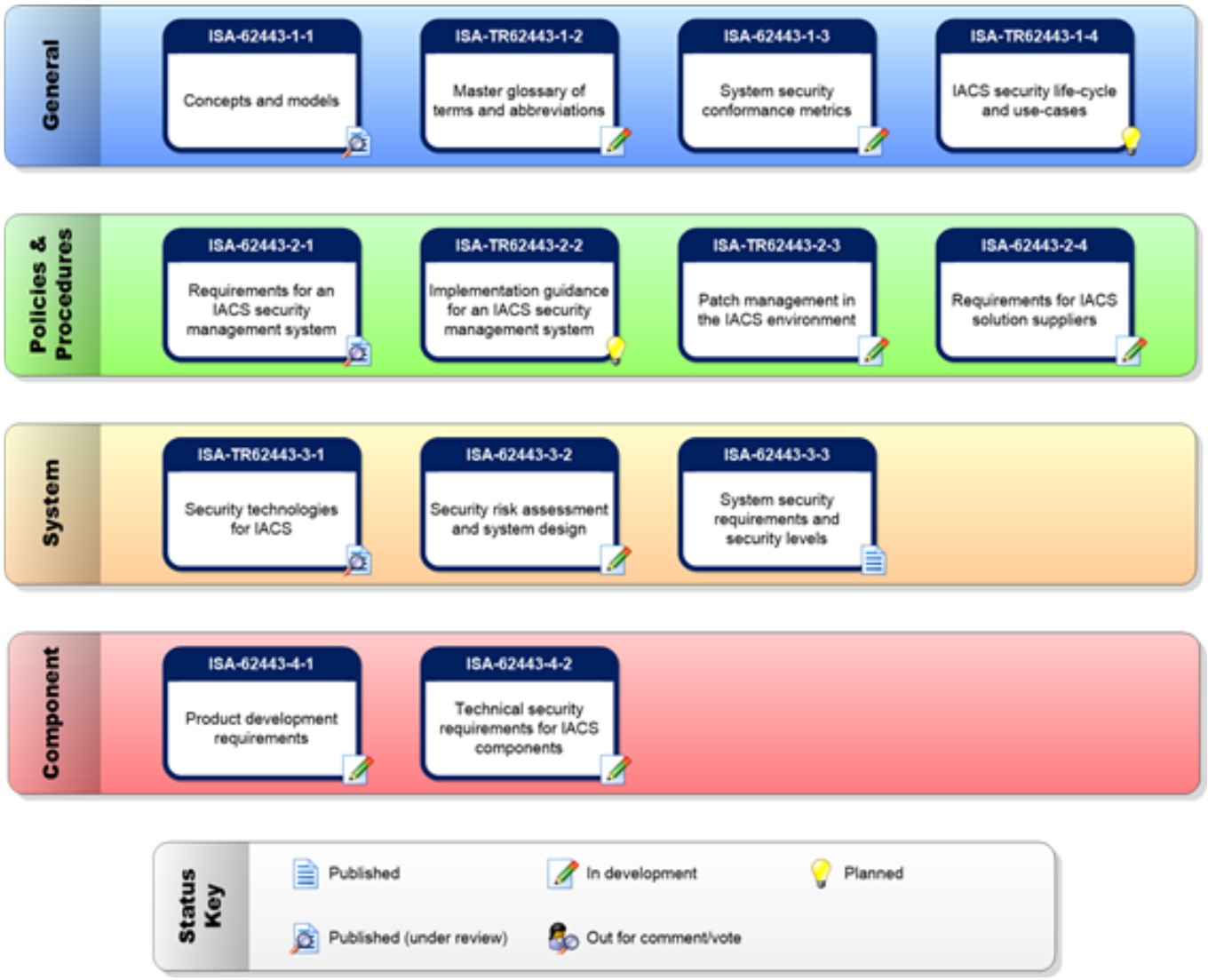


Figure 1 ISA/IEC 62443 parts overview

As can be seen, some of these standards are Technical Reports, which means they are not formal standards and do not contain binding requirements

5.2.6.2 Associated Evaluation Scheme and Governance

The IECEE is a multilateral certification system based on International Standards prepared by the IEC. Its members use the principle of mutual recognition of test results to obtain certification or approval at national levels around the world.

The IECEE has an active Task Force Cyber Security, which is working towards a unique approach for conformity assessment to the IEC 62443 series. A guidance Operational Document has been published to describe how the conformity assessment can be handled; this document can be found at http://www.iecee.org/search/?q=62443. It shows that IECEE intends to have separate certification processes for Processes, Products and Solutions, and for each offers two assessment scenarios:

- Scenario 1 – Capability Assessment: An assessment of a set of capabilities typically described in a plan or set of policies / procedures
- Scenario 2 – Application of Capabilities Assessment: Use of a Scenario 1 capability for a specific product or solution

Note: The ISA Security Compliance Institute (ISCI) also offers a certification program for organisations against ISA/IEC 62443. This ISASecure organisation process certification is meant for product development organisations. The Security Development Lifecycle Assurance (SDLA) certification promotes security development lifecycle practices intended to improve the quality of security in IAC systems. For more information on ISCI, see section 3.2.1.2.

5.2.6.3 Process

The applicant is responsible for both identifying the standards within the IEC 62443 series to be utilised in their assessment and for selecting the specific security requirements from the identified standards that are to be evaluated within the scope of the assessment. It is not required to select all security requirements from the identified standard. The Applicant selects the specific requirements for which they are requesting to be assessed. In addition, the Applicant may be required to identify the product(s) or solution to which the assessment applies.

As part of the submittal, the Applicant completes the applicable portions of a Test Report Form (TRF) and additionally provides evidence in support of the capabilities that are intended to demonstrate compliance to the selected requirement(s). Each selected IEC 62443 security requirement is evaluated against the supporting evidence supplied by the applicant.

5.2.6.4 Practice

As of February 2017, the IECEE conformance assessment to IEC 62443 was not yet active.

Note that the ISCI certification program is already active; see section 3.2.1.4.

5.2.6.5 Formal Status

None.

5.2.6.6 Relation to other standards / schemes

The ISA/IEC 62443 series builds on established standards for the security of general purpose information technology systems (e.g., the ISO/IEC 27000 series), identifying and addressing the important differences present in Industrial Automation and Control Systems (IACS). Many of these differences are based on the reality that cyber security risks with IACS may have Health, Safety or Environment (HSE) implications and the response should be integrated with other existing risk management practices addressing these risks.

The ISA/IEC 62443 series also refers to ISO/IEC 62351 (Power systems management and associated information exchange - Data and communications security), a multi-part specification of security measures for communication protocols in the ICS industry, as developed by IEC.

5.2.7 NIST SP 800-82 (Guide to Industrial Control Systems (ICS) Security)

5.2.7.1 Focus

Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures.

- SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralised data acquisition and control are critical to system operation. They are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems.
- DCS are used to control industrial processes such as electric power generation, oil refineries, water and wastewater treatment, and chemical, food, and automotive production. DCS are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated sub-systems that are responsible for controlling the details of a localised process.
- PLCs are computer-based solid-state devices that control industrial equipment and processes. While PLCs are control system components used throughout SCADA and DCS systems, they are often the primary components in smaller control system configurations used to provide operational control of discrete processes such as automobile assembly lines and power plant soot blower controls.

The purpose of the NIST 800-82 is to provide guidance for securing industrial control systems (ICS) through:

- The development and deployment of an ICS security program
    - Obtain senior management buy-in
    - Build and train a cross-functional team
    - Define charter and scope
    - Define specific ICS policies and procedures
    - Define and inventory ICS assets
    - Perform a risk and vulnerability assessment
    - Define the mitigation controls
    - Provide training and raise security awareness for ICS staff.
- Integrating security into network architectures
    - Firewalls
    - Network structure
- The implementation of the Security Controls from NIST SP 800-53
    - Management Controls
    - Operational Controls
    - Technical Controls

5.2.7.2 Associated Evaluation Scheme and Governance

There is no evaluation scheme. The document serves as a guide and should not be used purely as a checklist to secure a specific system. Readers are encouraged to perform a risk-based assessment on their systems and to tailor the recommended guidelines and solutions to meet their specific security, business and operational requirements.

This publication has been developed by NIST. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems,

5.2.7.3 Process

None.

5.2.7.4 Practice

The guide may be used by nongovernmental organisations on a voluntary basis, but the guide has been prepared for use by federal agencies.

5.2.7.5 Formal Status

None.

5.2.7.6 Relation to other standards / schemes

The ICS overlay is a partial tailoring of the controls and control baselines in SP 800-53, Revision 4, and adds supplementary guidance specific to ICS.

5.3 Standards and schemes for energy networks and smart grids (SWG 3.2)

5.3.1 Cybersecurity Capability Maturity Model

5.3.1.1 Focus

The C2M2 is aimed at Cybersecurity for Critical Energy Infrastructure. It focusses on practices within ten key domains that contribute to the overall cyber security posture of an organisation. These domains are:

- Risk Management
- Asset, change, and configuration management
- Identity and access management
- Threat and vulnerability management
- Situational Awareness
- Information sharing and communications
- Event and incident response, continuity of operations

- Supply chain and external dependencies management
- Workforce management
- Cybersecurity program management

5.3.1.2 Associated Evaluation Scheme and Governance

The C2M2 program is comprised of three cybersecurity capability maturity models:

- The Cybersecurity Capability Maturity Model
- The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
- The Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)

The ES-C2M2 and ONG-C2M2 models are energy sector-specific versions that include the core C2M2 as well as additional reference material and implementation guidance specifically tailored for the electricity and oil and natural gas segments of the energy sector.

The Cybersecurity Capability Maturity Model (C2M2) was derived from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) version 1.1 by removing sector-specific references and terminology. The ES-C2M2 was developed in support of a White House initiative led by the Department of Energy (DOE), in partnership with the Department of Homeland Security (DHS), and in collaboration with private- and public-sector experts.

5.3.1.3 Process

A team of DOE employees will visit the organisation and will conduct interviews with relevant employees that have management level knowledge of their function/department.

The different stakeholders will be asked to answer questions relevant to their functions. The C2M2 has over 300 questions in total which will generate dialogue between the participants and help the stakeholders understand the maturity of the cybersecurity capabilities.

The model provides maturity indicator levels (MILs) designed to discuss an organisation's operational capabilities and management of cybersecurity risk during both normal operations and times of crises.

However, the C2M2 can also be conducted as a self-evaluation following the Facilitator Guide which is available on the following website: https://www.energy.gov/oe/downloads/cybersecurity-capability-maturity-model-facilitator-guide-february-2014.

5.3.1.4 Practice

Not available.

5.3.1.5 Formal Status

None.

5.3.1.6 Relation to other standards / schemes

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cybersecurity standards provide specific requirements that apply to the bulk power system; see section 5.3.3. The NERC CIP standards were used as a reference when the C2M2 was developed. Although it is anticipated that entities subject to compliance with NERC CIP standards would use this model, compliance requirements are not altered in any way by this model.

The C2M2 is also related to the Framework for Improving Critical Infrastructure Cybersecurity released by The National Institute of Standards and Technology (NIST). A map of this framework and the C2M2 can be found in the following document: https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

5.3.2 ISO/IEC 27019 (Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry)

5.3.2.1 Focus

ISO/IEC 27019 provides guiding principles based on ISO/IEC 27002 for information security management applied to process control systems as used in the energy utility industry. The aim of ISO/IEC 27019 is to extend the ISO/IEC 27000 set of standards to the domain of process control systems and automation technology. This allows the energy utility industry to implement a standardised information security management system (ISMS) in accordance with ISO/IEC 27001 that extends from the business to the process control level.

The scope of ISO/IEC 27019 covers process control systems used by the energy utility industry for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes. This includes in particular the following systems, applications and components:

- The overall IT-supported central and distributed process control, monitoring and automation technology as well as it systems used for their operation, such as programming and parameterisation devices
- Digital controllers and automation components such as control and field devices or PLCs, including digital sensor and actuator elements
- All further supporting it systems used in the process control domain, e.g. for supplementary data visualisation tasks and for controlling, monitoring, data archiving and documentation purposes
- The overall communications technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology
- Digital metering and measurement devices, e.g. For measuring energy consumption, generation or emission values
- Digital protection and safety systems, e.g. protection relays or safety PLCs
- Distributed components of future smart grid environments
- All software, firmware and applications installed on above mentioned systems

5.3.2.2 Associated Evaluation Scheme and Governance

There is no related evaluation scheme.

However, see section 5.1.8.2 on the governance of ISO 27001.

5.3.2.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

5.3.2.4 Practice

The ISO survey (see section 5.1.8.4) does not give information on ISO 27019 separately, and an exact number therefore cannot be given.

5.3.2.5 Relation to other standards / schemes

The guidelines of ISO/IEC 27019 are based upon ISO/IEC 27002 (

ISO

5.3.3 NERC CIP 002-009

5.3.3.1 Focus

The North American Electric Reliability Corporation (NERC) is a nonprofit corporation whose major responsibilities include working with all stakeholders to develop standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient.

NERC maintains the Critical Infrastructures Protection (CIP) standards. CIP standards 002 through 009 address the security of cyber assets essential to the reliable operation of the electric grid.

5.3.3.2 Associated Evaluation Scheme

5.3.3.2.1 Audits

The NERC Compliance Operations department is responsible for the development and implementation of a compliance monitoring program to promote the reliability of the bulk energy system. To help fulfill its responsibilities NERC delegated certain responsibilities to eight qualified Regional Entities to monitor and enforce compliance of registered entities with NERC Reliability Standards.

The Regional Entities utilise several methods to carry out their compliance functions, including regularly scheduled compliance audits, spot checks, and self-certifications. NERC seeks to ensure consistency and fairness among the various Regional Entity programs. NERC carries out

its oversight and monitoring activities through the Compliance Monitoring and Enforcement Program (CMEP), including:

- Annual reviews of the Regional Entity implementation plans;
- Oversight audits on select registered entity audits;
- Annual assessments of select NERC Reliability Standards for consistency of approach
- Compliance Analysis Reports (CARs); and
- Audits of registered entities.

5.3.3.2.2 Sufficiency Review Program

The NERC's Sufficiency Review Program (SRP) provides a review of a registered entity's security program, including both physical security and cybersecurity. Since the inception of the SRP, NERC has conducted more than 30 SRP visits, which are voluntary and conducted in a non-audit environment. No content from those discussions may be used during a subsequent audit or compliance action unless it represents an imminent threat to the BES. NERC staff, Regional Entity representatives, and outside consultants sign nondisclosure agreements (NDAs) to ensure strict confidentiality of all discussions and materials. The discussions held during an SRP visit are educational to registered entity, NERC, and Regional Entity staffs and are intended to equally support infrastructure security efforts and compliance with the CIP standards. Key goals of an SRP visit are to increase the focus on future activities and issues related to compliance initiatives within the CIP standards and to focus on security initiatives at registered entities.

5.3.3.2.3 Self-Reports

Registered Entities are encouraged to submit a Self-Report any time an instance of non-compliance with a reliability standard is self-identified.

5.3.3.3 Governance

Within NERC, the Critical Infrastructure Protection Committee (CIPC) is responsible for maintaining the CIP standards. New versions of these standards are regularly published. In order to ensure a smooth transition from one version of a standard to the next, NERC creates Implementation Plans.

