

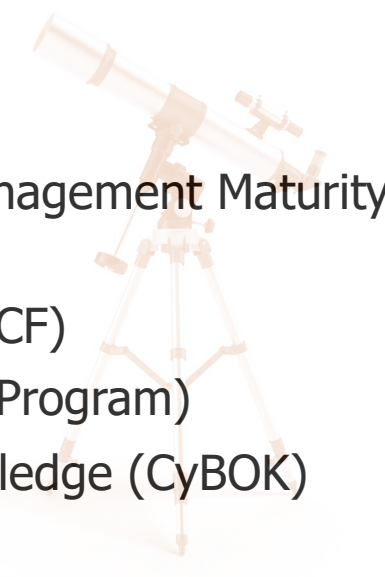
24

Great Cybersecurity Frameworks

1.0 lite, 11.12.2023, Andrey Prozorov
www.patreon.com/AndreyProzorov

Agenda

1. ISO 27001 (ISMS)
2. ISO 27002 (IS Controls)
3. Standard of Good Practice for Information Security (ISF SoGP)
4. NIST Cybersecurity Framework (CSF)
5. NIST SP 800-53 (Security and Privacy Controls)
6. CIS Critical Security Controls
7. PCI DSS
8. Katakri (Information Security Audit Tool for Authorities)
9. COBIT Focus Area: Information Security
10. Information Security Manual (ISM)
11. New Zealand Information Security Manual (NZISM)
12. Essential Cybersecurity Controls (ECC)
13. SAMA Cyber Security Framework
14. Cyber Essentials (UK)
15. IT-Grundschutz
16. CSA Cloud Controls Matrix (CCM)
17. State of the art (TeleTrust)
18. Cybersecurity Capability Maturity Model (C2M2)
19. CyberFundamentals Framework
20. ETSI Cybersecurity Standards
21. HITRUST CSF
22. Open Information Security Management Maturity Model (O-ISM3)
23. Secure Controls Framework (SCF)
24. IEC 62443-2-1 (IACS Security Program)
- The Cyber Security Body Of Knowledge (CyBOK)
- Other



ISO 27001

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ISO/IEC 27001 is the world's best-known standard for **information security management systems (ISMS)**. It defines requirements an ISMS must meet.

The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system.

Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.

Organisation: International Organization for Standardization (ISO)

Price: CHF 124 (\$140)

**Information security, cybersecurity
and privacy protection — Information
security management systems —
Requirements**

*Sécurité de l'information, cybersécurité et protection de la vie
privée — Systèmes de management de la sécurité de l'information —
Exigences*



Contents	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	1
4.1 Understanding the organization and its context.....	1
4.2 Understanding the needs and expectations of interested parties.....	1
4.3 Determining the scope of the information security management system.....	2
4.4 Information security management system.....	2
5 Leadership	2
5.1 Leadership and commitment.....	2
5.2 Policy.....	3
5.3 Organizational roles, responsibilities and authorities.....	3
6 Planning	3
6.1 Actions to address risks and opportunities.....	3
6.1.1 General.....	3
6.1.2 Information security risk assessment.....	4
6.1.3 Information security risk treatment.....	4
6.2 Information security objectives and planning to achieve them.....	5
7 Support	6
7.1 Resources.....	6
7.2 Competence.....	6
7.3 Awareness.....	6
7.4 Communication.....	6
7.5 Documented information.....	6
7.5.1 General.....	6
7.5.2 Creating and updating.....	7
7.5.3 Control of documented information.....	7
8 Operation	7
8.1 Operational planning and control.....	7
8.2 Information security risk assessment.....	8
8.3 Information security risk treatment.....	8
9 Performance evaluation	8
9.1 Monitoring, measurement, analysis and evaluation.....	8
9.2 Internal audit.....	8
9.2.1 General.....	8
9.2.2 Internal audit programme.....	9
9.3 Management review.....	9
9.3.1 General.....	9
9.3.2 Management review inputs.....	9
9.3.3 Management review results.....	9
10 Improvement	10
10.1 Continual improvement.....	10
10.2 Nonconformity and corrective action.....	10
Annex A (normative) Information security controls reference	11
Bibliography	19

ISO 27002

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls

ISO/IEC 27002 is an international standard that provides guidance for organizations looking to establish, implement, and improve an Information Security Management System (**ISMS**) focused on cybersecurity. While ISO/IEC 27001 outlines the requirements for an ISMS, ISO/IEC 27002 offers **best practices and control objectives related to key cybersecurity aspects** including access control, cryptography, human resource security, and incident response.

The standard serves as a practical blueprint for organizations aiming to effectively safeguard their information assets against cyber threats. By following ISO/IEC 27002 guidelines, companies can take a proactive approach to cybersecurity risk management and protect critical information from unauthorized access and loss.

Organisation: International Organization for Standardization (ISO)

Price: CHF 208 (\$240)

INTERNATIONAL
STANDARD

ISO/IEC
27002

Third edition
2022-02

**Information security, cybersecurity
and privacy protection — Information
security controls**

*Sécurité de l'information, cybersécurité et protection de la vie
privée — Mesures de sécurité de l'information*



Reference number
ISO/IEC 27002:2022(E)

© ISO/IEC 2022

ISO/IEC 27002:2022(E)

Contents

	Page
Foreword	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions.....	1
3.2 Abbreviated terms.....	6
4 Structure of this document	7
4.1 Clauses.....	7
4.2 Themes and attributes.....	8
4.3 Control layout.....	9
5 Organizational controls	9
5.1 Policies for information security.....	9
5.2 Information security roles and responsibilities.....	11
5.3 Segregation of duties.....	12
5.4 Management responsibilities.....	13
5.5 Contact with authorities.....	14
5.6 Contact with special interest groups.....	15
5.7 Threat intelligence.....	15
5.8 Information security in project management.....	17
5.9 Inventory of information and other associated assets.....	18
5.10 Acceptable use of information and other associated assets.....	20
5.11 Return of assets.....	21
5.12 Classification of information.....	22
5.13 Labelling of information.....	23
5.14 Information transfer.....	24
5.15 Access control.....	27
5.16 Identity management.....	29
5.17 Authentication information.....	30
5.18 Access rights.....	32
5.19 Information security in supplier relationships.....	33
5.20 Addressing information security within supplier agreements.....	35
5.21 Managing information security in the ICT supply chain.....	37
5.22 Monitoring, review and change management of supplier services.....	39
5.23 Information security for use of cloud services.....	41
5.24 Information security incident management planning and preparation.....	43
5.25 Assessment and decision on information security events.....	44
5.26 Response to information security incidents.....	45
5.27 Learning from information security incidents.....	46
5.28 Collection of evidence.....	46
5.29 Information security during disruption.....	48
5.30 ICT readiness for business continuity.....	48
5.31 Legal, statutory, regulatory and contractual requirements.....	50
5.32 Intellectual property rights.....	51
5.33 Protection of records.....	53
5.34 Privacy and protection of PII.....	54
5.35 Independent review of information security.....	55
5.36 Compliance with policies, rules and standards for information security.....	56
5.37 Documented operating procedures.....	57
6 People controls	58
6.1 Screening.....	58
6.2 Terms and conditions of employment.....	59

© ISO/IEC 2022 – All rights reserved

iii

ISO/IEC 27002:2022(E)

6.3 Information security awareness, education and training.....	60
6.4 Disciplinary process.....	62
6.5 Responsibilities after termination or change of employment.....	63
6.6 Confidentiality or non-disclosure agreements.....	63
6.7 Remote working.....	65
6.8 Information security event reporting.....	66
7 Physical controls	67
7.1 Physical security perimeters.....	67
7.2 Physical entry.....	68
7.3 Securing offices, rooms and facilities.....	70
7.4 Physical security monitoring.....	70
7.5 Protecting against physical and environmental threats.....	71
7.6 Working in secure areas.....	72
7.7 Clear desk and clear screen.....	73
7.8 Equipment siting and protection.....	74
7.9 Security of assets off-premises.....	75
7.10 Storage media.....	76
7.11 Supporting utilities.....	77
7.12 Cabling security.....	78
7.13 Equipment maintenance.....	79
7.14 Secure disposal or re-use of equipment.....	80
8 Technological controls	81
8.1 User endpoint devices.....	81
8.2 Privileged access rights.....	83
8.3 Information access restriction.....	84
8.4 Access to source code.....	86
8.5 Secure authentication.....	87
8.6 Capacity management.....	89
8.7 Protection against malware.....	90
8.8 Management of technical vulnerabilities.....	92
8.9 Configuration management.....	95
8.10 Information deletion.....	97
8.11 Data masking.....	98
8.12 Data leakage prevention.....	100
8.13 Information backup.....	101
8.14 Redundancy of information processing facilities.....	102
8.15 Logging.....	103
8.16 Monitoring activities.....	106
8.17 Clock synchronization.....	108
8.18 Use of privileged utility programs.....	109
8.19 Installation of software on operational systems.....	110
8.20 Networks security.....	111
8.21 Security of network services.....	112
8.22 Segregation of networks.....	113
8.23 Web filtering.....	114
8.24 Use of cryptography.....	115
8.25 Secure development life cycle.....	117
8.26 Application security requirements.....	118
8.27 Secure system architecture and engineering principles.....	120
8.28 Secure coding.....	122
8.29 Security testing in development and acceptance.....	124
8.30 Outsourced development.....	126
8.31 Separation of development, test and production environments.....	127
8.32 Change management.....	128
8.33 Test information.....	129
8.34 Protection of information systems during audit testing.....	130
Annex A (informative) Using attributes	132

ISO/IEC 27002:2022(E)

Annex B (informative) Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013	143
Bibliography	150

ISF SoGP

Standard of Good Practice for Information Security (SOGP), 2022

The most up-to-date, comprehensive and globally adopted security framework.

Exclusive to ISF Members, the SOGP presents **business-oriented information security topics with practical and trusted guidance**. The SOGP helps organisations deliver up-to-date good practice that can be integrated into their business processes, information security programme and policy, risk management and compliance arrangements.

Designed for risk management specialists, information security managers and security practitioners, SOGP helps organisations:

- Be agile when exploiting new opportunities whilst managing the associated risk
- Respond to rapidly evolving threats, avoiding costly incidents, operational impacts and reputational damage
- Identify and meet regulatory and compliance requirements

Organisation: Information Security Forum (ISF)

Price: For members only

ISF

2022

STANDARD OF GOOD PRACTICE

for Information Security



Comprehensive coverage of:
ISO/IEC 27002:2022 • CIS Controls V8 • NIST Cybersecurity Framework V1.1

CONTENTS

Click to navigate

Categories, Areas and Topics in SOGP	4
About the SOGP	7
SOGP: An information security enabler	8
Using the SOGP to manage risk	11
Target audience	13
How to use SOGP products	14
Key features and structure	15
Protecting Information	17
The SOGP 2022	
1 SG: Security Governance	19
2 IR: Information Risk Assessment	35
3 SM: Security Management	63
4 PM: People Management	91
5 IM: Information Management	117
6 PA: Physical Asset Management	141
7 SD: System Development	169
8 BA: Business Application Management	207
9 SA: System Access	223
10 SY: System Management	253
11 NC: Networks and Communications	277
12 SC: Supply Chain Management	301
13 TS: Technical Security Management	321
14 TM: Threat and Incident Management	343
15 PE: Physical and Environmental Management	371
16 BC: Business Continuity	387
17 AS: Security Assurance	407
Appendices	
A: Guidelines for Information Security	432
B: Information Asset Categories	437
C: The ISF Asset Model	439
D: The ISF Threat Event Catalogue	440
E: Information Security-related Standards and Frameworks	449
Index	452
Feedback	460
Services	461

Key features and structure

Fundamental and Specialised controls

The **SOGP** makes a distinction between those Topics that are considered 'Fundamental' and those that are considered 'Specialised'. This classification makes it easier to identify essential security arrangements likely to be relevant for most organisations, distinguishing them from those that depend on other factors that are not universal.

FUNDAMENTAL Topics are information security arrangements that are generally applied by ISF Members to form the foundation of their information security programme.

SPECIALISED Topics are information security arrangements that depend on subjective factors – such as the business environment and technology deployed – and are less likely to apply universally. Examples include **Virtualisation, Security Operation Centres** and **Industrial Control Systems**.

Structure

The **SOGP** is consistent with the structure and flow of the ISO/IEC 27000 suite of standards, and is suitable for those organisations that choose to use it as an enabler for ISO compliance or certification, or to implement one or more Information Security Management Systems (ISMSs).



FIGURE 4: The structure of the SOGP

The **SOGP** sets out statements of good practice as a series of 142 'Topics' or business activities, which are grouped into 34 higher-level 'Areas' and 17 'Categories'. Each of the 142 Topics contains a set of good practice controls relevant to that particular activity from an information security perspective.

The structure of the **SOGP** enables organisations to explore or examine specific areas of interest/concern (such as **Securing Cloud Services, Security Assurance, or Security Operation Centres**).

To facilitate assessment against the **SOGP**, the **Benchmark** provides questionnaires that reflect the structure and content described above.

NIST CSF

NIST Cybersecurity Framework (CSF)

V.1.1, April 2018. CSF 2.0 Draft is also published

The NIST Cybersecurity Framework can help an organization **begin or improve** their **cybersecurity program**.

Built off of practices that are known to be effective, it can help organizations improve their cybersecurity posture. It fosters communication among both internal and external stakeholders about cybersecurity, and for larger organizations, helps to better integrate and align cybersecurity risk management with broader enterprise risk management processes as described in the NISTIR 82865 series.

The Framework is organized by five key Functions – **Identify, Protect, Detect, Respond, Recover**. These five widely understood terms, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity risk over time.

Organisation: National Institute of Standards and Technology (NIST)

Price: Free

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

April 16, 2018

Cybersecurity Framework

Version 1.1

Table of Contents

Note to Readers on the Update	ii
Acknowledgements	iv
Executive Summary	v
1.0 Framework Introduction	1
2.0 Framework Basics	6
3.0 How to Use the Framework	13
4.0 Self-Assessing Cybersecurity Risk with the Framework	20
Appendix A: Framework Core	22
Appendix B: Glossary	45
Appendix C: Acronyms	48

List of Figures

Figure 1: Framework Core Structure	6
Figure 2: Notional Information and Decision Flows within an Organization	12
Figure 3: Cyber Supply Chain Relationships	17

List of Tables

Table 1: Function and Category Unique Identifiers	23
Table 2: Framework Core	24
Table 3: Framework Glossary	45

This publication is available free of charge from: <https://doi.org/10.6028/NIST.CSWP.04162018>

vii



The NIST Cybersecurity Framework 2.0

Initial Public Draft

National Institute of Standards and Technology

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.CSWP.29.ipd>

August 8, 2023

NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations

September 2020 (includes updates as of Dec. 10, 2020)

This publication provides a **catalog of security and privacy controls** for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks.

NIST SP 800-53

The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The controls address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines. Finally, the consolidated control catalog addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls).