5.3.3.4 Process

Registered entities are subject to regular audits by the NERC's delegated Regional Entities; see above. Self-certification is allowed, but are typically limited in scope and include instructions on how to perform the self-assessment, what evidence to collect and review, and what information to communicate to the Regional Entity. In some situations, guided Self-Certifications are also administered in place of a Compliance Audit for lower risk standards and requirements.

5.3.3.5 Practice

Because of their formal status (see below), the NERC CIP standards are quite actively used. According to the NERC website, over 200 registered entities must comply with these standards. There is a large body of information, tools, checklists etc. available, both from NERC and from third-party companies, to help registered entities to pass the NERC CIP audits.

5.3.3.6 Formal Status

In 2007, the US Federal Energy Regulatory Commission (FERC) designated NERC as the Electric Reliability Organisation (ERO) to develop and enforce compliance with mandatory reliability standards in the United States. Upon FERC's approval, NERC's Reliability Standards became mandatory within the United States for Bulk Electric System. These mandatory Reliability Standards include CIP standards 001 through 009. Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards to accomplish NERC's mission of ensuring the security and reliability of the electric grid.

5.3.3.7 Relation to other standards / schemes

In its 'Roadmap to Achieve Energy Delivery Systems Cybersecurity', NERC refers to a number of standards and schemes, such as:

- API STD 1164 (Pipeline SCADA Security), see section 5.2.2.
- IEEE 1686 (Substation IEDs Cybersecurity), see section 3.3.1.
- NIST SP 800-82 (Guide to ICS Security), see section 5.2.7.
- NIST SP 800-53: (Security and Privacy Controls for Federal Information Systems and Organizations), see section 5.6.3.
- ISO/IEC 62351 (Power systems management and associated information exchange - Data and communications security), a multi-part specification of security measures for communication protocols in the ICS industry, as developed by IEC.

5.3.4 NIST IR 7628 (Guidelines for Smart Grid Cybersecurity)

5.3.4.1 Focus

This three-volume report, Guidelines for Smart Grid Cybersecurity, presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities.

The Guidelines report is a companion document to the NIST Framework and Roadmap for Smart Grid Interoperability Standards (NIST SP-1108). SP-1108 describes a high-level conceptual reference model for the Smart Grid, identifies standards that are applicable (or likely to be applicable) to the ongoing development of an interoperable Smart Grid, and specifies a set of high-priority standards-related gaps and issues.

The guidelines are intended primarily for individuals and organizations responsible for addressing cyber security for Smart Grid systems and the constituent subsystems of hardware and software components.

- The first volume describes the approach, including the risk assessment process to identify the high-level security requirements. These requirements are sorted into 19 groups ('families with similar objectives'). Examples include Access Control, Awareness and Training, Incident Response and Smart Grid Information System and Information Integrity. The first volume concludes with a discussion of technical cryptographic and key management issues across the scope of Smart Grid systems and devices.

- The second volume provides awareness and discussion of topics regarding privacy issues. Additionally, the second volume provides recommendations, based on widely accepted privacy principles, for entities that participate within the Smart Grid.

- The third volume is a compilation of supporting analyses and references used to develop the high-level security requirements and other tools and resources presented in the first two volumes.

5.3.4.2 Associated Evaluation Scheme and Governance

None.

This publication has been developed by the U.S. National Institute of Standards and Technology (NIST), which is part of the U.S. Department of Commerce. Amongst its activities is to develop (IT) standards and guidelines to stimulate innovation, foster industrial competitiveness, and improve the quality of life.

5.3.4.3 Process

None.

5.3.4.4 Practice

Not publicly accessible.

5.3.4.5 Formal Status

None.

5.3.4.6 Relation to other standards / schemes

The document shows the relation of the requirements in the NIST IR 7628 with those in NIST SP 800-53 (see section 5.6.3), DHS Catalog of Control Systems Security (see section 5.2.4), and the NERC CIP standard (see section 5.3.3).

5.4 Standards and schemes for transportation (road, rail, air, sea) (SWG 3.3)

5.4.1 RTCA DO-326A (Airworthiness Security Process Specification)

5.4.1.1 Focus

The guidance of this document is intended to augment current guidance for aircraft certification to handle the information security threat to aircraft safety. It adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification.

The document is the first of a series of documents on Aeronautical Systems Security that together will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. It addresses only Aircraft Type Certification. Because of the impending introduction of aircraft with significant security-related features, this document addresses immediate concerns and establishes feedback on its implementation challenges.

5.4.1.2 Associated Evaluation Scheme and Governance

There is no DO-326A certificate, however, the DO-326A standard may be part of the airworthiness certification of airplanes. Before a newly developed aircraft model may enter into operation, it must obtain a type certificate from the responsible aviation regulatory authority. In Europe the EASA is responsible for the certification of aircraft and this certificate testifies that the type of aircraft meets the safety requirements set by the European Union. This certification process runs parallel witht that of other authorities such as the FAA for the US or TCCA for Canada. Conversely, EASA will validate the FAA certification of US aircraft models (or TCCA certification of Canadian models) according to applicable Bilateral Aviation Safety Agreements between the EU and the concerned Third Country.

5.4.1.3 Process

The certification process of the EASA is as follows:

- Technical Familiarisation and Certification Basis

  The aircraft manufacturer presents the project to EASA when it is considered to have reached a sufficient degree of maturity. The EASA certification team and the set of rules that will apply for the certification of this specific aircraft type are being established (Certification Basis).

- Establishment of the Certification Programme

  EASA and the manufacturer need to define and agree on the means to demonstrate compliance of the aircraft type with each requirement of the Certification Basis. This goes hand in hand with the identification of EASA's "level of involvement" during the certification process.

- Compliance demonstration

  The aircraft manufacturer must demonstrate compliance of its product with regulatory requirements: the structure, engines, control systems, electrical systems and flight performance are analysed against the Certification Basis. This compliance demonstration is done by analysis during ground testing (such as tests on the structure to withstand bird strikes, fatigue tests and tests in simulators) but also by means of tests during flight. EASA experts perform a detailed examination of this compliance demonstration, by means of document reviews in their offices in Cologne and by attending some of these compliance demonstrations (test witnessing).

- Technical closure and issue of approval

If technically satisfied with the compliance demonstration by the manufacturer, EASA closes the investigation and issues the certificate.

5.4.1.4 Practice

All airplanes need to be certified by the EASA. To what extent the standards of DO-326A are included is unclear.

5.4.1.5 Formal Status

See section on Practice.

5.4.1.6 Relation to other standards / schemes

DO-326A is issued in parallel with DO-355 to address developmental and continuing airworthiness concerns.

5.4.2 SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems) & ISO-SAE 21434 AWI (Road Vehicles – Cybersecurity Engineering)

5.4.2.1 Focus

Both the ISO-SAE AWI 21434 and the SAE J3061 standards describe the process of cybersecurity engineering for ground vehicles (SAE) respectively road vehicles (ISO). They structure their recommended security related process steps in frameworks. Those frameworks are similar to the frameworks in the established ISO 26262 standard for functional safety management.

5.4.2.1.1 ISO-SAE AWI 21434 Road vehicles – Cybersecurity engineering

ISO-SAE AWI 21434 is still in preparation, with a planned publication in October 2019. The aim of the standard is to standardise the cybersecurity engineering process and to be the cybersecurity pendant to the ISO 26262 standard for functional safety management. The document specifies requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (e.g. concept, design, development), production, operation, maintenance, and decommissioning.

A framework is defined that includes requirements for a cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders.

This document is applicable to road vehicles that include electrical and electronic (E/E) systems, their interfaces and their communications.

This document does not prescribe specific technology or solutions related to cybersecurity.

It is planned that the J3061 will be retrieved after publication of this standard.

5.4.2.1.2 SAE J3061 – Security Guidebook for Cyber-Physical Vehicle Systems

The SAE J3061 wants to recommend practice in the engineering process of Cybersecurity products in the automotive context and is mirroring the structure of ISO 26252. By that it does tightly couple itself with safety. The document claims to be goal oriented by combining general management, project management and engineering aspects into one process flow. Besides the safety aspects, the recommendations of the SAE J3061 is aggregated from several research projects with a mainly theoretical background.

The framework of SAE J3061 considers the entire life-cycle of the development of Cybersecurity related products from concept phase through production, and operation. The production related phases are companied by management and supporting processes. The core product development follows the V-Model and is segmented in system-, hardware-, and software-levels. The entire Framework is based on the ISO 26262 standard for automotive safety.

Management activities should include overall needed aspects, like, e.g. to build a security culture in the organisation or to establish methods. Whereas supporting processes include activities that are applicable across different life-cycle phases (e.g. configuration management, change management etc.)

5.4.2.2 Associated Evaluation Scheme and Governance

Not given yet for the ISO-SAE AWI 21434. The J3061 is a guidebook that summarise activities around the engineering process. Thus, an evaluation scheme is not applicable.

5.4.2.3 Process

None.

5.4.2.4 Practice

The ISO-SAE AWI 21434 is currently in negotiation and thus not public available yet. The standard is expected to be published in October 2019.

5.4.2.5 Formal Status

None.

5.4.2.6 Relation to other standards / schemes

ISO 26262, Common criteria, ISO 31000

5.4.3 The Guidelines on Cyber Security onboard Ships

5.4.3.1 Focus

As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are increasingly being networked together – and more frequently connected to the worldwide web. The aim of ‘The Guidelines on Cybersecurity onboard Ships’ is to offer guidance

to ship owners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems onboard their ships.

5.4.3.2 Associated Evaluation Scheme and Governance

The Guidelines are designed to develop understanding and awareness of key aspects of cybersecurity. The Guidelines are not intended to provide a basis for auditing or vetting the individual approach to cyber security taken by companies and ships.

5.4.3.3 Process

None.

5.4.3.4 Practice

Not known.

5.4.3.5 Formal Status

None.

5.4.3.6 Relation to other standards / schemes

Existing international standards and guidelines, for example the ISO/IEC 27000 series of Information Security Management Systems (ISMS) standards, cover cyber security issues for shoreside operations – whereas these Guidelines focus on the unique issues facing the shipping industry onboard ships.

5.5 Standards and schemes for financial services and insurance (SWG 3.4)

5.5.1 BITS Software Assurance Framework

5.5.1.1 Focus

The BITS Software Assurance Framework was created in 2012 by the Financial Services Roundtable to document the importance of secure development practices and to provide guidelines that financial services organisations can use to implement these practices more fully. BITS, a part of the Financial Services Roundtable, is made up of major US financial institutions. The Software Assurance Framework was developed to help financial institutions better follow secure development practices and avoid malicious attacks, theft of customer data and even corporate assets.

The Framework is rooted in education, integration of security in design using standards and threat modeling, best practices for coding, focused and comprehensive testing and followed with important implementation and response practices. The Framework was developed in

collaboration with Microsoft, and integrates the Microsoft Security Development Lifecycle at the foundation.

5.5.1.2 Associated Evaluation Scheme and Governance

None. The Framework is meant to be implemented by organisations, but apparently without any defined possibility to claim conformance.

The standard is maintained by BITS, a division of the Financial Services Roundtable.

5.5.1.3 Process

Not applicable.

5.5.1.4 Practice

Not known.

5.5.1.5 Formal Status

None.

5.5.1.6 Relation to other standards / schemes

Not known.

5.5.2 CBEST

5.5.2.1 Focus

CBEST is a framework for developing intelligence-led cyber threat vulnerability tests against financial institutions' critical systems. The CBEST tests mimic actions of groups and individuals who are perceived by the government and commercial threat intelligence providers as posing a genuine threat to systemically-important financial institutions within the Critical National Infrastructure.

5.5.2.2 Associated Evaluation Scheme and Governance

To support the boards of financial firms, infrastructure providers, and regulators in improving the understanding of the types of cyber-attack that could undermine the financial stability in the UK, and the extent to which the UK financial sector is vulnerable to those attacks, CBEST has been devised by the UK Financial Authorities in conjunction with CREST (the Council for Registered Ethical Security Testers) and Digital Shadows. Only CBEST member companies are accredited to perform a CBEST on a UK financial institution.

5.5.2.3 Process

The CBEST assessment process consists of four phases of work:

- the Initiation Phase during which the CBEST assessment is formally launched, the scope is established and threat Intelligence and penetration testing (TI/PT) service providers are procured;
- the Threat Intelligence Phase during which the core threat intelligence deliverables are produced, threat scenarios are developed into a draft Penetration Test Plan, threat intelligence capability is assessed and control is handed over to the PT service provider;
- the Penetration Testing Phase during which an intelligence-led penetration test against the target systems and services that underpin each Critical Function in scope is planned, executed and reviewed and detection and response capabilities are assessed;
- the Closure Phase during which: the Bank of England Sector Cyber Team (SCT) produces its Intelligence, Detection and Response Report, the Firm/Financial Market Infrastructure's Remediation Plan is finalised, the TI/PT service providers are debriefed, and the Regulator supervises the execution of the Remediation Plan.

5.5.2.4 Practice

At this point in time (3rd of February 2017) the UK Financial Authorities have only made CBEST available to firms and Financial Market Infrastructures (FMIs) which they consider to be core to the UK financial system.

5.5.2.5 Formal Status

The view of the UK Financial Authorities is that CBEST continues to be a voluntary program.

5.5.2.6 Relation to other standards / schemes

An accreditation under the CREST STAR scheme (see section 5.12.1) is a prerequisite for membership in the CBEST scheme. Only CBEST member companies are accredited to perform a CBEST on a UK financial institution.

5.5.3 ISO/IEC 27015 (Information security management guidelines for financial services)

5.5.3.1 Focus

ISO/IEC TR 27015 provides information security guidance complementing and in addition to information security controls defined in ISO/IEC 27002. This guidance is intended for initiating, implementing, maintaining, and improving information security within organizations providing financial services.

5.5.3.2 Associated Evaluation Scheme and Governance

There is no related evaluation scheme.

However, see section 5.1.8.2 on the governance of ISO 27001.

5.5.3.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

5.5.3.4 Practice

The ISO survey (see section 5.1.8.4) does not give information on ISO 27015 separately, and an exact number therefore cannot be given.

5.5.3.5 Relation to other standards / schemes

The guidelines of ISO/IEC 27015 are based upon ISO/IEC 27002 (see section 5.1.9).

5.6 Standards and schemes for public services / eGovernment / digital citizenship (SWG 3.5)

5.6.1 Application Security and Development Security Technical Implementation Guide (STIG)

5.6.1.1 Focus

The Application Security and Development (ASD) Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems.

The Application Security and Development STIG is designed to be applied to all enterprise applications connected via the network. This includes client applications installed on desktop computers which establish network connections to remote systems, HTML and browser-based applications comprised of numerous web technologies and architectures including Java, JavaScript, .NET, Cloud, RESTful-based, and SOA-oriented web services.

The ASD STIG contains 290 rules and requirements, covering aspects including:

- Application code
- Web server(s)
- Database server(s)
- Directory and authentication device(s) (e.g., Windows domain controllers, RADIUS, etc.)
- Firewall(s)
- Network and enclave configuration required to support the application
- Operating system platforms for any of the above

The full list of requirements can be viewed by:

- Downloading the STIG reader from
    - http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx

- Downloading the latest ASD STIG from
    - http://iase.disa.mil/stigs/Pages/a-z.aspx

5.6.1.2 Associated Evaluation Scheme and Governance

Products that fulfil the STIG requirements may be placed, after testing, on the Department of Defense Information Network (DoDIN) Approved Product List (APL).

The DoDIN APL process is managed by the Defense Information Systems Agency (DISA) Infrastructure Directorate (IE) Approved Products Certification Office (APCO). The APCO acts as the staff element for DISA IE to manage the APL. The APCO provides process guidance, coordination, information, and support to government Sponsors and Vendors throughout the entire process - from the registration phase to the attainment of APL status.