Organisation: National Institute of Standards and Technology (NIST)

Price: Free

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53r5>

Table of Contents

CHAPTER ONE INTRODUCTION	1
1.1 PURPOSE AND APPLICABILITY	2
1.2 TARGET AUDIENCE	3
1.3 ORGANIZATIONAL RESPONSIBILITIES	3
1.4 RELATIONSHIP TO OTHER PUBLICATIONS	5
1.5 REVISIONS AND EXTENSIONS	5
1.6 PUBLICATION ORGANIZATION	5
CHAPTER TWO THE FUNDAMENTALS	7
2.1 REQUIREMENTS AND CONTROLS	7
2.2 CONTROL STRUCTURE AND ORGANIZATION	8
2.3 CONTROL IMPLEMENTATION APPROACHES	11
2.4 SECURITY AND PRIVACY CONTROLS	13
2.5 TRUSTWORTHINESS AND ASSURANCE	14
CHAPTER THREE THE CONTROLS	16
3.1 ACCESS CONTROL	18
3.2 AWARENESS AND TRAINING	59
3.3 AUDIT AND ACCOUNTABILITY	65
3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING	83
3.5 CONFIGURATION MANAGEMENT	96
3.6 CONTINGENCY PLANNING	115
3.7 IDENTIFICATION AND AUTHENTICATION	131
3.8 INCIDENT RESPONSE	149
3.9 MAINTENANCE	162
3.10 MEDIA PROTECTION	171
3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION	179
3.12 PLANNING	194
3.13 PROGRAM MANAGEMENT	203
3.14 PERSONNEL SECURITY	222
3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY	229
3.16 RISK ASSESSMENT	238
3.17 SYSTEM AND SERVICES ACQUISITION	249
3.18 SYSTEM AND COMMUNICATIONS PROTECTION	292
3.19 SYSTEM AND INFORMATION INTEGRITY	332
3.20 SUPPLY CHAIN RISK MANAGEMENT	363
REFERENCES	374
APPENDIX A GLOSSARY	394
APPENDIX B ACRONYMS	424
APPENDIX C CONTROL SUMMARIES	428

CIS Critical Security Controls

CIS Critical Security Controls (CIS Controls)

v.8, May 2021

The CIS Critical Security Controls (CIS Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. The CIS Controls are a relatively **short list of high-priority, highly effective defensive actions** that provide a “must-do, do-first” starting point for every enterprise seeking to improve their cyber defense.

Prioritization is a key benefit to the CIS Controls. They were designed to help organizations rapidly define the starting point for their defenses, direct their scarce resources on actions with immediate and high-value payoff, and then focus their attention and resources on additional risk issues that are unique to their business or mission.

Organisation: Center for Internet Security (CIS)

Price: Free

CIS Critical Security Controls[®]

Version 8



Contents

Glossary	iv
Acronyms and Abbreviations	vii
Overview	
Introduction	1
Evolution of the CIS Controls	1
This Version of the CIS Controls	3
The CIS Controls Ecosystem ("It's not about the list")	4
How to Get Started	5
Using or Transitioning from Prior Versions of the CIS Controls	5
Structure of the CIS Controls	5
Implementation Groups	6
CIS Critical Security Controls	
Control 01 Inventory and Control of Enterprise Assets	8
Why is this Control critical?	8
Procedures and tools	9
Safeguards	10
Control 02 Inventory and Control of Software Assets	11
Why is this Control critical?	11
Procedures and tools	12
Safeguards	12
Control 03 Data Protection	14
Why is this Control critical?	14
Procedures and tools	15
Safeguards	15
Control 04 Secure Configuration of Enterprise Assets and Software	17
Why is this Control critical?	17
Procedures and tools	18
Safeguards	19
Control 05 Account Management	20
Why is this Control critical?	20
Procedures and tools	21
Safeguards	21

Control 06 Access Control Management	23
Why is this Control critical?	23
Procedures and tools	24
Safeguards	24
Control 07 Continuous Vulnerability Management	26
Why is this Control critical?	26
Procedures and tools	27
Safeguards	28
Control 08 Audit Log Management	29
Why is this Control critical?	29
Procedures and tools	29
Safeguards	30
Control 09 Email and Web Browser Protections	31
Why is this Control critical?	31
Procedures and tools	31
Safeguards	32
Control 10 Malware Defenses	34
Why is this Control critical?	34
Procedures and tools	34
Safeguards	35
Control 11 Data Recovery	36
Why is this Control critical?	36
Procedures and tools	37
Safeguards	37
Control 12 Network Infrastructure Management	38
Why is this Control critical?	38
Procedures and tools	38
Safeguards	39
Control 13 Network Monitoring and Defense	40
Why is this Control critical?	40
Procedures and tools	41
Safeguards	41
Control 14 Security Awareness and Skills Training	43
Why is this Control critical?	43
Procedures and tools	43
Safeguards	44

Control 15 Service Provider Management	46
Why is this Control critical?	46
Procedures and tools	47
Safeguards	47
Control 16 Application Software Security	49
Why is this Control critical?	49
Procedures and tools	50
Safeguards	52
Control 17 Incident Response Management	54
Why is this Control critical?	54
Procedures and tools	55
Safeguards	55
Control 18 Penetration Testing	57
Why is this Control critical?	57
Procedures and tools	58
Safeguards	59

Appendix

Resources and References	A1
Controls and Safeguards Index	A3

PCI DSS

Payment Card Industry Data Security Standard

v.4.0, March 2022

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance **payment card account data security** and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a **baseline of technical and operational requirements designed to protect account data**. While specifically designed to focus on environments with payment card account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem.

Organisation: PCI Security Standards Council (PCI SSC)

Price: Free



Payment Card Industry Data Security Standard

Requirements and Testing Procedures

Version 4.0

March 2022

Table of Contents

1	Introduction and PCI Data Security Standard Overview	1
2	PCI DSS Applicability Information	4
3	Relationship between PCI DSS and PCI SSC Software Standards	7
4	Scope of PCI DSS Requirements	9
5	Best Practices for Implementing PCI DSS into Business-as-Usual Processes	19
6	For Assessors: Sampling for PCI DSS Assessments	22
7	Description of Timeframes Used in PCI DSS Requirements	25
8	Approaches for Implementing and Validating PCI DSS	28
9	Protecting Information About an Entity's Security Posture	31
10	Testing Methods for PCI DSS Requirements	32
11	Instructions and Content for Report on Compliance	33
12	PCI DSS Assessment Process	34
13	Additional References	35
14	PCI DSS Versions	36
15	Detailed PCI DSS Requirements and Testing Procedures	37
	Build and Maintain a Secure Network and Systems	39
	Requirement 1: Install and Maintain Network Security Controls	39
	Requirement 2: Apply Secure Configurations to All System Components	60
	Protect Account Data	73
	Requirement 3: Protect Stored Account Data	73
	Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	102
	Maintain a Vulnerability Management Program	111
	Requirement 5: Protect All Systems and Networks from Malicious Software	111
	Requirement 6: Develop and Maintain Secure Systems and Software	124
	Implement Strong Access Control Measures	149
	Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know	149
	Requirement 8: Identify Users and Authenticate Access to System Components	161

Requirement 9: Restrict Physical Access to Cardholder Data	190
Regularly Monitor and Test Networks	212
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	212
Requirement 11: Test Security of Systems and Networks Regularly	231
Maintain an Information Security Policy	259
Requirement 12: Support Information Security with Organizational Policies and Programs	259
Appendix A Additional PCI DSS Requirements	298
Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers	298
Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS PCI Terminal Connections	304
Appendix A3: Designated Entities Supplemental Validation (DESV)	308
Appendix B Compensating Controls	330
Appendix C Compensating Controls Worksheet	332
Appendix D Customized Approach	333
Appendix E Sample Templates to Support Customized Approach	335
Appendix F Leveraging the PCI Software Security Framework to Support Requirement 6	341
Appendix G PCI DSS Glossary of Terms, Abbreviations, and Acronyms	344

Katakri

Information security auditing tool for authorities – Katakri, 2020

Katakri is the authorities' auditing tool, which an authority can use in assessing the target organisation's ability to protect an authority's classified information.

Katakri can be used as an auditing tool when assessing a company's security arrangements in the facility security clearance and in evaluations of the security of the authorities' information systems. It can also be used to help companies, organisations and the authorities in other security work and its development.

Katakri is used with the aim of ensuring that the target organisation has **adequate security arrangements to prevent the disclosure of an authority's classified information** in all of the environments where the information is handled.

Organisation: National Security Authority of Finland

Price: Free

Katakri 2020

Information Security Audit Tool for Authorities

National Security Authority of Finland



Contents

Introduction	5
The structure of Katakri	5
Principal of usage	6
Competent authorities in supported use cases	6
Area of application	7
Subdivision T: Security Management	8
Administrative information security measures	9
Personnel security	17
Subdivision F: Physical Security	22
General requirements	24
Requirements for Security Areas	33
Data security requirements	57
Subdivision I: Information Assurance	63
Communications Security	65
System Security	75
Operations Security	94
ANNEX I: Facility Security Clearance procedure	107
ANNEX II: Assessment of information systems	109
ANNEX III: Security assessment using Katakri Security Model	114

COBIT Focus Area: Information Security

COBIT Focus Area: Information Security, 2020

The publication provides **guidance related to information security and how to apply COBIT to specific information security topics/practices** within an enterprise. The publication is based on the COBIT core guidance for governance and management objectives, and enhances the core guidance by highlighting security-specific practices and activities as well as providing information security-specific metrics.

Key publication details include:

- Provides a contemporary view on information security governance and management
- Clarifies roles of governance and management and shows how they relate to each other in the context of information security
- Provides a clear end-to-end view into distinction within the enterprise and during all process steps between information security governance and information security management practices
- Provides a comprehensive and holistic guidance on information security – not only to processes but to all components in an enterprise, including organization structure, skills, policies, etc.
- Additional information security-specific activities, metrics and information flows.

Organisation: ISACA

Price: \$50 (for members) / \$90

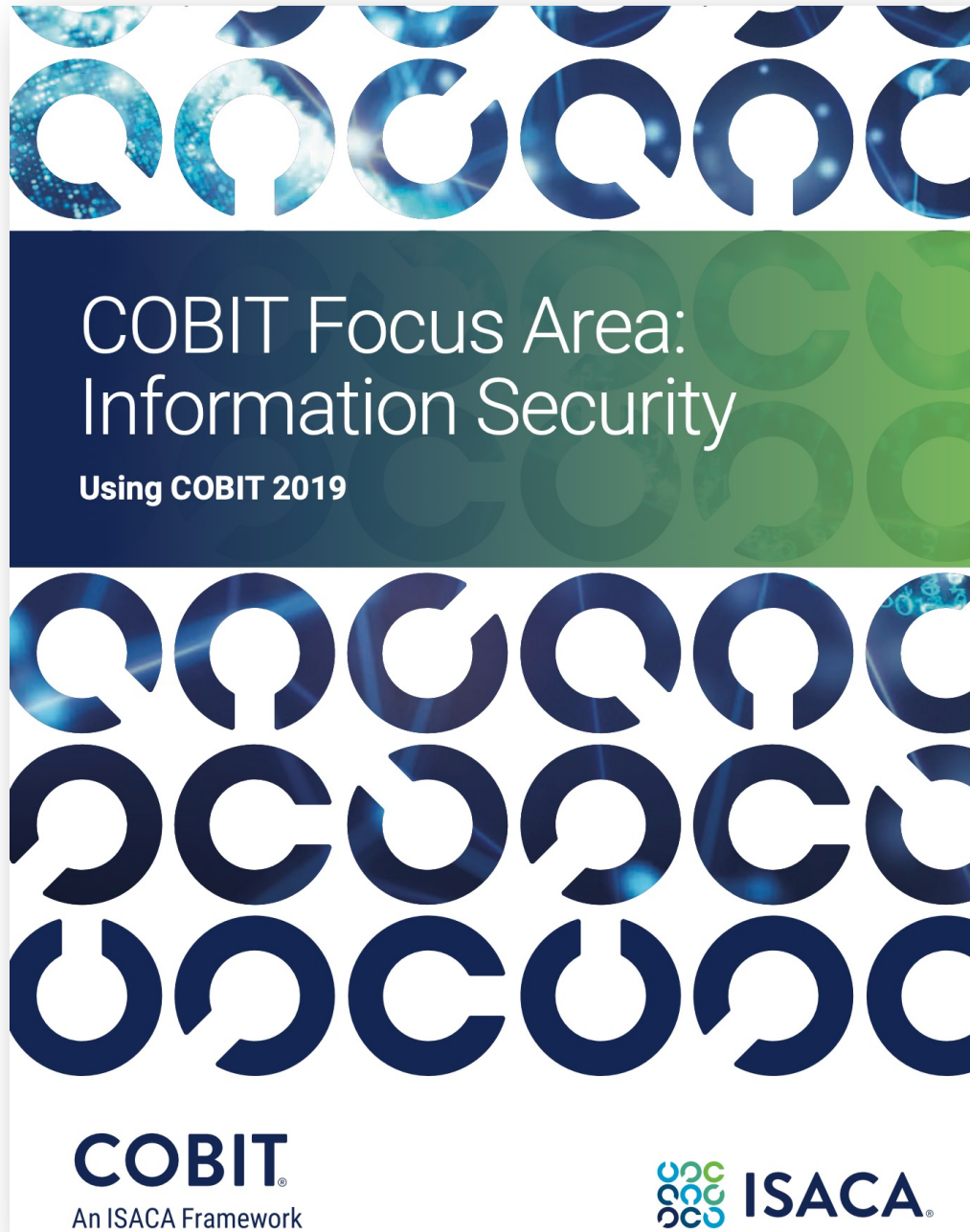


TABLE OF CONTENTS

TABLE OF CONTENTS

List of Figures7

Chapter 1. Introduction.....9

- 1.1 COBIT as an Information and Technology (I&T) Governance Framework9
 - What Is COBIT and What Is It Not?9
- 1.2 COBIT Overview10
- 1.3 Terminology and Key Concepts of the COBIT Framework11
 - 1.3.1 Governance and Management Objectives11
 - 1.3.2 Components of the Governance System12
 - 1.3.3 Focus Areas14
- 1.4 Information Security Focus Area Overview14
 - 1.4.1 Drivers15
 - 1.4.2 Benefits16

Chapter 2. Structure of This Publication and Intended Audience19

- 2.1 Structure of This Publication19
- 2.2 Intended Audience19

Chapter 3. Structure of COBIT Governance and Management Objectives21

- 3.1 Introduction21
- 3.2 Governance and Management Objectives21
- 3.3 Component: Process22
- 3.4 Component: Organizational Structures23
 - 3.4.1 Introduction23
 - 3.4.2 Key Organizational Structures and Roles for Information Security27
- 3.5 Component: Information Flows and Items31
- 3.6 Component: People, Skills and Competencies38
- 3.7 Component: Principles, Policies and Procedures44
 - 3.7.1 Principles44
 - 3.7.2 Policies47
- 3.8 Component: Culture, Ethics and Behavior50
- 3.9 Component: Services, Infrastructure and Applications54

Chapter 4. COBIT Governance and Management Objectives—Detailed Information Security-specific Guidance.....57

- 4.1 Evaluate, Direct and Monitor (EDM)57
- 4.2 Align, Plan and Organize (APO)71
- 4.3 Build, Acquire and Implement (BAI)119
- 4.4 Deliver, Service and Support (DSS)159
- 4.5 Monitor, Evaluate and Assess (MEA)181

Information Security Manual (ISM)

Information Security Manual (ISM)

Published: 1 December 2023

The purpose of the ISM is to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats.