Other parties involved in the process are:

- A Certification Authority (CA), which is an entity authorized by the External Certifying Authority (ECA) Policy Management Authority (part of the DoD), to create, sign, and issue public key certificates. ECA vendors that have been approved are: Operational Research Consultants, Symantec and IdenTrust.
- The Joint Interoperability Test Command (JITC) is DoD's Joint Interoperability Certifier and only non-Service Operational Test Agency for Information Technology (IT)/National Security Systems (NSS). JITC provides risk based Test Evaluation & Certification services, tools, and environments.

5.6.1.3 Process

The process to get a product listed on the APL is as follows:

1. The vendor needs to obtain government sponsorship, which can be any DoD Component user of the DISN with acquisition or management-level responsibilities of equipment can sponsor a product for testing. The sponsor will support the vendor throughout the process and needs to agree to the configuration and device type submitted by the Vendor.
2. The vendor needs to submit a request of testing, together with the required documentation to the APCO.
3. The product is then assigned a tracking number, test lab, Testing Action Officer (AO), and JITC AO.
4. The Testing AO coordinates scheduling of the Initial Contact Meeting (ICM). Required ICM attendees include the Vendor, Sponsor, Testing and JITC AO, Certifying Authority (CA) representative, and APCO. The outcome of the ICM will be:
    - The assignment of a Unified Capabilities Requirements (UCR) device type
    - Agreement on applicable UCR requirements
    - Business model determination
    - SUT configuration
    - Cybersecurity and IO requirements (finalized STIGs and UCR LoC templates)
    - Test location
    - Products included by similarity (if applicable)
    - Certification document deliverables
    - Confirm test dates (if available)

5. Based upon the outcome of the ICM a testing plan will be developed. Once testing is completed and the product is approved, the APCO will notify Testers, Sponsors, and Vendors and the product will be placed on the APL website

5.6.1.4 Practice

The list of approved products can be found on: http://iase.disa.mil/stigs/app-security/Pages/index.aspx and https://aplits.disa.mil/processAPList.action

5.6.1.5 Formal Status

The DoDIN APL is the single approving authority for all Military Departments (MILDEPs) and Department of Defence (DoD) agencies in the acquisition of communications equipment that is to be connected to the Defense Information Systems Network (DISN).

5.6.1.6 Relation to other standards / schemes

DISA considered all the applicable technical NIST SP 800-53 requirements (see section 5.6.3) while developing this STIG.

5.6.2 National Security Framework (Esquema Nacional de Seguridad - ENS)

5.6.2.1 Focus

The Spanish National Security Framework (ENS or NSF) covers the basic principles, minimum requirements and security measures to be applied by the public sector in Spain. The Framework was developed using state-of-the-art methodologies concerning information security.

The main goals pursued by this framework are the following:

- To create the necessary conditions of trust, through measures to ensure IT security for the exercise of rights and the fulfillment of duties through the electronic access to public services.
- To promote the continuous management of security, regardless of the impulses of the moment or lack thereof.
- To promote best practices for prevention, detection and reaction.
- To provide a common language, concepts and elements of security andto provide guidance to public administrations in the implementation of ICT security.
- To enable cooperation to deliver e-government services.
- To facilitate the interaction between public administrations. The NSF complements the National Interoperability Framework.
- To facilitate the communication of security requirements to industry. This ensures that industry finds that all public administrations speak the same language.

The National Security Framework foresees a series of so-called Technical Security Instructions, which provide more detailed information on:

a) reporting on the security status

b) notification of security incidents
c) performing security audits
d) achieving compliance with the National Security Framework.
e) acquisition of security products.
f) application of cryptography in the National Security Framework.
g) achieving interoperability in the National Security Framework.
h) safety requirements in outsourced environments.

5.6.2.2 Associated Evaluation Scheme and Governance

Public sector organisations in Spain and private sector service providers can be certified against the National Security Framework by independent certification bodies. These certification bodies should be accredited against ISO/IEC 17065 by ENAC (Entidad Nacional de Acreditación – The National Accreditation Entity). ENAC is the body appointed by the Spanish government to act as the sole accreditation body in Spain.

5.6.2.3 Process

The Technical Security Instruction of Compliance with the National Security Framework establishes the criteria and procedures for the determination of compliance with the ENS and for the advertising of Conformity.

The Certification of Conformity with the ENS, of systems of categories MEDIUM or HIGH, will be issued by a certifying entity.

This certification can be displayed by public sector entities or by private sector operators that provide services or provide solutions that are required to comply with the ENS. In accordance with the above-mentioned Technical Security Instruction, the National Accreditation Entity (ENAC) made available the accreditation scheme (according to ISO/IEC 17065) for entities that wish to certify compliance with the ENS.

If required providers should be able to show:

- a Declaration of Compliance with the NSF (in the case of category systems BASIC) or
- a Certification of Compliance with the NSF (mandatory in the case of MEDIUM or HIGH category systems, and of voluntary application in the case of BASIC category systems), using the same procedures as those required for public entities.

5.6.2.4 Practice

The certification process against the National Security Framework was launched in 2017. For this reason, even though approximately half of the information systems of public sector entities are already in compliance with the ENS, only a few entities have so far obtained the Certification of Conformity.

5.6.2.5 Formal Status

Compliance with NSF (and the public exhibition of the corresponding Conformity Seals) is mandatory by law for the information systems of the approximately 20,000 entities of the Spanish

public sector, in addition to all those private companies that provide services supported in information systems to such entities.

5.6.2.6 Relation to other standards / schemes

The Guide CCN-STIC 825 develops the compliance with the National Security Framework using ISO/IEC 27001 and identifies the possible gaps to be covered. Annex A of Guide CCN-STIC 823 contains the controls of ISO 27002 and the CCM matrix, together with their correspondence to meet the requirements of the NSF.

In the case of systems, products or equipment classified as high security, the ENS indicates that the administration will give preference to IT products for which security has been evaluated and certified by independent bodies according to the ISO/IEC 15408 standard (Common Criteria) or an equivalent.

5.6.3 NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organisations)

5.6.3.1 Scope

The purpose of the NIST SP 800-53 standard is to provide guidelines for selecting and specifying security controls for organisations and information systems. The standard aims to support the executive agencies of the federal government to meet the requirements of FIPS Publication 200 (Minimum Security Requirements for Federal Information and Information Systems). The guidelines apply to all components of an information system that process, store, or transmit federal information.

The guidelines are organised into the following 18 families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorisation
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Program Management

5.6.3.2 Associated Evaluation Scheme and Governance

Next to the SP 800-53 publication, NIST has published SP 800-53A. This publication applies to the security and privacy controls defined in Special Publication 800-53. The purpose of this publication is to provide: (i) guidelines for building effective security assessment plans and privacy assessment plans; and (ii) 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.

This publication includes a catalog of procedures to assess the security controls and control enhancements in Special Publication 800-53.

NIST, the National Institute of Standards and Technology is part of the U.S. Department of Commerce and provides and sets the industry with technology, measurements and standards.

5.6.3.3 Process

Assessors select assessment procedures from the catalogue in 800-53A to assess the security controls and control enhancements in 800-53. Assessors obtain the required evidence during the assessment process to allow the appropriate organisational officials to make objective determinations about the effectiveness of the security and privacy controls and the overall security and privacy state of the information system.

Individuals with information security assessment and monitoring responsibilities are, but are not limited to, Inspectors General, system evaluators, assessors, independent verifiers/validators, auditors, analysts, information system owners, and common control providers.

5.6.3.4 Practice

US Government agencies must follow these standards and guidelines. No data is available regarding the exact number of agencies and sites to which this requirement is applicable.

5.6.3.5 Formal Status

US Government agencies must follow these standards and guidelines.

5.6.3.6 Relation to other standards / schemes

SP 800-53 provides mapping tables to provide organisations with a general indication of security control coverage with respect to ISO/IEC 27001.

5.7 Standards and schemes for healthcare (SWG3.6)

5.7.1 ISO/IEC 27799 (Health informatics - Information security management in health using ISO/IEC 27002)

5.7.1.1 Focus

ISO 27799 provides implementation guidance for the controls described in ISO/IEC 27002 (see section 5.1.9) and supplements them where necessary, so that they can be effectively used for managing health information security.

5.7.1.2 Associated Evaluation Scheme and Governance

None.

5.7.1.3 Process

None.

5.7.1.4 Practice

As the ISO survey (see section 5.1.8.4) does not give information on ISO 27799 separately, it is hard to get an overview.

5.7.1.5 Formal Status

ISO/IEC 27002 is already being used extensively for health informatics IT security management through the agency of national or regional guidelines in Australia, Canada, France, the Netherlands, New Zealand, South Africa, the United Kingdom and elsewhere.

5.7.1.6 Relation to other standards / schemes

ISO/IEC 27002 (see section 5.1.9)

5.7.2 ISO/IEC 62304 (Medical device software – Software life cycle processes)

5.7.2.1 Focus

ISO/IEC 62304 defines the life cycle requirements for medical device software. The set of processes, activities, and tasks described in this standard establishes a common framework for medical device software life cycle processes. The standard covers both stand-alone medical software and software embedded into a medical device.

This standard contains requirements on the processes implemented by a manufacturer of medical device software:

- General processes, such as quality management and risk management,
- Software development processes, from development planning to test and release,
- Software maintenance processes, such as problem analysis and modification implementation
- Software risk management processes, such as hazard analysis, taking risk control measures and risk management of software changes
- Software configuration management,
- Software problem resolution.

5.7.2.2 Associated Evaluation Scheme and Governance

There is no official evaluation scheme for ISO/IEC 62304. However, there are organizations offering certification against this standard, such as TÜV SÜD. Following their guidelines, in order to certify software, organizations must hold a valid TÜV SÜD certificate in accordance with ISO 13485 Quality Management System for Medical Devices. If assessment is completed with a positive result, the client obtains a certificate and can use the respective TÜV SÜD certification mark on its software in the future.

5.7.2.3 Process

Initial certification of a product requires review of the quality management system documentation in accordance with the IEC 62304 standard, and assessment of life-cycle documentation of the relevant software product (stand-alone software or embedded software).

During the certification period, which is set at a maximum of three years, software changes need to be reported to the certification body

5.7.2.4 Practice

Not publicly available.

5.7.2.5 Formal Status

Not known.

5.7.2.6 Relation to other standards / schemes

None.

5.7.3 IT Health CHECK Service (CHECK)

5.7.3.1 Focus

The IT Health Check (ITHC) Service provides assurance for both external as well as internal systems of health providers:

- **External systems** are to be protected from unauthorised access or change, and do not provide an unauthorised entry point into systems that consume PSN services. This should include systems that provide services on the internet such as email servers, web servers and other systems such as the firewalls that are in place to prevent unauthorised access from the internet into your organisation. External testing should also include any systems in place to allow staff or third party suppliers to connect remotely. These remote access solutions normally involve VPN that should be tested.
- **Internal systems** are tested to provide further assurance that no significant weaknesses exist on network infrastructure or individual systems that could allow one internal device to intentionally or unintentionally impact on the security of another.

  Internal testing should include vulnerability scanning and manual analysis the internal network. At a minimum it should include:

  - Desktop and server build and configuration, and network management security
  - Patching at operating system, application and firmware level
  - Configuration of remote access solutions (including solutions for managed devices and BYOD)
  - Build and Configuration of laptops and other mobile devices such as phones and tablets used for remote access
  - Internal security gateway configuration (including PSN gateway)
  - Wireless network configuration

The testing should include representative vulnerability scanning across the entire estate covering end-points (including thick and thin clients), servers, network devices and appliances. The scanning needs to include applications on devices, this is typically achieved through credentialed vulnerability scanning. In organisations with a large number of devices.

5.7.3.2 Associated Evaluation Scheme and Governance

The CHECK scheme enables penetration testing by NCSC-approved companies, employing penetration testing personnel qualified to assess IT systems for the British Government and other public sector bodies.

For UK Central Government Departments and their associated agencies:

- All systems processing data that is protectively marked OFFICIAL (see section 3.1.2.5) will be assessed by companies approved under CHECK.
- Requests for testing on systems processing data protectively marked SECRET and above should be sent to the NCSC. NCSC may, depending on the details, recommend that the task be performed by a CHECK company.

For other British public sector bodies, NCSC strongly recommends that all systems be assessed by a CHECK company.

5.7.3.3 Process

- Once the organization has hired a CHECK company, the scope of the CHECK assessment will be determined. The scope may differ between organizations.

- The organization must allow that the auditors will have full physical and digital access to the organization.
- Annual audits will be conducted by the CHECK company.

5.7.3.4 Practice

No public database

5.7.3.5 Formal Status

None

5.7.3.6 Relation to other standards / schemes

In order to become a CHECK provider, a company must have at least one team member qualifying as a CHECK Team Leader. The other team members must have qualified as a CHECK Team Member. When approving CHECK Team Leader and Team Member status, NCSC accept passes from one of the following examinations:

- A relevant CREST certification; see section 6.9.
- A relevant Cyber Scheme certification; see section 6.2.
- A relevant Tigerscheme certification.

5.8 Standards and schemes for smart cities and smart buildings (SWG3.7)

5.8.1 ISA/IEC 62433 (Security for Industrial Automation and Control Systems)

5.8.1.1 Focus

Building Control Systems (BCS) is a generic term that includes Heating, Ventilation and Air Conditioning (HVAC) systems, but also many other types of systems such as electronic security systems, fire alarm systems, sprinkler systems, digital signage systems, elevators and escalators, lighting control systems, etc.

In January 2017, the ISA Security Compliance Institute (ISCI) Building Controls Systems Working Group (BCSWG) completed a study to determine the applicability of ISA/IEC 62443 control systems cybersecurity standards to Building Control Systems (BCS). The report can be downloaded from http://www.isasecure.org/en-US/Building-Control-Systems-Report.Its main conclusions were the following:

- BCS-specific cybersecurity standards and guidelines are under development by a number of entities, but no product-specific cybersecurity standards exist yet.
- However, the IEC 62443 standards (see sections 3.2.1 and 5.2.6) are applicable to BCS. The IEC 62443 standards do not duplicate any BCS industry cybersecurity standards.

- Moreover, the ISASecure certification scheme (see section 3.2.1.2) is applicable to BCS. No BCS cybersecurity certification scheme exists that would be duplicated by the ISASecure certification scheme for BCS.
- The major difficulty in applying the IEC 62443 standards and the ISASecure scheme to BCS is achieving a common understanding of terminology. This is due to the fact that these standards largely reflect the language of traditional process industries.

5.8.1.2 Associated Evaluation Scheme and Governance

See sections 3.2.1.2 and 5.2.6.2.

5.8.1.3 Process

See sections 3.2.1.3 and 5.2.6.3.

5.8.1.4 Practice

See sections 3.2.1.4 and 5.2.6.4.

5.8.1.5 Formal Status

See sections 3.2.1.5 and 5.2.6.5.

5.8.1.6 Relation to other standards / schemes

Other initiatives relating to the cybersecurity of building control systems include:

- The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). ASHRAE developed BACnet, a data communication protocol for Building Automation and Control Networks. See http://www.bacnet.org/.
- The Continental Automated Buildings Associations (CABA) published a number of whitepapers on cybersecurity related to connected homes and intelligent buildings. See http://www.caba.org/Search?SearchTerms=cybersecurity.