The ISM is intended for Chief Information Security Officers, Chief Information Officers, cyber security professionals and information technology managers.

Organisation: Australian Signals Directorate (ASD) / Australian Cyber Security Centre (ACSC)

Price: Free



Australian Government
Australian Signals Directorate

ACSC Australian
Cyber Security
Centre

Information Security Manual

Published: 22 June 2023

cyber.gov.au

ACSC Australian
Cyber Security
Centre

Table of Contents

Using the Information Security Manual	1
Executive summary	1
Applying a risk-based approach to cyber security	2
Cyber Security Principles	5
The cyber security principles	5
Guidelines for Cyber Security Roles	7
Chief Information Security Officer	7
System owners	10
Guidelines for Cyber Security Incidents	11
Managing cyber security incidents	11
Responding to cyber security incidents	14
Guidelines for Procurement and Outsourcing	17

cyber.gov.au

AC

[Guidelines for Communications Infrastructure](#)

Cabling infrastructure	
Emanation security	
Guidelines for Communications Systems	
Telephone systems	
Video conferencing and Internet Protocol telephony	
Fax machines and multifunction devices	

[Guidelines for Enterprise Mobility](#)

Mobile device management	56
Mobile device usage	59
Guidelines for Evaluated Products	63
Evaluated product procurement	63
Evaluated product usage	65
Guidelines for ICT Equipment	66
ICT equipment usage	66
ICT equipment maintenance and repairs	68
ICT equipment sanitisation and destruction	69
ICT equipment disposal	72
Guidelines for Media	73
Media usage	73
Media sanitisation	75
Media destruction	78
Media disposal	81
Guidelines for System Hardening	82

cyber.gov.au

Operating system hardening	82
User application hardening	88
Server application hardening	91
Authentication hardening	95
Virtualisation hardening	101
Guidelines for System Management	103
System administration	103
System patching	105
Data backup and restoration	108
Guidelines for System Monitoring	111
Event logging and monitoring	111
Guidelines for Software Development	113
Application development	113
Web application development	116

[Guidelines for Database Systems](#)

Database servers	
Databases	
Guidelines for Email	
Email usage	
Email gateways and servers	
Guidelines for Networking	
Network design and configuration	
Wireless networks	
Service continuity for online services	

cyber.gov.au

ACSC Australian
Cyber Security
Centre

ACSC Australian
Cyber Security
Centre

[Guidelines for Cryptography](#)

Cryptographic fundamentals	140
ASD-Approved Cryptographic Algorithms	143
ASD-Approved Cryptographic Protocols	146
Transport Layer Security	147
Secure Shell	148
Secure/Multipurpose Internet Mail Extension	150
Internet Protocol Security	150

[Guidelines for Gateways](#)

Gateways	153
Cross Domain Solutions	156
Firewalls	158
Diodes	158
Web proxies	159
Web content filters	160
Content filtering	161
Peripheral switches	163
Guidelines for Data Transfers	165
Data transfers	165
Cyber Security Terminology	168
Glossary of abbreviations	168
Glossary of cyber security terms	172

cyber.gov.au

Information Security Manual (ISM)

New Zealand Information Security Manual (NZISM)

Version 3.6, September 2022

The New Zealand Information Security Manual (NZISM) is the New Zealand Government's manual on information assurance and information systems security.

The NZISM is a practitioner's manual designed to meet the needs of agency information security executives as well as vendors, contractors and consultants who provide services to agencies.

Organisation: New Zealand Government

Price: Free

1. About information security

1.1. Understanding and using this Manual

Objective

1.1.1. The New Zealand Information Security Manual details processes and controls essential for the protection of all New Zealand Government information and systems. Controls and processes representing good practice are also provided to enhance the baseline controls. Baseline controls are minimum acceptable levels of controls and are often described as "systems hygiene".

Context

Scope

1.1.2. This manual is intended for use by New Zealand Government departments, agencies and organisations. Crown entities, local government and private sector organisations are also encouraged to use this manual.

1.1.3. This section provides information on how to interpret the content and the layout of content within this manual.

1.1.4. Information that is Official Information or protectively marked UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE or RESTRICTED is subject to a single set of controls in this NZISM. These are essential or minimum acceptable levels of controls (baseline controls) and have been consolidated into a single set for simplicity, effectiveness and efficiency.

1.1.5. All baseline controls will apply to all government systems, related services and information. In addition, information classified CONFIDENTIAL, SECRET or TOP SECRET has further controls specified in this NZISM.

1.1.6. Where the category "All Classifications" is used to define the scope of rationale and controls in the Manual, it includes any information that is Official Information, UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET or any endorsements, releasability markings or other qualifications appended to these categories and classifications.

The purpose of this Manual

1.1.7. The purpose of this manual is to provide a set of essential or baseline controls and additional good and recommended practice controls for use by government agencies. The use or non-use of good practice controls MUST be based on an agency's assessment and determination of residual risk related to information security.

1.1.8. This manual is updated regularly. It is therefore important that agencies ensure that they are using the latest version of this Manual.

Target audience

1.1.9. The target audience for this manual is primarily security personnel and practitioners within, or contracted to, an agency. This includes, but is not limited to:

- security executives;
- security and information assurance practitioners;
- IT Security Managers;
- Departmental Security Officers; and
- service providers.

Structure of this Manual

1.1.10. This manual seeks to present information in a consistent manner. There are a number of headings within each section, described below.

- Objective – the desired outcome when controls within a section are implemented.
- Context – the scope, applicability and any exceptions for a section.
- References – references to external sources of information that can assist in the interpretation or implementation of controls.
- Rationale & Controls
 - Rationale – the reasoning behind controls and compliance requirements.
 - Control – risk reduction measures with associated compliance requirements.

1.1.11. This section provides a summary of key structural elements of this manual. The detail of processes and controls is provided in subsequent chapters. It is important that reference is made to the detailed processes and controls in order to fully understand key risks and appropriate mitigations.

The New Zealand Government Security Classification System

1.1.12. The requirements for classification of government documents and information are based on the **Cabinet Committee Minute EXG (00) M 20/7** and **CAB (00) M42/4G(4)**. The Protective Security Requirements (PSR) **INFOSEC2** require agencies to use the **NZ Government Security Classification System** and the NZISM for the classification, protective marking and handling of information assets. For more information on classification, protective marking and handling instructions, refer to the **Protective Security Requirements, NZ Government Security Classification System**.

Key definitions

Accreditation Authority

Contents

- 1. About information security
 - + 1.1. Understanding and using the NZISM
 - + 1.2. Applicability, Authority and Compliance
- + 2. Information Security Services within Government
- + 3. Information security governance - roles and responsibilities
- + 4. System Certification and Accreditation
- + 5. Information security documentation
- + 6. Information security monitoring
- + 7. Information Security Incidents
- + 8. Physical Security
- + 9. Personnel Security
- + 10. Infrastructure
- + 11. Communications Systems and Devices
- + 12. Product Security
- + 13. Media and IT Equipment Management, Decommissioning and Disposal
- + 14. Software security
- + 15. Email security
- + 16. Access Control and Passwords
- + 17. Cryptography
- + 18. Network security
- + 19. Gateway security
- + 20. Data management
- + 21. Distributed Working
- + 22. Enterprise systems security
- + 23. Public Cloud Security
- + 24. Supporting Information

Essential Cybersecurity Controls (ECC)

Essential Cybersecurity Controls (ECC – 1: 2018)

The Essential Cybersecurity Controls has developed to set the **minimum cybersecurity requirements** based on best practices and standards to minimize the cybersecurity risks to the information and technical assets of organizations that originate from internal and external threats. The Essential Cybersecurity Controls consist of 114 main controls, divided into five main domains: Cybersecurity Governance, Cybersecurity Defense, Cybersecurity Resilience, Third-party and Cloud Computing Cybersecurity, Industrial Control Systems Cybersecurity.

The Essential Cybersecurity Controls are mandatory where all organizations, within the scope of these controls must implement whatever necessary to ensure continuous compliance with the controls.

Organisation: National Cybersecurity Authority, Saudi Arabia

Price: Free



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Essential Cybersecurity Controls (ECC – 1 : 2018)

Sharing Indicator : **White**
Document Classification: **Unclassified**

Table of Contents

Executive Summary	6
Introduction	7
Objectives	8
Scope of Work and Applicability	9
ECC Scope of Work	9
ECC Statement of Applicability	9
Implementation and Compliance	10
Evaluation and Compliance Tool	10
Update and Review	10
ECC Domains and Structure	11
Main Domains	11
Subdomains	12
Structure	13
The Essential Cybersecurity Controls (ECC)	14
1- Cybersecurity Governance	14
2- Cybersecurity Defense	19
3- Cybersecurity Resilience	26
4- Third-Party and Cloud Computing Cybersecurity	27
5- Industrial Control Systems Cybersecurity	29
Appendices	30
Appendix (A): Terms and Definitions	30
Appendix (B): List of the Abbreviations	36
List of the Tables	
Table (1): ECC Structure	13
Table (2): Terms and Definitions	30
Table (3): List of Abbreviations	36
List of the Figures & Illustrations	
Figure (1): ECC Main Domains	11
Figure (2): ECC Subdomains	12
Figure (3): Controls Coding Scheme	13
Figure (4): ECC Structure	13

SAMA Cyber Security Framework

v.1.0, May 2017

The issuance of a Framework seeks to support our regulated entities in their efforts to have an appropriate cyber security governance and to build a robust infrastructure along with the necessary detective and preventive controls. The Framework articulates appropriate controls and provides guidance on how to assess maturity level.

The adoption and implementation of the Framework is a vital step for ensuring that Saudi Arabian Banking, Insurance and Financing Companies sectors can manage and withstand cyber security threats.

Organisation: Saudi Arabian Monetary Authority (SAMA)

Price: Free

SAMA Cyber Security
Framework



Cyber Security Framework

Saudi Arabian Monetary Authority

Version 1.0

May 2017



Contents

1	Introduction	5
1.1	Introduction to the Framework	5
1.2	Definition of Cyber Security	5
1.3	Scope	6
1.4	Applicability	6
1.5	Responsibilities	7
1.6	Interpretation	7
1.7	Target Audience	7
1.8	Review, Updates and Maintenance	7
1.9	Reading Guide	7
2	Framework Structure and Features	8
2.1	Structure	8
2.2	Principle-based	9
2.3	Self-Assessment, Review and Audit	9
2.4	Cyber Security Maturity Model	10
2.4.1	Maturity Level 3	10
2.4.2	Maturity Level 4	11
2.4.3	Maturity Level 5	12
3	Control domains	13
3.1	Cyber Security Leadership and Governance	13
3.1.1	Cyber Security Governance	13
3.1.2	Cyber Security Strategy	14
3.1.3	Cyber Security Policy	14
3.1.4	Cyber Security Roles and Responsibilities	15
3.1.5	Cyber Security in Project Management	17
3.1.6	Cyber Security Awareness	17
3.1.7	Cyber Security Training	18
3.2	Cyber Security Risk Management and Compliance	19
3.2.1	Cyber Security Risk Management	19
3.2.2	Regulatory Compliance	22
3.2.3	Compliance with (inter)national industry standards	22
3.2.4	Cyber Security Review	22



3.2.5	Cyber Security Audits	23
3.3	Cyber Security Operations and Technology	24
3.3.1	Human Resources	24
3.3.2	Physical Security	24
3.3.3	Asset Management	25
3.3.4	Cyber Security Architecture	25
3.3.5	Identity and Access Management	26
3.3.6	Application Security	27
3.3.7	Change Management	27
3.3.8	Infrastructure Security	28
3.3.9	Cryptography	29
3.3.10	Bring Your Own Device (BYOD)	30
3.3.11	Secure Disposal of Information Assets	30
3.3.12	Payment Systems	31
3.3.13	Electronic Banking Services	31
3.3.14	Cyber Security Event Management	33
3.3.15	Cyber Security Incident Management	33
3.3.16	Threat Management	34
3.3.17	Vulnerability Management	35
3.4	Third Party Cyber Security	36
3.4.1	Contract and Vendor Management	36
3.4.2	Outsourcing	37
3.4.3	Cloud Computing	37
	Appendices	39
	Appendix A - Overview previous issued SAMA circulars	40
	Appendix B - How to request an Update to the Framework	41
	Appendix C - Framework Update request form	42
	Appendix D - How to request a Waiver from the Framework	43
	Appendix E - Framework Waiver request form	44
	Appendix F - Glossary	45

Cyber Essentials (UK)

Cyber Essentials: Requirements for IT infrastructure

v.3.1, April 2023

Cyber Essentials helps you **to guard against the most common cyber threats** and **demonstrate your commitment to cyber security**.

Cyber Essentials is an effective, Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

There are two levels of certification:

- Cyber Essentials (self-assessment)
- Cyber Essentials Plus (+technical verification)

Organisation: National Cyber Security Centre, UK

Price: Free

Cyber Essentials: Requirements for IT infrastructure v3.1

Contents

What's new in this version.....	3
A. Introducing the technical controls.....	3
B. Definitions.....	3
C. Scope.....	4
Scope overview.....	4
Asset management and Cyber Essentials.....	4
(i) Bring your own device (BYOD).....	5
(ii) Home working.....	5
(iii) Wireless devices.....	6
(iv) Cloud services.....	6
(v) Accounts used by third parties and managed infrastructure.....	7
(vi) Devices used by third parties.....	7
(vii) Web applications.....	7
D. Requirements by technical control theme.....	8
1. Firewalls.....	8
Aim.....	8
Introduction.....	8
Requirements.....	8
2. Secure configuration.....	9
Aim.....	9
Introduction.....	9
Requirements.....	9
3. Security update management.....	10
Aim.....	10
Introduction.....	10
Requirements.....	10
4. User access control.....	11
Aim.....	11
Introduction.....	11
Requirements.....	12
Password-based authentication.....	12
Multi-factor authentication (MFA).....	13
5. Malware protection.....	13

Aim.....	13
Introduction.....	13
Requirements.....	14
E. Further guidance.....	14
Backing up your data.....	14
Zero trust and Cyber Essentials.....	14

IT-Grundschutz

IT-Grundschutz. A systematic basis for information security

v.1.0, 2017

As a sound and sustainable methodology for information security management systems (**ISMS**), IT-Grundschutz covers technical, organisational, infrastructural and personnel aspects in equal measure. With its broad foundation, IT-Grundschutz offers a **systematic approach to information security** that is compatible to ISO/IEC 27001.