5.9 Standards and schemes for telecom, media and content (SWG 3.8)

5.9.1 GSMA Security Accreditation Scheme

5.9.1.1 Focus

The Universal Integrated Circuit Card (UICC) in mobile devices, and its applications and data play a fundamental role in ensuring the security of the network, the subscriber's account and related services and transactions. To safeguard the integrity of the UICC, of Embedded SIMs with remote provisioning capabilities, and of their applications and data, it is essential that the supplier environment and processes that are used to manufacture and/or manage UICCs and Embedded SIMs are secure.

The GSMA's Security Accreditation Scheme (SAS) enables mobile operators, regardless of their resources or experience, to assess the security of their UICC and Embedded SIM suppliers, and of their Embedded SIM subscription management service providers. Two schemes operate under SAS:

- SAS for UICC Production (SAS-UP): This is a well-established and voluntary scheme operating successfully since 2000 through which UICC manufacturers subject their production sites and processes to a comprehensive security audit. Successful sites are awarded security accreditation for a period of one year, extending to two further years upon each successful renewal. This scheme has accredited some of the industry's largest UICC suppliers. GSMA also provides advice to its members on how to benefit from SAS-UP. The scope of this scheme has recently been broadened to include the production of Embedded SIMs.
- SAS for Subscription Management (SAS-SM): To ensure industry confidence in the security of remote provisioning for Embedded SIMs, the successful SAS model in place for UICC production has been re-used to enable security auditing and accreditation of the providers of Embedded SIM subscription management services.

5.9.1.2 Associated Evaluation Scheme and Governance

The GSMA has developed the auditing standards, requirements and methodologies for SAS in collaboration with SIM suppliers and security auditing companies, which conduct the audits on behalf of the GSMA.

Supporting guidelines are available on request to help sites interpret the security standards and requirements. A certification body is maintained within the GSMA to oversee and develop the scheme and to formally award accreditation.

5.9.1.3 Process

The GSMA has published audit methodologies for both schemes. The purpose of an audit is to ensure that suppliers have implemented adequate security measures to protect the interests of mobile network operators (MNOs). Audits are conducted by specialist auditing companies over a number of days, typically in a single site visit. The Auditors will check compliance against the relevant standard and its supporting documents by various methods such as document review, interviews and tests in specific areas.

The auditing process consists of the following steps:

1. Audit set-up
2. Audit preparation (off-site)
3. Audit process (on-site)
4. Certification
5. Notification and publication of certification

The standard duration of certification for sites without an existing valid certificate is 1 year. The standard duration of certification of sites with an existing valid certificate is 2 years.

5.9.1.4 Practice

A list of SAS auditors can be found at: http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme/sas-auditors. Currently, four auditors are listed.

A list of SAS-accredited sites can be found at: http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme/sas-accredited-sites-list. Currently, around 40 sites are listed for UICC Production and 3 sites are listed for Subscription Management.

5.9.1.5 Formal Status

None.

5.9.1.6 Relation to other standards / schemes

Not known.

5.9.2 ISO/IEC 27011 (Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations)

5.9.2.1 Focus

ISO/IEC 27011 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security controls in telecommunications organizations based on ISO/IEC 27002 (see section5.1.9).

This standard provides an implementation baseline of information security controls within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities, services and information handled, processed or stored by the facilities and services.

5.9.2.2 Associated Evaluation Scheme and Governance

There is no related evaluation scheme.

However, see section 5.1.8.2 on the governance of ISO 27001.

5.9.2.3 Process

See section 5.1.8.3 on the certification process for ISO 27001.

5.9.2.4 Practice

The ISO survey (see section 5.1.8.4) does not give information on ISO 27011 separately, and an exact number therefore cannot be given.

5.9.2.5 Relation to other standards / schemes

The guidelines of ISO/IEC 27011 are based upon ISO/IEC 27002 (see section 5.1.9)

5.9.3 TL 9000 Quality Management System

5.9.3.1 Focus

TL 9000 is a standard for quality management, based on ISO 9001, but particularly focused on the ICT sector. The standard contains a few requirements for establishing and maintaining methods for the identification and analysis of security risks and vulnerabilities for the product throughout its life cycle. The results of the risk analysis must be used to support secure network operation by prevention or mitigation of security vulnerabilities in the product design and operational controls.

The continuing effectiveness of the design and operational controls must be assessed throughout the product life cycle by the selection and use of appropriate security measurements. The QuEST forum (see below) published a document called Security Measurements Guidance, which can be downloaded from http://tl9000.org/links.html. It contains a catalog of security measurements that may be used by organisations implementing TL9000. These measurements are adapted from the CIS Consensus Security Benchmarks (see section 5.1.2) and the NIST SP 800-53 (see section 5.6.3). Implementing these security measurements is not mandatory.

The focus of TL9000 is on *measuring* security-related aspects of the product life cycle, rather than on *establishing or improving* a secure product development process.

5.9.3.2 Associated Evaluation Scheme and Governance

The QuEST forum oversees the standard. QuEST forum is made up of ICT companies who constantly maintain and refine the Requirements and Measurements standards in order to meet the changing needs of the ICT industry. Accredited Certification Bodies (CBs) provide registrar auditors, who must meet extensive training and audit experience requirements. Each CB is overseen by an Accreditation Body (AB) who reviews all audits and findings to ensure proper rigor was exercised in each audit.

5.9.3.3 Process

Companies wishing to be certified must choose their own CB from a list of accredited certification bodies provided by QuEST Forum. An initial certification audit is conducted by their chosen CB. The CB's findings are then reviewed by the AB to ensure the audit followed proper procedures. The company then works to correct their findings, with all action plans and closure evidence closely monitored by the CB for effectiveness. Once certification is bestowed, the company undergoes surveillance audits for the next two years, based on sampling. In the third year another extensive re-certification is conducted. QuEST Forum performs occasional validation audits on its approved CBs to ensure that audits are conducted according to TL 9000 standards.

5.9.3.4 Practice

TL 9000 members and current certifications of companies can be found at: http://www.questforum.org/about-us/member-directory/ and http://portal.questforum.org/tl9000/stats/locations_by_company_country.jsf

Approximately 700 organisations, covering 1750 locations, have been certified as of 2017. It is not known how many of these have chosen to implement the security measurements in the Security Measurements Guidance document.

5.9.3.5 Formal Status:

TL 9000 is global and widely used and recognised standard, but no official mandate exists.

5.9.3.6 Relation to other standards / schemes

TL 9000 uses ISO 9001 as its basis and includes all ISO 9001 requirements.

5.10 Standards and schemes for critical infrastructures

5.10.1 AEI Seal of Cybersecurity for Organisations

See section 5.1.1.

Although the Seal of Cybersecurity scheme is suitable for any type of organisation, its scope includes specifically also Critical Infrastructure operators and companies providing products and/or services to them.

5.10.2 KRITIS

5.10.2.1 Focus

The German Federal Ministry of the Interior, the Federal Office for Civil Protection and Disaster Response and the Federal Criminal Police Office have evolved a baseline protection concept for the protecting critical infrastructures. The aim of this baseline protection concept is to reduce the vulnerability of critical infrastructures to natural events and accidents as well as terrorist attacks and criminal acts. In this context it focuses on building-related, organisational, personal and technical protection measures. The baseline protection concept is referred to as KRITIS.

Whereas the scope of KRITIS is very wide, the Bundesampt fur Sicherheit in der Informationstechnik (BSI) focuses particularly on IT threats, that is on critical information infrastructure protection.

5.10.2.2 Associated Evaluation Scheme and Governance

For security evaluations of the IT infrastructure of critical infrastructures, the BSI is using the IT Grundschutz (see section 5.1.7) as a basis.

Although it is hard to find any information, it seems that the plan is to start in March 2018 with the evaluation of companies from the energy sector. Since IT Grundschutz is very big and generic, it is expected that for these evaluations a more concrete (sub)set of requirements will be used. These requirements are however not public.

5.10.2.3 Process

See section 5.7.1.3 for IT Grundschutz.

5.10.2.4 Practice

The BSI has not certified any sites at the moment.

5.10.2.5 Formal Status

Undergoing a KRITIS evaluation is mandatory under German law for all critical infrastructures. Nine sectors have been identified as (potentially) belonging to critical infrastructures, namely Energy, Health, State and Administration, Nutrition, Transport and traffic, Finance and insurance, IT and telecommunication, Media and culture and Water. Whether or not an organisation is obliged to undergo a KRITIS evaluation may furthermore depend on the number of citizens that are served by the organization.

5.10.2.6 Relation to other standards / schemes

KRITIS is Germany's contribution to the announced "European Program for Critical Infrastructure Protection" (EPCIP).

5.10.3 NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)

5.10.3.1 Focus

The NIST Cybersecurity Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally in an organization and externally. It can be used to help identify and prioritise actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organisations or it can be focused on the delivery of critical services within an organisation. Different types of entities – including sector coordinating structures, associations, and organisations – can use the Framework for different purposes, including the creation of common Profiles.

The Framework enables organisations - regardless of size, degree of cyber security risk, or cybersecurity sophistication - to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.

The Framework provides a common taxonomy and mechanism for organisations to:

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritise opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state;
- Communicate among internal and external stakeholders about cybersecurity risk.

Because the Framework references globally recognised standards for cybersecurity, it can also be used by organisations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts:

- the **Framework Core** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Framework Core consists of five Functions—Identify, Protect, Detect, Respond and Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards for each Subcategory.
- the **Framework Implementation Tiers** describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4).
- A **Framework Profile** is a representation of the outcomes that a particular organization has selected from the Framework Categories and Subcategories. By developing a 'Current' Profile and a 'Target' Profile, organisations can establish a roadmap for reducing cybersecurity risk.

5.10.3.2 Associated Evaluation Scheme and Governance

The U.S. National Institute of Standards and Technology (NIST) is responsible for this Framework. However, NIST has no plans to develop a conformity assessment program. NIST encourages the private sector to determine its conformity needs, and then develop appropriate conformity assessment programs. NIST is able to discuss conformity assessment-related topics with interested parties.

Currently (March 2017), legislation has been proposed that would mandate that agencies adopt the NIST framework and would task the NIST with auditing other federal agencies' cyber protections. See http://www.nextgov.com/cybersecurity/2017/03/nist-enforcer-house-committee-passes-bill-expand-agencys-responsibilities/135805/.

5.10.3.3 Process

Since the use of the Framework is voluntary, no official evaluation process exists. However, several organisations (both public and private) have published case studies describing their experiences with implementing the Framework and/or have written guidelines for the implementation of the Framework in specific industries. For an overview, see https://www.nist.gov/cyberframework/industry-resources.

The same website also lists a large number of tools that incorporate the Framework.

5.10.3.4 Practice

The NIST Cybersecurity Framework was originally focused on the Critical Infrastructure sectors but is quickly being adopted by organizations of all types and sectors. However, hard numbers have not been found.

5.10.3.5 Formal Status

Use of the Framework is voluntary, both for private-sector organisations and for U.S. federal agencies. Federal agencies are required to fulfill the security requirements defined in the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) policies, and NIST standards and guidelines as expressed in Federal Information Processing Standards and Special Publications. However, the NIST Cybersecurity Framework is not a FIPS or SP.

5.10.3.6 Relation to other standards / schemes

The Framework references many other standards and schemes, especially the CIS Critical Security Controls (section 5.1.2), ISA/IEC 62443 (section 5.2.6), NIST SP 800-53 (section 5.6.3), ISO 27001 (section 5.1.8) and COBIT 5.

The Framework is adaptive to provide a flexible and risk-based implementation that can be used with a broad array of cybersecurity risk management processes. Examples of cybersecurity risk management processes include ISO 31000, ISO/IEC 27005, NIST SP 800-39 and the Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline 7.

On the Framework website, NIST discusses the relationship between the Framework and a number of other approaches and initiatives in more detail.

5.10.4 Référentiel Général de Sécurité (RGS)

5.10.4.1 Focus

The focus of the French Référentiel Général de Sécurité (RGS) scheme lies on the electronic exchanges between administrative authorities and citizens. The framework covers the development of online services and electronic exchanges between government administrations and end users. The administrative authorities must guarantee the security of their information systems of the parties involved in the implementation of these services. The RGS aims to raise

the level of security of information systems and to protect information assets of administrative authorities, in particular the data entrusted to them by citizens.

On the one hand, the RGS framework serves as a methodology oriented around the accountability of the administrative authorities as well as their information systems through an approval / validation process. On the other hand, it contains more defined rules and good practices that are to be applied by administrations when using specific services, such as electronic certificates and time stamping, or security audits.

5.10.4.2 Associated Evaluation Scheme and Governance

ANSSI is the national authority in the area of cyber defense and network and information security (NIS) body for France. The mission of ANSSI consists of a broad range of regulatory and operational activities, from issuing regulations and verifying their application, to monitoring, alert and rapid response – particularly on government networks.

Under the RGS, audits are carried out by accredited third-party information systems security auditors (PASSIs) – see also section 5.12.1. A list of PASSIs can be found at: https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/

5.10.4.3 Process

A risk analysis will be performed to identify the security requirements of the information system based on threats and potential issues. The risk analysis approach consists of identifying events that may affect the safety of the system, estimating the consequences and potential impacts and then deciding what actions to take to reduce the risk to an acceptable level.

The threats that are to be taken into account are those that pose risks to the system and the information it processes, transmits and stores, in the environment in which it is located. When the information system integrates electronic certificates or electronic timestamps, the risk analysis will decide the appropriate strength of the security levels to be implemented (signature, authentication, confidentiality, etc.).

For the detailed explanation and guidance of the RGS process, see the following document: https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf.

See also section 5.12.1.3 for the PASSI and PSCE / PSHE schemes.

Price and duration are not indicated.

5.10.4.4 Practice

See section 5.12.1.4 for the PASSI and PSCE / PSHE schemes.

5.10.4.5 Formal Status

The RGS framework is adopted in respect to relevant French law.

5.10.4.6 Relation to other standards / schemes

RGS recommends to use the ISO 27005 standard, which sets a framework for risk management. Furthermore, the practical implementation of RGS can be facilitated by explanations and tools proposed by the *Expression des Besoins et Identification des Objectifs de Sécurité* (EBIOS) method. The EBIOS method was created in 1995 and is maintained by ANSSI.

5.11 Standards and schemes for general secure software development

5.11.1 BSI PAS 754

5.11.1.1 Focus

The BSI PAS 754 (Software trustworthiness –Governance and management - Specification) provides consensus for software trustworthiness. The specification identifies five aspects of software trustworthiness: safety, reliability, availability, resilience and security. It describes a widely applicable approach to achieving software trustworthiness, which is based on the following concepts:

- Governance: Before producing or using any software which has a trustworthiness requirement, an appropriate set of governance and management measures shall be set up
- Risk assessment: The risk assessment process involves considering the set of assets to be protected, the nature of the adversities that may be faced, and the way in which the software may be susceptible to such adversities
- Control application: Risk shall be managed through the treatment of risk by the application of appropriate personnel, physical, procedural and technical controls
- Compliance: A compliance regime shall be set up to ensure that creators and users of software ensure that governance, risk and control decisions have been implemented.

5.11.1.2 Associated Evaluation Scheme and Governance

None.

This document is a Public Available Standard whose development was facilitated by the British Standards Institution and sponsored by the UK Trustworthy Software Initiative.

5.11.1.3 Process

An organisation may claim conformance with PAS 754. A claim of conformance can be made on the basis of either a self-assessment or a third-party conformity assessment. However, there are no officially accredited certification bodies for PAS 754.

5.11.1.4 Practice

Not known.