With the BSI Standards, IT-Grundschutz offers essential publications for all kinds of institutions who want to set up an ISMS:

- BSI Standard 200-1 defines the general requirements for an ISMS
- BSI Standard 200-2 explains how an ISMS can be built based on one of three different approaches
- BSI Standard 200-3 contains all risk-related tasks
- BSI Standard 200-4 covers Business Continuity Management (BCM)
- Guide to Basic Protection based on IT - Grundschutz

Organisation: Federal Office for Information Security (BSI), Germany

Price: Free

BSI-Standard 200-1

Information Security Management Systems (ISMS)

www.bsi.bund.de/grundschutz

Version 1.0

Table of contents

Table of contents

Table of contents	4
1 Introduction	6
1.1 Version history	6
1.2 Objective	6
1.3 Addressees	7
1.4 Application	8
2 Introduction to information security	9
2.1 Overview of standards for information security	9
2.1.1 ISO standards on information security	10
2.1.2 Selected BSI publications and standards on information security	11
IT-Grundschutz	11
Series of BSI standards on information security: Topic IS management	12
Information security revision policy based on IT-Grundschutz	13
2.1.3 Additional standards	14
COBIT 5 A Business Framework for the Governance and Management of Enterprise IT	14
ITIL	14
PCI DSS	14
NIST	14
ISF – The Standard of Good Practice	14
3 ISMS definition and process description	16
3.1 Components of an information security management system	16
3.2 Process description and lifecycle model	18
3.2.1 The lifecycle in information security	18
3.2.2 Description of the information security process	18
4 Management principles	20
4.1 The tasks and duties of management	20
4.2 Communication and knowledge	22
4.3 Performance review within the security process	24
4.4 Continuous improvement of the security process	24
5 Resources for information security	25
6 Involving employees in the security process	26
7 The security process	27
7.1 Planning of the security process	27
7.2 Establishing a security organisation [DOC]	28
7.3 Implementation of the information security policy	29
7.4 Maintaining information security	29
7.5 Continuous improvement of information security	30
8 Security concept	31

8.1 Creating a security concept	31
8.2 Implementation of the security concept	34
8.3 Performance review of the security concept	35
8.4 Continuous improvement of the security concept	36
9 Certification of the ISMS	37
10 The ISMS based on BSI IT-Grundschutz	38
10.1 Introduction	38
10.2 The security process in accordance with IT-Grundschutz	38
10.2.1 Integrated risk assessment in IT-Grundschutz	39
10.2.2 Security concept	41
11 Appendix	44
11.1 References	44

CSA Cloud Controls Matrix (CCM)

CSA Cloud Controls Matrix (CCM)

Release Date: 07.06.2021, v.4

The CSA Cloud Controls Matrix (CCM) is a **cybersecurity control framework for cloud computing**.

It is composed of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology. It can be used as a tool for the systematic assessment of a cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain. The controls framework is aligned to the ***CSA Security Guidance for Cloud Computing***, and is considered a de-facto standard for cloud security assurance and compliance.

Organisation: Cloud Security Alliance (CSA)

Price: Free

	A	B	C	D	E	F	G	H	I	J	K	L
1	CCM	CLOUD CONTROLS MATRIX v4.0.10										
2	Introduction											
3	This section explains the CCM V4 spreadsheet structure and describes its components.											
4												
5	I. Structure											
6	The CCM V4 spreadsheet includes five tabs:											
7	• Introduction.											
8	• CCM Controls.											
9	• CCM Implementation Guidelines.											
10	• CCM Auditing Guidelines.											
11	• CCM Scope Applicability (Mappings).											
12	• Consensus Assessments Initiative Questionnaire (CAIQ).											
13	• Acknowledgments.											
14												
15	II. Components Description											
16												
17	a. CCM Controls											
18	This is the core of the CCM V4. It includes 197 controls structured in 17 domains.											
19	Each control is described by a:											
20	• Control Domain: the name of the domain to which the control pertains.											
21	• Control Title: the title of the control.											
24	Introduction CCM Implementation Guidelines Auditing Guidelines Scope Applicability (Mappings) CAIQ Acknowledgments Change Log +											



TABLE OF CONTENTS

DOMAIN 1 Cloud Computing Concepts and Architectures	DOMAIN 2 Governance and Enterprise Risk Management	DOMAIN 3 Legal Issues, Contracts and Electronic Discovery	DOMAIN 4 Compliance and Audit Management
DOMAIN 5 Information Governance	DOMAIN 6 Management Plans and Business Continuity	DOMAIN 7 Infrastructure Security	DOMAIN 8 Virtualization and Containers
DOMAIN 9 Incident Response	DOMAIN 10 Application Security	DOMAIN 11 Data Security and Encryption	DOMAIN 12 Identity, Enrollment, and Access Management
DOMAIN 13 Security as a Service	DOMAIN 14 Related Technologies		

Security Guidance v4.0 © Copyright 2021, Cloud Security Alliance. All rights reserved. 6

"State of the art"
in IT security

IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "State of the art", Technical and organisational measures (TOMs), 2023

When the German IT Security Act came into effect in July 2015, the IT Security Association Germany (TeleTrust) launched the Task Force "State of the art" to provide interested parties with recommended actions and guidelines on the "state of the art" required for **technical and organisational measures**.

These guidelines are considered a starting point for determining statutory IT security measures that correspond to the state of the art. They are not a replacement for technical, organisational or legal advice or assessment in individual cases.

Organisation: TeleTrust + ENISA

Price: Free

IT Security Act (Germany) and EU General Data Protection Regulation:

Guideline "State of the art"

Technical and organisational measures

2023

English version

In co-operation with



Contents

Principles of the guideline	6
1 Introduction	7
1.1 IT Security Act.....	7
1.2 German BSI security standards for CI operators in specific sectors.....	8
1.3 European implications.....	8
1.4 General Data Protection Regulation.....	9
1.5 Appropriateness of measures.....	10
2 Determining the state of technology	11
2.1 Definition.....	11
2.2 Method for determining the state of technology.....	12
2.3 Quality assurance process for the guide.....	14
2.4 Required protection objectives.....	14
3 Technical and organisational measures (TOMs)	16
3.1 General information.....	16
3.2 Technical measures.....	19
3.2.1 Authentication methods and procedures.....	19
3.2.2 Evaluation and enforcement of strong passwords.....	20
3.2.3 Multi-factor authentication.....	21
3.2.4 Cryptographic procedures.....	24
3.2.5 Disk encryption.....	25
3.2.6 Encryption of files and folders.....	27
3.2.7 E-mail encryption.....	28
3.2.8 Securing electronic data communication with PKI.....	29
3.2.9 Use of VPNs (layer 3).....	32
3.2.10 Layer 2 encryption.....	34
3.2.11 Cloud-based data exchange.....	36
3.2.12 Data storage in the cloud.....	37
3.2.13 Use of mobile voice and data services.....	39
3.2.14 Communication through instant messenger.....	40
3.2.15 Mobile Device Management.....	41
3.2.16 Router security.....	42
3.2.17 Network monitoring using Intrusion Detection System.....	44
3.2.18 Web traffic protection.....	46
3.2.19 Web application protection.....	47
3.2.20 Remote network access/ remote maintenance.....	49
3.2.21 Server hardening.....	50
3.2.22 Endpoint Detection & Response Platform.....	53
3.2.23 Using internet with web isolation.....	54
3.2.24 Attack detection and analysis (SIEM).....	56
3.2.25 Confidential computing.....	58
3.2.26 Sandboxing for malicious code analysis.....	59
3.2.27 Cyber threat intelligence.....	61
3.2.28 Securing administrative IT systems.....	62
3.2.29 Monitoring of Directory Services and Identity-Based Segmentation.....	64
3.2.30 Network segmentation and segregation.....	66
3.3 Organisational measures.....	69
3.3.1 Standards and norms.....	69
3.3.2 Processes.....	72
3.3.3 Secure software development.....	80
3.3.4 Process certification.....	84
3.3.5 Vulnerability and patch management.....	86
3.3.6 Management of information security risks.....	88
3.3.7 Personal certification.....	91
3.3.8 Dealing with providers.....	94
3.3.9 Information Security Management Systems (ISMS).....	96
3.3.10 Securing privileged accounts.....	98