5.11.1.5 Formal Status

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

5.11.1.6 Relation to other standards / schemes

Not known.

5.11.2 BSIMM

5.11.2.1 Focus

The Building Security in Maturity Model (BSIMM) is a study of existing software security initiatives. By quantifying the practices of many different software-developing organisations, BSIMM describes the common ground shared by many, as well as the variation that makes each unique. As such, it acts as a measuring stick to compare an organisation's level of maturity with regard to secure software development to those of other organisations in the same vertical.

The model is comprised of 113 activities that are undertaken by organisations to improve their software security. These activities are grouped into 12 practices, which are themselves grouped into four domains: Governance, Intelligence, SSDL Touchpoints and Deployment.

Each year, an update of the BSIMM is published; the most recent version is BSIMM7 (2016). The data in BSIMM7 is collected from 95 participating companies, typically large enterprises active in the financial services, independent software vendors, cloud, healthcare, Internet of Things, and insurance industries. Verticals with lower representation in the BSIMM population include: telecommunications, security, retail, and energy.

5.11.2.2 Associated Evaluation Scheme and Governance

There is no official evaluation scheme for the BSIMM, as the philosophy behind it is to describe what is being done rather that what should be done. The BSIMM is primarily the work of the three authors mentioned in section 2.3, although there are a number of 'BSIMM Advisors' mentioned on the website as well. These three authors are employed by Synopsys (previously Cigital) and Netsuite.

5.11.2.3 Process

To assess its level of maturity using BSIMM, an organisation can basically count how many of the 113 activities it performs. This results in a 'spider chart' depicting the firm's maturity on each of the 12 practices discussed above. Since each version of the BSIMM also contains the average score of all members of BSIMM, as well as the average score of members in a certain vertical, it is possible to benchmark the organisation's maturity.

It is also possible for an organisation to become a member of BSIMM, which means that data on the activities performed by that organisation will be used to create the next version of the BSIMM.

Next to that, BSIMM also has a light-weight variety called ‘BSIMM for vendors’, which can be used by organisations as a security control for vendor management of third-party software providers.

5.11.2.4 Practice

Membership of BSIMM grows continually, from 67 firms in 2013, via 78 in 2014, to 95 in 2016. BSIMM claims it describes the work of 1,111 Software Security Group members working with a satellite of 3,595 people to secure the software developed by 272,782 developers.

It is not known how many firms use the BSIMM to measure their maturity regarding software security and to guide the improvement of their software security practices.

5.11.2.5 Formal Status

None.

5.11.2.6 Relation to other standards / schemes

Not known.

5.11.3 ISO/IEC 21827 (Systems Security Engineering - Capability Maturity Model)

5.11.3.1 Focus

ISO/IEC 21827 specifies the Systems Security Engineering - Capability Maturity Model (SSE-CMM), which describes the essential characteristics of an organisation's security engineering process that must exist to ensure good security engineering. ISO/IEC 21827 does not prescribe a particular process or sequence, but captures practices generally observed in industry. The model is a standard metric for security engineering practices covering the following:

- the entire life cycle, including development, operation, maintenance and decommissioning activities;
- the whole organisation, including management, organisational and engineering activities;
- concurrent interactions with other disciplines, such as system, software, hardware, human factors and test engineering; system management, operation and maintenance;
- interactions with other organisations, including acquisition, system management, certification, accreditation and evaluation.

The objective is to facilitate an increase of maturity of the security engineering processes within the organisation. The SSE-CMM is related to other CMMs which focus on different engineering disciplines and topic areas and can be used in combination or conjunction with them.

5.11.3.2 Associated Evaluation Scheme and Governance

The SSE-CCM was originally developed by the System Security Engineering Association, a non-profit membership organisation. There is an evaluation scheme for the SSE-CCM, called the

SSE-CMM Appraisal Method (SSAM). The SSAM is a method for using the SSE-CMM to evaluate the process capability of an organisation or enterprise's systems security engineering function. It provides guidance for the preparation and conduct of an appraisal. However, the SSAM is a community effort. There does not seem to be an official organisation, including governance, which oversees the appraisal process.

5.11.3.3 Process

According to the SSAM documentation, an SSE-CCM appraisal consists of four steps:

- **Planning**: Establish the framework under which the appraisal will be conducted as well as to prepare the logistical aspects for the On-Site Phase
- **Preparation:** Prepare the Appraisal Team for the On-Site activities, and conduct a preliminary gathering and analysis of data through a questionnaire.
- **On-Site:** Explore the results of the preliminary data analysis, and provide an opportunity for practitioners at the appraised entity to participate in the data gathering and validation process
- **Reporting:** Appraisal Team performs its final analysis of all data gathered during the previous three phases and presents its findings to the Sponsor.

5.11.3.4 Practice

In general, it seems both SSE-CCM itself and in particular the SSAM have not been used much over the last decade or so. Most references that could be found date from 2005 or earlier. In fact, the ISSEA website itself could not be found.

5.11.3.5 Formal Status

None.

5.11.3.6 Relation to other standards / schemes

None.

5.11.4 Microsoft Security Development Lifecycle

5.11.4.1 Focus

The Security Development Lifecycle (SDL) is a security assurance process that is focused on software development. As a company-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in software and culture at Microsoft. Combining a holistic and practical approach, the SDL aims to reduce the number and severity of vulnerabilities in software. The SDL introduces security and privacy throughout all phases of the development process.

The Microsoft SDL is based on three core concepts: education, continuous process improvement, and accountability. The ongoing education and training of technical job roles within a software development group is critical. The appropriate investment in knowledge transfer helps organisations to react appropriately to changes in technology and the threat landscape. Because

security risk is not static, the SDL places heavy emphasis on understanding the cause and effect of security vulnerabilities and requires regular evaluation of SDL processes and introduction of changes in response to new technology advancements or new threats. Data is collected to assess training effectiveness, in-process metrics are used to confirm process compliance and post-release metrics help guide future changes. Finally, the SDL requires the archival of all data necessary to service an application in a crisis. When paired with detailed security response and communication plans, an organisation can provide concise and cogent guidance to all affected parties.

5.11.4.2 Associated Evaluation Scheme and Governance

Microsoft Services and the SDL Pro Network offer training, consulting services, and tools to help you adopt the SDL process. The SDL Pro Network is a selection of commercial parties specialised within the SDL (https://www.microsoft.com/en-us/SDL/adopt/pronetwork.aspx).

Microsoft is one of the world's largest producers of software and is an authority upon the subject.

5.11.4.3 Process

The core concepts education, continuous process improvement, and accountability, are defined in seven phases:

1. TRAINING	2. REQUIREMENTS	3. DESIGN	4. IMPLEMENTATION	5. VERIFICATION	6. RELEASE	7. RESPONSE
1. Core Security Training	2. Establish Security Requirements	5. Establish Design Requirements	8. Use Approved Tools	11. Perform Dynamic Analysis	14. Create an Incident Response Plan	Execute Incident Response Plan
	3. Create Quality Gates/Bug Bars	6. Perform Attack Surface Analysis/ Reduction	9. Deprecate Unsafe Functions	12. Perform Fuzz Testing	15. Conduct Final Security Review	
	4. Perform Security and Privacy Risk Assessments	7. Use Threat Modeling	10. Perform Static Analysis	13. Conduct Attack Surface Review	16. Certify Release and Archive	

5.11.4.4 Practice

Since firms are not DSL certified, it is impossible to create a list of organisations applying the DSL. It is known, however, that Microsoft has made the DSL mandatory for their internal software development.

5.11.4.5 Formal Status

None.

5.11.4.6 Relation to other standards / schemes

None.

5.11.5 OWASP Software Assurance Maturity Model

5.11.5.1 Focus

The OWASP Software Assurance Maturity Model (or OWASP SAMM) is an open framework to help organisations formulate and implement a strategy for software security that is tailored to the specific risks facing the organisation. The foundation of the model are four core business functions of software development: Governance, Construction, Verification and Deployment. The model ties three security practices to each of these, each with an objective, two associated activities, an assessment method and a list of expected results. Moreover, for each of the 12 security practices three maturity levels are defined. The overall maturity level of an organisation results from the maturity levels achieved for each practice.

5.11.5.2 Associated Evaluation Scheme and Governance

There is no official evaluation scheme for SAMM.

5.11.5.3 Process

For each practice and each maturity level, the model describes activities that need to be properly in place for that level. The process of evaluation is therefore the assessment whether these activities are properly in place or not.

OWASP published an ‘assessment toolbox’ in the form of an Excel spreadsheet, which can be used for a self-evaluation of the current maturity level of an organisation. This is done by answering questions on all activities. Once all questions are answered, the toolbox creates ratings and visualisations. The toolbox also offers a way to set a roadmap towards a desired future maturity level.

5.11.5.4 Practice

The SAMM website lists 12 official adopters. It is likely that there are many more given that this a mature OWASP standard.

5.11.5.5 Formal Status

None.

5.11.5.6 Relation to other standards / schemes

A mapping between OWASP SAMM and BSIMM is available.

5.12 Standards and schemes for Cybersecurity service providers

5.12.1 ANSSI requirements for security service providers (PDIS, PRIS, PASSI, PSCE, PSHE)

5.12.1.1 Focus

A security operations center (SOC) may offer different security services to a commission entity. This includes auditing, monitoring and defending enterprise information systems, providing electronic certificates and providing electronic timestamps. Depending on the challenges, needs and resources of the commissioning entity, a SOC can be internal or outsourced, and when outsourced, it can be dedicated or shared.

ANSSI has developed or is in the process of developing approval processes for companies offering several types of SOC services:

- **Security incident detection service providers** – *Prestataires de détection des incidents de sécurité* (PDIS) in French. This covers security incident identification and qualification, collection and storage, and reporting on detected security incidents:
- **Security incident response service providers** - *Prestataires de réponse aux incidents de sécurité* (PRIS) in French. This covers reaction and remediation activities, such as defining a security incident response method, collecting and analyzing relevant information from systems and networks, identifying an attacker's mode of operation and purpose, assisting in assessing the impact of an attack, and propose remedial measures.
- **Information system security auditing service providers** - *Prestataires d'audit de la sécurité des systèmes d'information* (PASSI) in French. This covers the competence of auditors, the confidentiality of data, reports and documents exchanged, and the appropriateness of the methodology for security audits. Several types of audits are distinguished, to wit: architecture audits, configuration audits, source code audits, physical and organisation audits and penetration tests.
- **Electronic certificates service providers** - *Prestataires de service de certification Electronique* (PSCE) in French. This covers service providers issuing digital certificates for different purposes, such as encryption, authentication of persons and machines, and electronic signatures.
- **Electronic timestamping service providers** - *Prestataires de services d'horodatage électronique* (PSHE) in French. This covers service providers that provide signed time stamps proving that a given data point existed at a given time.

ANSSI has published requirements for each of these types of service provider:

- PDIS requirements are available in both English and French, available at https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v1.0_en.pdf.
- PRIS requirements are available in French only at https://www.ssi.gouv.fr/uploads/IMG/pdf/PRIS_Referentiel_d_exigences_anssi.pdf.

- PASSI requirements are available in French only at https://www.ssi.gouv.fr/uploads/2014/12/PASSI_referentiel-exigences_v2.1.pdf
- PSCE and PSHE requirements are in fact part of the documentation underlying the *Référentiel Général de Sécurité* scheme, see section 5.10.4. They can be found at https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-techniques-psco/. For PSCEs, three different security levels are distinguished; for PSHEs, there is only security level.

5.12.1.2 Associated Evaluation Scheme and Governance

ANSSI is the French national authority in the area of cyber defense and network and information security (NIS). The mission of ANSSI consists of a broad range of regulatory and operational activities, from issuing regulations and verifying their application, to monitoring, alert and rapid response – particularly on government networks.

5.12.1.3 Process

5.12.1.3.1 General

The next sections describe the process for the PASSI, PSCE and PCSH qualifications. Note that these processes are in fact carried out under the *Référentiel Général de Sécurité* scheme, see section 5.10.4. Process descriptions for PDIS and PRIS could not be found.

All of these approval processes can be used both for internal and third-party security service providers. In the first case, the service is used to fulfill an organisation's own need for security services.

5.12.1.3.2 PASSI

A request for qualification can be sent by e-mail to the certification body (LSTI). Upon receipt and analysis of all provided information, LSTI transmits to the applicant a financial proposal accompanied by the PASSI qualification regulation which constitutes the general evaluation conditions and the exhaustive list of documents to be provided. The cost of a PASSI qualification is partly flat-rate, partly depending on the number of geographical sites and the number of auditors for which the PASSI qualification should be valid.

After acceptance of the financial conditions by the candidate provider, a qualification contract is established. It includes the information provided in the application and constitutes the special conditions for qualification.

A PASSI evaluation is carried out in three stages:

- An on-site evaluation of headquarters of the candidate provider
- An on-site assessment of other sites (control observation)
- Written and oral examinations of the auditors

Assessments are carried out by LSTI assessors and experts. They consist in verifying the effective implementation of procedures, instructions, operating procedures and tools defined by PASSI to meet the PASSI requirements.

Auditors routinely review the audit practice (ISO / IEC 19011) and then review the activities they have selected from the five audit activities. The duration of each examination is 30 minutes.

Depending on the result of the written examinations, the auditors are invited or not to the oral examination. Auditors who obtain at least the minimum marks set out in the qualification rules shall be considered competent for the audit activities for which they have been successful.

The granting of the qualification results in the issue of a qualification certificate describing the audit activities for which the service provider is qualified and the sites concerned. Certificates of competence are also sent to the auditors who passed the examinations. A PASSI qualification is valid for three years, subject to 18-month supervision; the validity period of an auditor's certificate of competence is 3 years, provided the auditor does not leave the PASSI service provider.

5.12.1.3.3 PSCE / PSHE

A request for qualification as a PSCE or PSHE can be sent to a certification body accredited by the French Committee of Accreditation (Cofrac). The certification body gathers relevant information, such as:

- The architecture of the key management infrastructure
- The organisation of registration of holders
- The technical service providers involved
- The geographical location of the certification / timestamp authority and of the registration authority
- The certification / timestamping policy and a declaration of practices

The certification body then sends an offer to the applicant. If this is accepted, an initial audit takes place, which is split into two parts called step 1 and step 2 which are spaced in time from about 2 to 6 weeks:

- The purpose of step 1 is to verify the readiness of the organisation and to conduct the literature review in order to validate the organisation planned for step 2.
- Step 2 is an on-site check of the application of the technical and organisational provisions.

Qualification is awarded to organisations that do not present a major departure from the requirements. It is sent to ANSSI and published in the European Trusted List, see https://ec.europa.eu/digital-single-market/en/news/eu-trusted-lists-certification-service-providers

Qualification is valid for three years, subject to annual monitoring. An annual audit program is planned to verify compliance.

5.12.1.4 Practice

ANSSI is currently conducting trials with selected service providers to test the applicability of the PDIS and PRIS requirements. The current status of these trials is summarised here: http://www.nicp.nato.int/wp-content/uploads/2015/01/Cyberdefence-trusted-service-providers-in-France.pdf. At the moment, no services providers have been qualified yet, but the ANSSI website provides a list of services providers that are in the process of being qualified for both programmes.

The qualification programme for PASSI is already live; the document linked above lists four service providers that have been qualified by ANSSI and more than ten that are in process of being qualified.

Service providers wishing to obtain PSCE and PSHE qualification are qualified under the RGS scheme. For PSCE, around 275 service providers have been qualified. For PSHE, the number of qualified service providers could not be found.

5.12.1.5 Formal Status

Participating in one of these schemes is voluntary, except for a company wishing to perform audits for the *Référentiel Général de Sécurité* scheme (see section 5.10.4). Such a company must be a qualified PASSI.

5.12.1.6 Relation to other standards / schemes

This scheme is related to the ANSSI SecNumCloud scheme for cloud service providers, see section 4.1.

5.12.2 CREST Simulated Targeted Attack and Response (STAR)

5.12.2.1 Focus

Working alongside the Bank of England (BoE), government, and industry, CREST developed a framework to deliver controlled, bespoke, intelligence-led cyber security tests. STAR (Simulated Targeted Attack and Response) incorporates penetration testing and threat intelligence services to accurately replicate threats to critical assets. The STAR tests use Threat Intelligence to deliver these attack simulations in order to provide assurance that organisations have appropriate countermeasures and responses to detect and prevent cyber-attack. Accreditation under the STAR scheme is a prerequisite for membership of the BoE CBEST scheme, used to provide assurance to the most critical parts of the UK's financial services.

5.12.2.2 Associated Evaluation Scheme and Governance

The Council for Registered Ethical Security Testers (CREST) is a not-for-profit accreditation and certification body that represents and supports the technical information security market. CREST was set up in 2006 in response to the clear need for more regulated professional services and is now recognised globally as a cyber assurance body for the technical security industry.

CREST provides internationally recognised accreditations for organisations and individuals providing penetration testing, cyber incident response and threat intelligence services. All CREST member companies undergo stringent assessment; while CREST qualified individuals have to pass rigorous professional level examinations to demonstrate knowledge, skill and competence. CREST also supports the industry by providing in-depth guidance material and commissioning detailed research projects all of which is provided to the industry free of charge.

CREST is managed by an Executive of nine senior industrialists, two of whom represent the CREST assessors. There are two legal Directors who devolve responsibility to the Executive for the day to day management of the organisation. At an operational level, responsibility is divided into the following areas:

- Governance
- Standards and Operations
- Marketing and Communications
- HR & Remuneration
- Finance

5.12.2.3 Process

One of the prerequisites for accreditation is to have a number of employees which hold relevant CREST certification (for Penetration Testing: both CCSAM and CCSAS; for Threat Intelligence, CCTIM). The testing is being executed Approved Member Companies.

5.12.2.4 Practice

Not known.

5.12.2.5 Formal Status

CREST provides internationally recognised accreditations for organisations and individuals providing penetration testing, cyber incident response and threat intelligence services. Accreditation under the STAR scheme is a prerequisite for membership of the Bank of England (BoE) CBEST scheme.

5.12.2.6 Relation to other standards / schemes

Accreditation under the STAR scheme is a prerequisite for membership of the Bank of England (BoE) CBEST scheme, see section 5.5.2. Only CBEST member companies are accredited to perform a CBEST on a UK financial institution. One of the prerequisites for accreditation is to have a number of employees which hold relevant CREST certification (for Penetration Testing: both CCSAM and CCSAS; for Threat Intelligence, CCTIM). See section 6.9.

5.13 Standards and schemes for the payment industry

5.13.1 PCI Data Security Standard (PCI DSS)

5.13.1.1 Focus

The PCI Data Security Standard (DSS) was crafted to augment and promote cardholder data security and to implement a standardised global data security measures. it has 12 foundational requirements. These requirements can be categorised into six general overviews, namely:

- building and maintaining a secure network;
- cardholder data protection;
- maintaining a vulnerability management program;
- implementing strong access measures;
- regular monitoring and testing of networks;
- maintaining an information security policy.

PCI DSS applies to all entities that store, process, and/or transmit payment account data or can affect the security of cardholder data. These entities include merchants, service providers (e.g. payment gateway, processor), card issuers and acquiring banks. For these companies, compliance with the standard is obligatory, though depending on the volume of cards processed, different validation requirements apply.

5.13.1.2 Associated Evaluation Scheme and Governance

The PCI Security Standards Council maintains, evolves, and promotes the Payment Card Industry Security Standards. The Council's founding members, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., have agreed to incorporate the PCI Data Security Standard (PCI DSS) as part of the technical requirements for each of their data security compliance programs. Each founding member also recognises the Qualified Security Assessors and Approved Scanning Vendors qualified by the PCI Security Standards Council.

All five payment brands, along with Strategic Members, share equally in the Council's governance, have equal input into the PCI Security Standards Council and share responsibility for carrying out the work of the organisation. Other Participating Organisations include merchants, banks, processors, hardware and software developers, and point-of-sale vendors.

Note that enforcement of compliance with the PCI DSS and determination of any non-compliance penalties are carried out by the individual payment brands and not by the Council.

Qualified Security Assessor (QSA) companies are independent security organisations that have been qualified by the PCI Security Standards Council to validate an entity’s adherence to PCI DSS. QSA Employees are individuals who are employed by a QSA Company and have satisfied and continue to satisfy all QSA Requirements.

5.13.1.3 Process

Validation of compliance with the PCI Data Security Standard is determined by individual payment brands. All have agreed to incorporate the PCI Data Security Standard as part of the technical requirements for each of their data security compliance programs. The payment brands also recognise qualified security assessors and approved scanning vendors qualified by the PCI Security Standards Council.

The Council does not enforce compliance; this is done by individual payment brands or acquiring banks.

A PCI DSS evaluation is carried out in a three-step process:

- Assess. Identifying cardholder data, taking an inventory of IT assets and business processes for payment card processing, and analyzing them for vulnerabilities.
- Remediate. Fixing vulnerabilities and eliminating the storage of cardholder data unless absolutely necessary.
- Report. Compiling and submitting required reports to the appropriate acquiring bank and card brands.

5.13.1.4 Practice

PCI does not make available a list of PCI DSS-certified organisations. However, many payment schemes have a public list of compliant service providers, which implies PCI DSS certification. Information for MasterCard and Visa is available at:

- MasterCard: https://www.mastercard.us/content/dam/mccom/en-us/documents/service-provider-list-03-02-2017.pdf
- Visa Inc: http://www.visa.com/splisting/searchGrsp.do
- Visa Europe: https://www.visaeurope.com/media/images/Visa%20Europe%20Merchant%20Agent%20List%20March%202017-73-40623.pdf

These lists contain up to 4500 separate organisations. Note that this excludes member banks.

5.13.1.5 Formal Status

The Council's founding members, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., have agreed to incorporate the PCI Data Security Standard (PCI DSS) as part of the technical requirements for each of their data security compliance programs. Each founding member also recognises the Qualified Security Assessors and Approved Scanning Vendors qualified by the PCI Security Standards Council.

5.13.1.6 Relation to other standards / schemes

ENISA listed the PCI DSS certification scheme on its Cloud Certification Schemes List (CCSL) – see https://resilience.enisa.europa.eu/cloud-computing-certification.

5.14 Standards and schemes for IoT device vendors

5.14.1 BITAG Internet of Things (IoT) Security and Privacy Recommendations

5.14.1.1 Focus

The following recommendations that BITAG believes are actionable in the short term using existing technology are discussed in the document:

- IoT Devices Should Use Best Current Software Practices
- IoT Devices Should Follow Security & Cryptography Best Practices
- IoT Devices Should Be Restrictive Rather Than Permissive in Communicating
- IoT Devices Should Continue to Function if Internet Connectivity is Disrupted
- IoT Devices Should Continue to Function If the Cloud Back-End Fails
- IoT Devices Should Support Addressing and Naming Best Practices
- IoT Devices Should Ship with a Privacy Policy That is Easy to Find & Understand
- Disclose Rights to Remotely Decrease IoT Device Functionality
- The IoT Device Industry Should Consider an Industry Cybersecurity Program

5.14.1.2 Associated Evaluation Scheme and Governance

There is no evaluation scheme, just recommendations.

BITAG is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on broadband network management practices and other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

The list of members can be found at:
https://www.bitag.org/bitag_organization.php?action=history#

5.14.1.3 Process

None.

5.14.1.4 Practice

Not publicly available.

5.14.1.5 Formal Status

None.

5.14.1.6 Relation to other standards / schemes

None.

5.14.2 Future-proofing the Connected World

5.14.2.1 Focus

This document provides considerations and guidance for designing and developing reasonably secure IoT devices. The following list provides steps toward developing more secure IoT devices which are discussed in-depth in the document:

1. Secure development methodology
2. Secure development and integration environment

3. Identify framework and platform security features
4. Establish privacy protections
5. Hardware security engineering
6. Protect data
7. Secure associated apps/svcs
8. Protect interfaces/APIs
9. Provide secure update capability
10. Implement secure authorization
11. Establish secure key management
12. Provide logging mechanisms
13. Perform security reviews

5.14.2.2 Associated Evaluation Scheme and Governance

There is no evaluation scheme, this document only serves as a guide

The Cloud Security Alliance (CSA) is dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

5.14.2.3 Process

None.

5.14.2.4 Practice

Not publicly known.

5.14.2.5 Formal Status

None.

5.14.2.6 Relation to other standards / schemes

None.

5.14.3 GSMA IoT Security Guidelines

5.14.3.1 Focus

The IoT Security Guidelines created by the GSMA promote a methodology for developing secure IoT services. They ensure that 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. Recommendations are presented as critical, high priority, medium priority and low priority recommendations.

The guidelines are split in two components of IoT: the Endpoint Ecosystem and the Service Ecosystem. The Service Ecosystem represents the set of services, platforms, protocols and other

technologies required to provide capabilities and collect data from Endpoints deployed in the field. The critical recommendations for these systems are:

- Implement a Service Trusted Computing Base
- Define an Organizational Root of Trust
- Define a Bootstrap Method
- Define a Security Infrastructure for Systems Exposed to the Public Internet
- Define a Persistent Storage Model
- Define an Administration Model
- Define a Systems Logging and Monitoring Approach
- Define an Incident Response Model
- Define a Recovery Model
- Define a Sunsetting Model
- Define a Set of Security Classifications
- Define Classifications for Sets of Data Types

The Endpoint Ecosystem consists of low-complexity devices, rich devices and gateways that connect the physical world to the digital world via several types of wired and wireless networks. The critical recommendations for these systems are:

- Implement an Endpoint Trusted Computing Base
- Utilize a Trust Anchor
- Use a Tamper Resistant Trust Anchor
- Define an API for Using the TCB
- Defining an Organizational Root of Trust
- Personalize Each Endpoint Device Prior to Fulfilment
- Minimum Viable Execution Platform (Application Roll-Back)
- Uniquely Provision Each Endpoint
- Endpoint Password Management
- Use a Proven Random Number Generator
- Cryptographically Sign Application Images
- Remote Endpoint Administration
- Logging and Diagnostics
- Enforce Memory Protection
- Bootloading Outside of Internal ROM
- Locking Critical Sections of Memory
- Insecure Bootloaders
- Perfect Forward Secrecy
- Endpoint Communications Security
- Authenticating an Endpoint Identity

For network Operators, IoT Service Providers and other partners in the IoT ecosystem the “IoT Security Guidelines for Network Operators” is developed, which provides top-level security guidelines for Network Operators who intend to provide services to IoT Service Providers to ensure system security and data privacy.

5.14.3.2 Associated Evaluation Scheme and Governance

A self-assessment checklist is provided which enables the suppliers of IoT products, services and components to self-assess the conformance of their products, services and components to the GSMA IoT Security Guidelines.

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem

5.14.3.3 Process

1. Assess your IoT product, service or component for compliance with the recommendations and controls stated in the GSMA Security IoT Self-Assessment Checklist document, and sign the declaration.
2. The GSMA will perform an administrative check of the summary information contained within the checklist and, if completed correctly, the GSMA will assign a unique reference number to the checklist.
3. The GSMA will publish the summary information.

5.14.3.4 Practice

Published checklist summaries can be found here:

www.gsma.com/connectedliving/completed-self-assessments/

5.14.3.5 Formal Status

None.

5.14.3.6 Relation to other standards / schemes

None.

5.14.4 Industrial Internet of Things Security Framework

5.14.4.1 Focus

The purpose of the Industrial Internet of Things, Volume G4: Security Framework (IISF) developed by the Industrial Internet Consortium (IIC) 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.

An IIoT system exhibits end-to-end characteristics that emerge as a result of the properties of its various components and the nature of their interactions. The five characteristics that most affect the trust decisions of an IIoT deployment are:

- Security
- Safety
- Reliability
- Resilience
- Privacy

These are referred to as key system characteristics. Others, for example, scalability, usability, maintainability, portability or composability may be important in general too but are not considered “key” in respect to trustworthiness.

5.14.4.2 Associated Evaluation Scheme and Governance

There is no evaluation scheme. However, the IIC has testbeds within five different markets: Energy, Healthcare, Manufacturing, Smart Cities, and Transportation. The testbeds are where the innovation and opportunities of the Industrial Internet – new technologies, new applications, new products, new services, new processes – can be initiated, thought through, and rigorously tested to ascertain their usefulness and viability before coming to market.

The security evaluations of these testbeds provide continuous feedback that will be used to update the information in subsequent versions of the IISF and aid in creating evaluation material including security checklists and maturity models for industrial systems.

The Industrial Internet Consortium is a broad based, international consensus driven organisation consisting of large and small companies, academia, and government collectively focused on the totality of realizing the Industrial Internet of Things through requirements identification, testbed experimentation, and reports and tools delivery to facilitate rapid realisation of the IIoT across a broad spectrum of global industries and applications.

5.14.4.3 Process

Testbed proposals are submitted at the IIC, after which they are evaluated. A successful testbed:

- Provides rigorous, transparent, and replicable testing of new technologies
- Applies new technologies to create new products & services
- Shows how new technologies can be usefully deployed
- Fuels R&D ideas and opportunities
- Generates an appreciable and measurable impact on new and existing markets

Once approved, requests for potential partners are posted in the members area of the IIC.

5.14.4.4 Practice

An overview of the testbeds and the participating members can be found on the following website: http://www.iiconsortium.org/test-beds.htm.

5.14.4.5 Formal Status

None.

5.14.4.6 Relation to other standards / schemes

The IISF builds on the 'Industrial Internet Reference Architecture' (IIRA). The representation of the content of the IIRA is based on the joint ISO/IEC/IEEE 42010 (Systems and software engineering — Architecture description) standard. The content in the IIRA is based on the contributions of the IIC members. For more information on this standard, see: http://www.iso-architecture.org/ieee-1471.

5.14.5 IoT Security Compliance Framework

5.14.5.1 Focus

The IoT Security Compliance Framework, created by the IoT Security Foundation, is a checklist to guide an organisation through the assurance process and gather structured evidence to demonstrate conformance with best practices. These best practices are categorized as follows:

- Business Security Processes and Responsibility
- Device Hardware & Physical Security
- Device Application
- Device Operating System
- Device Wired and Wireless Interfaces
- Authentication and Authorisation
- Encryption and Key Management for Hardware
- Web User Interface
- Mobile Application
- Privacy
- Cloud and Network Elements
- Secure Supply Chain and Production
- Configuration

5.14.5.2 Associated Evaluation Scheme and Governance

There is no certification scheme, however, the document provides a questionnaire based upon the best practices, allowing to test for compliance.

The IoT Security Foundation is a non-profit organization, and is member-driven, led by an executive steering board.

5.14.5.3 Process

The questionnaire elicits a set of responses to security requirements for aspects of the organisation and product. Each question needs to be confirmed, with evidence to support compliance with the requirement. Alternatively, if the requirement is deemed to be not applicable, an explanation must be provided as to why.