3.3.11 Dark Web Monitoring.....	102
3.3.12 Software Bill of Materials (SBOM).....	103
4 Appendix	105
4.1 Excursion: Measures against ransomware attacks.....	105

List of figures

Figure 1: Three-step theory according to the Kalkar decision.....	11
Figure 2: Evaluation criteria.....	13
Figure 3: Example of state of technology classification.....	13
Figure 4: Process outline for evaluating technical measures in chapter 3.2.....	14
Figure 5: Structure levels of standards relevant to information security.....	70
Figure 6: PDCA model.....	75
Figure 7: Risk process according to ISO 31000.....	89

List of tables

Table 1: Overview of ISO/IEC 27000 series.....	70
Table 2: Differentiation of ISO 27001 vs. BSI's IT basic protection.....	71

C2M2

Cybersecurity Capability Maturity Model (C2M2)

V.2.1, June 2022

The Cybersecurity Capability Maturity Model (C2M2) is a free tool **to help organizations evaluate their cybersecurity capabilities and optimize security investments**. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments.

While the U.S. energy industry led development of the C2M2 and championed its adoption, any organization—regardless of size, type, or industry—can use the model to evaluate, prioritize, and improve their cybersecurity capabilities.

Organisation: Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Price: Free

Cybersecurity Capability Maturity Model (C2M2)

Version 2.1
June 2022

TABLE OF CONTENTS

Acknowledgments.....	iv
Cautionary Note	viii
Intended Scope and Use of This Publication.....	viii
Note to Readers on the Update	ix
1. Introduction.....	11
1.1 Intended Audience.....	11
1.2 Document Organization.....	12
2. Background.....	13
2.1 Model Development Approach.....	13
3. Core Concepts	15
3.1 Maturity Models.....	15
3.2 Enterprise, Organization, and Function.....	15
3.2.1 Function	16
3.3 Assets	17
3.3.1 IT Assets, OT Assets, and Information Assets.....	17
3.3.2 Additional Asset Subgroupings.....	18
4. Model Architecture	21
4.1 Domains, Objectives, and Practices	21
4.2 Maturity Indicator Levels	24
4.2.1 Summary of MIL Characteristics	24
4.3 Approach Progression.....	25
4.4 Management Progression	26
4.5 Enterprise-Focused Domains	27
4.5.1 Cybersecurity Program Management.....	28
4.5.2 Risk Management	28
4.5.3 Cybersecurity Architecture	28
4.6 Considerations for the Cybersecurity Architecture Domain	29
4.6.1 Cybersecurity Architecture Defined.....	29
4.6.2 Cybersecurity Architecture Framework	29
4.6.3 Implementing the Cybersecurity Architecture	29
4.6.4 Considering the Cybersecurity Architecture in C2M2	30
4.7 Example Lists Included in Practices	30
4.8 Practice Reference Notation.....	31
5. Using the Model.....	32
5.1 Step 1: Perform a Self-Evaluation.....	32

TABLE OF CONTENTS

5.2 Step 2: Analyze Identified Gaps	33
5.3 Step 3: Prioritize and Plan	34
5.4 Step 4: Implement Plans and Periodically Reevaluate	34
6. Model Domains	36
6.1 Asset, Change, and Configuration Management (ASSET).....	36
6.2 Threat and Vulnerability Management (THREAT)	39
6.3 Risk Management (RISK)	42
6.4 Identity and Access Management (ACCESS).....	46
6.5 Situational Awareness (SITUATION).....	49
6.6 Event and Incident Response, Continuity of Operations (RESPONSE).....	52
6.7 Third-Party Risk Management (THIRD-PARTIES).....	56
6.8 Workforce Management (WORKFORCE)	59
6.9 Cybersecurity Architecture (ARCHITECTURE)	63
6.10 Cybersecurity Program Management (PROGRAM)	68
APPENDIX A: References	71
APPENDIX B: Glossary.....	79
APPENDIX C: Acronyms.....	93
NOTICE.....	95

LIST OF FIGURES

Figure 1: Example of the Structure of a Notional Entity	16
Figure 2: Groups of Assets	20
Figure 3: Model and Domain Elements.....	22
Figure 4: Example List Included in Practice ASSET-1e.....	30
Figure 5: Example of Referencing an Individual Practice: ASSET-1a.....	31
Figure 6: Potential Approach for Using the Model.....	32

CyberFundamentals Framework

01.03.2023

The CyberFundamentals Framework is a **set of concrete measures** to:

- protect data,
- significantly reduce the risk of the most common cyber-attacks,
- increase an organisation's cyber resilience.

The framework is based on and linked with 4 commonly used cybersecurity frameworks: NIST CSF, ISO 27001 / ISO 27002, CIS Controls and IEC 62443.

To respond to the severity of the threat an organization is exposed to, in addition to the starting level Small, 3 assurance levels are provided: Basic, Important and Essential.

Organisation: Cybersecurity Centre Belgium (CCB)

Price: Free

CyberFundamentals
Framework



CYBER FUNDAMENTALS

ESSENTIAL

Version 2023-03-01

Centre for Cyber security Belgium
18 Rue de la Loi
1000 Brussels
Belgium

info@ccb.belgium.be
www.ccb.belgium.be



UNDER THE AUTHORITY
OF THE PRIME MINISTER

Table of Contents

Introduction	6
PROTECT	
ID.AM-1: Physical devices and systems used within the organization are inventoried	8
ID.AM-2: Software platforms and applications used within the organization are inventoried	9
ID.AM-3: Organizational communication and data flows are mapped	10
ID.AM-4: External information systems are catalogued	11
ID.AM-5: Resources are prioritized based on their classification, criticality, and business value	12
ID.AM-6: Cybersecurity roles, responsibilities, and authorities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	13
ID.BE-1: The organization's role in the supply chain is identified and communicated	14
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	14
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	15
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	15
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	16
ID.GV-1: Organizational cybersecurity policy is established and communicated	17
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood, and managed	18
ID.GV-4: Governance and risk management processes address cybersecurity risks	18
ID.RA-1: Asset vulnerabilities are identified and documented	19
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	20
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	20
ID.RA-6: Risk responses are identified and prioritized	21
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	22
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	22
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	22
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	23
ID.SC-2: Suppliers and third parties are identified, established, assessed, managed, and agreed to by organizational stakeholders	23
ID.SC-3: Contracts with suppliers and third parties are designed to meet the organization's risk management objectives	23
ID.SC-4: Suppliers and third parties are evaluated to ensure they meet the organization's risk management objectives	23
ID.SC-5: Response and recovery plans are established, managed, and agreed to by organizational stakeholders	23
RECOVER	
PR.AC-1: Identities and credentials are managed, and processes are established to ensure their integrity	23

© 2023 - Centre for Cybersecurity

PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	53
PR.PT-4: Communications and control networks are protected	53
DETECT	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	55
DE.AE-2: Detected events are analysed to understand attack targets and methods	55
DE.AE-3: Event data are collected and correlated from multiple sources and sensors	56
DE.AE-4: Impact of events is determined	56
DE.AE-5: Incident alert thresholds are established	