In order to apply an appropriate level of security compliance to a product, the requirements that are listed in the questionnaire have their applicability determined by the category of the product and the compliance class. The following categories and classes are available:

- Categories
  - Consumer (Domestic)
  - Enterprise
  - Industrial
  - Medical
  - Automotive
  - Public Agency
  - Critical National Infrastructure
- Classes
  0. Where compromise to the data generated or level of control provided is likely to result in little discernible impact on an individual or organisation.
  1. Where compromise to the data generated or level of control provided is likely to result in no more than limited impact on an individual or organisation.
  2. In addition to class 1, the device is designed to resist attacks on availability that would have significant impact an individual or organisation, or impact many individuals, for example by limiting operations of an infrastructure to which it is connected.
  3. In addition to class 2, the device is designed to protect sensitive data including sensitive personal data.
  4. In addition to class 3, where the data generated or level of control provided or in the event of a security breach have the potential to affect critical infrastructure or cause personal injury.

5.14.5.4 Practice

Not publicly available.

5.14.5.5 Formal Status

None.

5.14.5.6 Relation to other standards / schemes

None.

5.14.6 Online Trust Alliance IoT Trust Framework

5.14.6.1 Focus

The IoT Trust Framework created by the Online Trust Alliance includes a set of strategic principles to help secure IoT devices and their data when shipped and throughout their entire life-cycle. The Framework outlines mandatory requirements and is broken down into four areas:

- Security Principles: Applicable to any device or sensor and all applications and back end cloud services. These range from the application of a rigorous software development

security process to adhering to data security principles for data stored and transmitted by the device, to supply chain management, penetration testing and vulnerability reporting programs. Further principles outline requirements for life-cycle security patching.

- User Access & Credentials: Requirement of encryption of all passwords and user names, shipment of devices with unique passwords, implementation of generally accepted password re-set processes and integration of mechanisms to help prevent “brute” force login attempts.
- Privacy, Disclosures & Transparency: Requirements consistent with generally accepted privacy principles including prominent disclosures on packaging, point of sale and/or posted on line, capability for users to having the ability to reset devices to factory settings and compliance with applicable regulatory requirements including the EU GDPR (ref. [2]) and children’s privacy regulations. Required disclosures include the impact to product features or functionality if connectivity is disabled.
- Notifications & Related Best Practices: Key to maintaining device security is having mechanisms and processes to promptly notify a user of threats and action(s) required. These principles include requiring email authentication for security notifications. In addition messages must be written for maximum user comprehension and tamper-proof packaging and accessibility considerations are recommended.

5.14.6.2 Associated Evaluation Scheme and Governance

There is no associated evaluation scheme.

The Online Trust Alliance (OTA) is a non-profit organisation based in Washington (USA) with the mission to enhance online trust and empower users, while promoting innovation and the vitality of the internet.

5.14.6.3 Process

As there is no evaluation scheme associated with the framework, there is also no process.

5.14.6.4 Practice

The framework is supported by a wide range of organisations. A list of supporters can be found in the following press release:

https://otalliance.org/news-events/press-releases/coalition-embraces-iot-security-privacy-trust-framework.

5.14.6.5 Formal Status

None.

5.14.6.6 Relation to other standards / schemes

None.

5.14.7 OWASP Internet of Things Project

5.14.7.1 Focus

The OWASP Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies. Currently (March 2017), this project is under development.

A set of attack surface areas for IoT devices, and the vulnerabilities related to these attack surface areas, have been defined. The following attack surfaces are included:

- Ecosystem (general)
- Device Memory
- Device Physical Interfaces
- Device Web Interface
- Device Firmware
- Device Network Services
- Administrative Interface
- Local Data Storage
- Cloud Web Interface
- Third-party Backend APIs
- Update Mechanism
- Mobile Application
- Ecosystem Communication
- Network Traffic
- Authentication/Authorization
- Privacy
- Hardware (Sensors)

This serves as the backbone for the framework, and the following ten controls have been defined as being the most important:

- Insecure Web Interface
- Lack of Transport Encryption
- Insufficient Security Configurability
- Poor Physical Security
- Insufficient Authentication / Authorization
- Insecure Cloud Interface
- Insecure Software / Firmware
- Privacy Concerns
- Insecure Mobile Interface
- Insecure Network Services

5.14.7.2 Associated Evaluation Scheme and Governance

At the time of writing the IoT testing guides are still under development

The OWASP Internet of Things Project is open source.

5.14.7.3 Process

None.

5.14.7.4 Practice

Not known.

5.14.7.5 Formal Status

None.

5.14.7.6 Relation to other standards / schemes

None.

5.14.8 Strategic Principles for Securing the Internet of Things (IoT)

5.14.8.1 Focus

The principles set forth below are designed to improve security of IoT across the full range of design, manufacturing, and deployment activities:

- Incorporate Security at the Design Phase
  - Enable security by default
  - Recent operating system
  - Hardware that incorporates security features
  - Design with system and operational disruption in mind
- Promote Security Updates and Vulnerability Management
  - Secure the device over network connections or through automated means
  - Coordinating software updates among third-party vendors
  - Automated mechanisms for addressing vulnerabilities
  - Coordinated disclosure of vulnerabilities
  - End-of-life strategy
- Build on Recognized Security Practices
  - Basic software security and cybersecurity practices
  - Sector-Specific Guidance
  - Practice defence in depth
  - Information sharing platforms
- Prioritize Security Measures According to Potential Impact
  - Intended use and environment

    - Red-teaming" exercise
    - Identify and authenticate the devices connected to the network
- Promote Transparency across IoT
    - Third party vendor risks,
    - Publicly disclosed mechanism for using vulnerability reports
    - Software bill of materials
- Connect Carefully and Deliberately
    - Advise IoT consumers on the intended purpose of any network connections
    - Make intentional connections
    - Build in controls selective connectivity

5.14.8.2 Associated Evaluation Scheme and Governance

There is no associated evaluation scheme.

The Strategic Principles for Securing the Internet of Things is developed by the Department of Homeland Security, a department of the US government.

5.14.8.3 Process

None.

5.14.8.4 Practice

Not publicly known.

5.14.8.5 Formal Status

None.

5.14.8.6 Relation to other standards / schemes

None.

6 Cybersecurity standards and schemes for security professionals

6.1 CompTIA certifications

6.1.1 Focus

The Computing Technology Industry Association (CompTIA) offers a wide variety of certifications, amongst them the CompTIA Security+ certificate. The CompTIA Security+ certification covers network security, compliance and operation security, threats and vulnerabilities as well as application, data and host security. Also included are access control, identity management, and cryptography.

6.1.2 Associated Evaluation Scheme and Governance

CompTIA offers training materials such that the IT professional can prepare for a final exam which will grant the professional a three-year valid certification. This exam consists of both multiple choice questions as well as performance-based questions (PBQs). These PBQs test the ability to solve problems in a simulated environment.

CompTIA is a large non-profit trade organisation and has issued over 2,000,000 IT certifications worldwide. More than 200 IT vendors and IT distributors are members of CompTIA. This vendor and distributor membership program is designed to encourage collaboration and help organisations support their channel. It creates a path to provide educational resources, research, and business tools, and community involvement to solution providers around the globe and enables to grow businesses.

6.1.3 Process

The IT professional may do the final test with or without the provided training. Certification exams are held at test locations of Pearson VUE.

6.1.4 Practice

Companies acknowledging CompTIA certificates include, but are not limited to:

- Apple
- Dell
- HP
- IBM
- Intel
- U.S. Department of Defense

- Booz Allen Hamilton
- Network Solutions
- U.S. Army
- U.S. Navy
- Verizon Telematics

6.1.5 Formal Status

There is no formal status, but employers may require this certificate.

6.1.6 Relation to other standards / schemes

CompTIA Security+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA).

6.2 CREST certifications

6.2.1 Focus

CREST offers certifications within four different areas which can be obtained at different levels. The levels mainly indicate the number of hours of experience of the certificate holder: practitioner (2500 hours), registered tester (6000 hours) and certified tester (10000 hours). Dependent on the area and the level, different skills and knowledge are required:

- **Penetration testing:** A penetration tester identifies security vulnerabilities. Levels and exams

  1. Practitioner security analyst
  2. Registered penetration tester
  3.a. Certified web application tester
  3.b. Certified infrastructure tester
  3.c. Certified wireless specialist
  4.a. Crest simulated attack specialist (red teaming)
  4.b. Crest certified simulated attack manager
- **Threat intelligence** (STAR): These exams are for Simulated Target Attack and Response. Vulnerabilities are identified during a simulated attack after which clients are advised based on the findings. Levels and exams:

  1. Practitioner level (under development)
  2. Registered level (under development)
  3. Crest certified threat intelligence manager
- **Incident response:** Within incident response, evidence of security breaches are identified and appropriate action is taken. Levels and exams:

  1. Practitioner level (under development)
  2. Registered intrusion analyst

3.a. Certified network intrusion analyst
3.b. Certified host intrusion analyst
3.c. Certified malware reverse engineer
3.d. Certified incident manager

- **Technical security architecture:** Within this discipline, secure IT systems and networks are designed and built. Levels and exams:

  1. Practitioner level (under development)
  2. Registered level (under development)
  3. Registered technical security architect

6.2.2 Associated Evaluation Scheme and Governance

CREST is a not-for-profit organisation that serves the needs of a technical information security marketplace that requires the services of a regulated professional services industry.

6.2.3 Process

The certifications are based upon written and practical exams and the examinations are valid for three years.

6.2.4 Practice

A list of UK's CREST members, companies which have been successfully assessed against CREST criteria for the supply of services and have CREST qualified consultants, can be found at http://www.crest-approved.org/uk/members/index.html.

6.2.5 Formal Status

There is no formal status, but employers may require this certificate.

6.2.6 Relation to other standards / schemes

Part of becoming a CREST-registered technical security architect is completing the CCP certification (section 6.9).

6.3 EC-Council certifications

6.3.1 Focus

EC-Council offers certifications within different areas:

- Certified Chief Information Security Officer (CCISO)
  - Governance

    - Security Risk Management, Controls & Audit management
    - Security Program Management & Operations
    - Information Security Core Concepts
    - Strategic Planning, Finance & Vendor Management
- Certified Ethical Hacker (CEH)
    - Look for weaknesses and vulnerabilities in systems using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a system(s).
- Certified Network Defender (CND)
    - Protect, detect and respond approach to network security
- Certified Network Defense Architect (CNDA)
    - The CNDA has been specially designed for Government Agencies around the world. Other than the name the content is exactly the same as the CEH.
- Certified Secure Computer User (CSCU)
    - Fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, virus and backdoors, emails hoaxes, sex offenders lurking online, loss of confidential information, hacking attacks and social engineering.
- Computer Hacking Forensic Investigator (CHFI)
    - Detecting hacking attacks and properly extracting evidence to report a crime and conduct audits to prevent future attacks
- EC-Council Certified Disaster Recovery Professional (EDRP)
    - The ability to plan, organise, and direct the testing of disaster response, recovery support, and business recovery procedures
- EC-Council Certified Encryption Specialist (ECES)
    - The foundations of modern symmetric and key cryptography including the details of algorithms such as Feistel Networks, DES, and AES
- EC-Council Certified Incident Handler (ECIN)
    - Handle various types of incidents, risk assessment methodologies, and various laws and policies related to incident handling
- EC-Council Certified Secure Programmer - Java (ECSP-JAVA)
    - Knowledge of Java security features, policies, strengths, and weaknesses
- EC-Council Certified Secure Programmer - .NET (ECSP-.NET)
    - The ability to identify security flaws and implement security countermeasures throughout the software development life cycle, following the best practices by experienced experts in the various domains
- EC-Council Certified Security Analyst (ECSA)
    - Full exploitation of the skills learned in the CEH by utilizing EC-Council's published penetration testing methodology
- EC-Council Certified Security Specialist (ECSS)
    - The fundamentals of information security, network security, and computer forensics.
- Licensed Penetration Tester (LPT)
    - Show mastery skill of the Reconnaissance phase, where a pen tester gets familiar with the network by observing and scanning, Exploitation phase where the tester, using the intelligence from the previous phase, actually breaks into the network and/or individual machines; and Post-Exploitation phase where data exfiltration,

documentation and effect of exploitation is documented and enumerating leading to deeper vulnerabilities that eventually lead to ownership of the core network and key machines controlling the entire organisations computer systems

6.3.2 Associated Evaluation Scheme and Governance

The EC-Council provides a training with an exam. However, for some exams (like the LPT) the training is to pass other exams (CEH and CSA for LPT).

The International Council of E-Commerce Consultants, also known as EC-Council, is a member-based organisation that certifies individuals in various e-business and information security skills.

6.3.3 Process

Individuals need to pass a theoretical and/or practical exam in order to obtain the certificate. These exams are usually preceded by a training provided by EC-Council.

6.3.4 Practice

Individuals from the following organisations have obtained EC-Council certificates:

- The US Army
- the FBI
- Microsoft
- IBM
- the United Nations

6.3.5 Formal Status

Employees may be required to have EC-Council certifications, including employees from governmental organisations such as the US army and the FBI, giving these certificates a somewhat formal status.

6.3.6 Relation to other standards / schemes

The US Government National Security Agency (NSA) and the Committee on National Security Systems (CNSS) has certified several programs for meeting the 4011, 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals:

4011	National Training Standard for Information Systems Security (INFOSEC)Professionals
4012	National Training Standard for Designated Approving Authority (DAA)
4013	National Training Standard for System Administration in Information Systems Security
4014	National Training Standard for Information Systems Security Officers (ISSO)

4015 National Training Standard for Systems Certifiers

4016 National Training Standard for Risk Analyst

6.4 GIAC certifications

6.4.1 Focus

GIAC offers certifications attesting that an individual has the knowledge and skills necessary for a practitioner in key areas of computer, information and software security within different areas:

- Cyber defense
  - The essential skills and techniques needed to protect and secure an organisation's critical information assets, business systems, and industrial controls.
  - Training courses: 18 | giac certifications: 10
- Penetration testing
  - The identification and assessment of potential attacks and vulnerabilities, and implementation of defenses and immediate responses to contain, mitigate, and remediate risks.
  - Training courses: 13 | giac certifications: 7
- Digital forensics
  - The acquisition and examination of evidence from digital systems to find and recover known artifacts essential to information and systems security.
  - Training courses: 8 | giac certifications: 5
- Application security
  - The design, development, and defense of secure application software and systems.
  - Training courses: 6 | giac certifications: 3
- Management, legal and audit
  - The leadership and management of security teams and risk analysis techniques to conduct a technical audit of essential information systems.
  - Training courses: 14 | giac certifications: 6

6.4.2 Associated Evaluation Scheme and Governance

GIAC (Global Information Assurance Certification) only offers examination, and does not offer training. However, GIAC was founded in 1999 by the SANS Institute (Escal Institute of Advanced Technologies) which provides the required training for these certifications. The SANS institute is a US for-profit organisation

6.4.3 Process

Registration for the exam is sufficient.

6.4.4 Practice

A list of certified professionals can be found at https://www.giac.org/certified-professionals/directory.

6.4.5 Formal Status

None, but employers may require a GIAC certificate for specific jobs.

6.4.6 Relation to other standards / schemes

None

6.5 ISACA certifications

6.5.1 Focus

ISACA offers certifications to IT professionals in different areas:

- Certified Information Systems Auditor (CISA)
  - To audit, control, monitor and assess an organisation's information technology and business systems.
- Certified Information Security Manager (CISM)
  - To design, build and manage enterprise information security programs
- Certified in the Governance of Enterprise IT (CGEIT)
  - Have knowledge and application of enterprise IT governance principles and practices
- Certified in Risk and Information Systems Control (CRISC)
  - A combination of IT risk management and enterprise risk management
- Cyber Security Nexus (CSX) Practitioner
  - Knowledge of the most current cyber security standards

6.5.2 Associated Evaluation Scheme and Governance

ISACA only offers certification of individuals, and no training. However, exam resources are offered and can be bought on the website.

Established in 1969, ISACA is a global non-profit association of 140,000 professionals in 187 countries.

6.5.3 Process

Registration for the exam is sufficient

6.5.4 Practice

ISACA certifications do not seem to be officially recognised by large industrial and governmental parties.

6.5.5 Formal Status

None, but employers may require such a certificate

6.5.6 Relation to other standards / schemes

None

6.6 ISA/IEC 62443 Cybersecurity Certificate Programs

6.6.1 Focus

These certificates assure knowledge and awareness of the ISA/IEC 62443 standard:

- Certificate 1: ISA/IEC 62443 Cybersecurity Fundamentals Specialist
  - Understanding the Current Industrial Security Environment, How Cyberattacks Happen, Creating A Security Program, Risk Analysis, Addressing Risk with Security Policy, Organisation, and Awareness, Addressing Risk with Selected Security Counter Measures, Addressing Risk with Implementation Measures, and Monitoring and Improving the CSMS
- Certificate 2: ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
  - Identify and understand the high-risk vulnerabilities that require mitigation
- Certificate 3: ISA/IEC 62443 Cybersecurity Design Specialist
  - The design and implementation of IACS cybersecurity countermeasures
- Certificate 4: ISA/IEC 62443 Cybersecurity Maintenance Specialist
  - Network diagnostics and troubleshooting, security monitoring and incident response, and maintenance of cybersecurity countermeasures implemented in the Design & Implementation phase
- ISA/IEC 62443 Cybersecurity Expert:
  - Individuals who achieve Certificates 1, 2, 3, and 4 are designated as ISA/IEC 62443 Cybersecurity Experts.

6.6.2 Associated Evaluation Scheme and Governance

ISA offers both training as well as an examination. The International Society of Automation (ISA) is a non-profit professional association active around the world.

6.6.3 Process

The candidate should attend the training and pass the exam.

6.6.4 Practice

ISA standards are accepted worldwide.

6.6.5 Formal Status

Since ISA/IEC 62443 is ISA's own standard, ISA can be regarded as an authority upon the subject which gives formal weight to the certificate.

6.6.6 Relation to other standards / schemes

These certifications are (obviously) related to ISA/IEC 62443, see sections 3.2.1 and 5.2.6.

6.7 (ISC)² certifications

6.7.1 Focus

The International Information System Security Certification Consortium, also known as (ISC)², offers the following certifications:

- Associate

  The Associate of (ISC)² allows those just starting out in the information security workforce to demonstrate their competence in the field. Associates have passed a rigorous (ISC)² certification exam, proving their cybersecurity knowledge, and maintaining their continuing professional education (CPE) requirements while working toward completing the experience requirements to become fully certified

- Certified Information Systems Security Professional (CISSP)

  CISSP recognizes information security leaders with the knowledge and experience to design, develop, and manage the overall security posture of an organization.

- Certified Cloud Security Professional (CCSP)

  CCSP recognizes knowledge and competency in applying best practices to cloud security architecture, design, operations, and service orchestration.

- Systems Security Certified Practitioner (SSCP)

  SSCP recognizes practitioners in information security or IT operational roles with hands-on, technical skills to implement, monitor and administer IT infrastructure in accordance

with information security policies and procedures that ensure data confidentiality, integrity and availability.

- Certified Authorization Professional (CAP)

  CAP recognizes the key qualifications of managers responsible for authorizing and maintaining information systems.

- Certified Secure Software Lifecycle Professional (CSSLP)

  CSSLP recognizes the key qualifications of developers building secure software applications.

- Certified Cyber Forensic Professional (CCFP)

  CCFP recognizes cyber forensics professionals with the knowledge and experience in forensics techniques and procedures to support investigations.

- HealthCare Information Security Privacy Practitioner (HCISPP)

  HCISPP recognizes the key qualifications of healthcare information security and privacy practitioners with the knowledge required to successfully implement, manage, or assess security and privacy controls for healthcare and patient information.

- Information Systems Security Architecture Professional (CISSP)

  Concentrations recognize CISSPs who expand their knowledge into specific subject matter areas such as architecture, engineering, and management.

6.7.2 Associated Evaluation Scheme and Governance

(ISC)² is a non-profit membership association, with over 123,000 members made up of certified cyber, information, software and infrastructure security professionals.

6.7.3 Process

1. Obtain the required experience: apart from the associate certification, all other certifications require working experience
2. Optional: join training offered by (ISC)²
3. Passing the exam
4. Maintaining the certification: Recertification is required every three years

6.7.4 Practice

On the following website the number of members (certified professionals) per country can be found: https://www.isc2.org/member-counts.aspx

6.7.5 Formal Status

None

6.7.6 Relation to other standards / schemes

None

6.8 ISO/IEC 27021 (Competence requirements for ISMS professionals)

6.8.1 Focus

In order to stabilize the market for training and certifying professionals for ISO 27001-related implementation projects and audits, a standard is planned that will lay out the competence requirements for ISMS professionals.

ISO/IEC 27021 concerns the knowledge, skills and competencies required in respect of ISO/IEC 27001, 27002, 27005 and 27007 i.e. the management of information security. The standard does not specify a personal certification or qualification scheme as such, but in effect serves as a reference for the bodies that run such schemes. The standard does not cover auditor competence.

6.8.2 Associated Evaluation Scheme and Governance

There is no official evaluation scheme related to ISO 27021. Various training and certification organizations are already active in the information security field, several of which offer ISO 27001-related courses and qualifications such as the ISO/IEC 27001 Lead Auditor and Lead Implementer designations. At present, these schemes make up their own curricula and assessment criteria with no guidance from ISO/IEC except the other ISO27k standards. ISO/IEC 27021 should provide a degree of commonality between the various qualifications, giving recruiters and employers greater confidence in the quality, competence and suitability of qualified candidates and employees.

6.8.3 Process

None.

6.8.4 Practice

The standard is in preparation and should be published in 2017.

6.8.5 Formal Status

None.

6.8.6 Relation to other standards / schemes

ISO/IEC CD 19896-1 Information technology -- Security techniques -- Competence requirements for information security testers and evaluators -- Part 1: Introduction, concepts and general requirements

ISO/IEC CD 19896-2 Information technology -- Security techniques -- Competence requirements for information security testers and evaluators -- Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

ISO/IEC NP 19896-3 Information technology -- Security techniques -- Competence requirements for information security testers and evaluators -- Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

6.9 NCSC Certified Professional (CCP) certifications

6.9.1 Focus

The CCP is a framework for certifying IT professionals who meet competency and skill requirements for specified roles or responsibilities. It includes a set of role definitions and a certification process and for each role and role level the purpose, skills required, and responsibility are defined:

The set of role definitions covers the most commonly used roles across the public sector, many of which have equivalent roles in the private sector:

- Accreditor
- IA Architect
- IA Auditor
- Communications Security Family of Roles
- Information System Security Officer (ISSO) / Information Security System Manager (ISSM) / IT Security Officer (ITSO)
- Security & Information Risk Advisor (SIRA)

The CCP defines different levels at which the roles will be practiced:

- Practitioner
- Senior Practitioner
- Lead Practitioner

6.9.2 Associated Evaluation Scheme and Governance

The framework has been developed by the CESG (now The National Cyber Security Centre, the NCSC, a department of the UK Government Communications Headquarter, GCHQ) in consultation with government departments, academia, security, industry, the certification bodies, members of the former CESG Listed Advisor Scheme (CLAS) and CREST.

The NCSC acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security, including the management of cyber security incidents. The NCSC's main purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. It does so by working together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management.

The certification process:

- Assesses applicants against the requirements of the role definitions,
- Includes the issue of certificates endorsed by CESG stating the cyber security/IA role and responsibility level at which the applicant has been assessed as having performed competently

6.9.3 Process

The certification process is operated by three Certifying Bodies, appointed by the NCSC.

- APMG: The assessment process for all roles and levels is interview based, incorporating feedback from referees (ex- colleagues), in order to determine whether you meet the competencies expected of the role
- BCS: For the level of practitioner a written submission and exam is sufficient, for the senior and lead levels the exam is replaced with an interview
- IISP: does not provide information about the certification process.

All CCP certifications are valid for three years.

6.9.4 Practice

Currently the scheme is only available to individuals working in the United Kingdom who have a UK address. There is no list of certified persons available online.

6.9.5 Formal Status

It is not required for IT professionals to have the CCP qualification, but employers may require cyber security professionals to have such a qualification. A quick search on monsterboard.co.uk shows that some employers do in fact require persons to be CCP-qualified.

6.9.6 Relation to other standards / schemes

Professionals certified with the CCP often needs to be aware of policies and standards such as the ISO 27000 series on cyber security, the ISO 31000 on Risk management, ISO 22300 on Societal Security, or ISO 9000 on Quality Management.

In order to pass the IA Architect role at Senior/Lead level by the IISP, RHUL and CREST consortium, candidates will need to have passed the CREST Registered Technical Security Architecture (CRTSA) examination (see section 6.9).

7 Further Reading

7.1 European Commission Directives and Regulations

Ref.	Title	Author	Version	Date
[1]	DIRECTIVE (EU) 2016/1148 (concerning measures for a high common level of security of network and information systems across the Union) (Better known as the 'NIS Directive')	EC	-	6 July 2016
[2]	REGULATION (EU) 2016/679 (on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) ('General Data Protection Regulation')	EC	-	27 April 2016
[3]	DIRECTIVE 2013/40/EU (on attacks against information systems)	EC	-	12 August 2013
[4]	DIRECTIVE 2002/58/EC (concerning the processing of personal data and the protection of privacy in the electronic communications sector)	EC	-	12 July 2002
[5]	DIRECTIVE 2009/136/EC (amending Directive 2002/22/EC, Directive 2002/58/EC and Regulation (EC) No 2006/2004)	EC	-	25 November 2009

7.2 ENISA reports

Ref.	Title	Author	Version	Date
[6]	Definition of Cybersecurity – Gaps and overlaps in standardisation	ENISA	1.0	December 2015
[7]	Smart grid security certification in Europe - Challenges and recommendations	ENISA	-	December 2014
[8]	Indispensable baseline security requirements for the procurement of secure ICT products and services	ENISA	1.0	December 2016
[9]	Information Security Certifications - A Primer: Products, people, processes	ENISA	-	December 2007
[10]	Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools	ENISA	-	June 2006
[11]	Secure ICT Procurement in Electronic Communications - Analysis and recommendations for procuring ICT securely	ENISA	-	December 2014

in the Electronic Communications Sector			
[12] Security Guide for ICT Procurement – ICT Procurement Security Guide for Electronic Communications Service Providers	ENISA	-	December 2014
[13] Certification of Cyber Security skills of ICS/SCADA professionals - Good practices and recommendations for developing harmonised certification schemes	ENISA	-	December 2014
[14] Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a	ENISA	2.0	October 2014
[15] Good Practices on Reporting Security Incidents	ENISA	-	December 2009
[16] Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards	ENISA	1.1	June 2016
[17] Protecting Industrial Control Systems - Annex III: ICS Security Related Standards, Guidelines and Policy Documents	ENISA	-	September 2012
[18] Communication network dependencies for ICS/SCADA Systems	ENISA	-	December 2016
[19] Cyber Security and Resilience of smart cars - Good practices and recommendations	ENISA	-	December 2016

7.3 ETSI Technical Reports

Ref.	Title	Author	Version	Date
[1]	ETSI TR 103 306 (CYBER; Global Cyber Security Ecosystem)	ETSI	1.1.1	2015-11
[2]	ETSI TR 103 304 (PII Protection in mobile and cloud services)	ETSI	1.1.1	2016-07
[3]	ETSI TR 103 303 (CYBER; Protection measures for ICT in the context of Critical Infrastructure)	ETSI	1.1.1	2016-04

7.4 Vocabulary

Ref.	Title	Author	Version	Date
[1]	ISO/IEC 2382 (Information technology – Vocabulary)	ISO / IEC	-	2015

Other standards that contain much-used glossaries and definitions of terminology in the area of cybersecurity are:

- ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary; see also section 5.1.8

- IEC 62443-1-1 Industrial communication networks — Network and system security — Part 1-1: Terminology, concepts and models; see also section 3.2.1.
- NIST 800-53; see section 5.6.3.
- NIST IR 7298 Glossary of Key Information Security Terms http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
- ISO SC 27 Standing Document 6 (SD6): Glossary of IT Security Terminology; http://www.din.de/en/meta/jtc1sc27/downloads
- Internet Security Glossary, version 2; https://tools.ietf.org/html/rfc4949
- OWASP glossary; https://www.owasp.org/index.php/Category:Glossary
- SANS glossary; http://www.sans.org/security-resources/glossary-of-terms/

7.5 Other

Ref.	Title	Author	Version	Date
[2]	White Paper No. 01 Recommendations for a Strategy on European Cyber Security Standardisation	CEN/CENELEC/ETSI Cyber Security Coordination Group	01.08	-
[3]	European Commission Rolling Plan for ICT Standardization 2017, esp. pages 29 - 32	EC	-	-

Appendix 1 The JHAS attack rating methodology

The 'JHAS attack rating' refers to a methodology for rating the resistance of a smart card to specific attacks. It was developed by the JIL Hardware Attacks Subgroup (JHAS) and published in a SOG-IS guidance document called 'Application of Attack Potential to Smartcards'. See also section 3.1.3.3. This is a (partially) public document; a limited-distribution companion document called 'Attack Methods for Smart Cards and Similar Devices' describes the attacks themselves.

According to this document, an attack consists of two phases: the identification phase and the exploitation phase. The identification phase corresponds to the effort required to create the

attack, and to demonstrate that it can be successfully applied to the target. The identification phase results in a script that (in more or less detail) describes how to carry out the attack. Using this script, other attackers can replicate the attack in the exploitation phase. Both phases are considered necessary for a successful attack.

The resistance of a smart card to a specific attack can then be rated by measuring a number of factors that are needed to successfully carry out both phases:

- Elapsed time
  - One hour, one week, one month, more
- Expertise
  - Layman, proficient user, expert, multiple experts (in different domains)
- Knowledge of the target
  - Public, restricted, sensitive, critical, very critical (hardware design)
- Availability of samples
  - Public, restricted, sensitive, critical
- Number of samples needed
  - < 10, <100, more
- Equipment
  - None, standard, specialised, bespoke, multiple different bespoke

The JHAS method assigns a number of points to each of these factors. For example, if the identification phase of an attack can be carried out in under a day, this results in 1 point being awarded. If the exploitation phase of that same attack would necessitate access to over a hundred of samples, another 6 points are awarded.

At the end of the evaluation the evaluator has to assess the time, effort, knowledge of the target etc. it would take to carry out the easiest of all the attacks described by the JIL or otherwise envisaged. The number of points resulting from this easiest attack constitutes the JHAS attack rating of that target.

Finally, a certification body can set a minimum rating that is needed to pass the associated security evaluation. For example, EMVCo and the respective payment schemes, as well as Common Criteria using the BSI-CC-PP-0084-2014 protection profile for smart cards, and the MIFARE Security Evaluation all require at least 31 points.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU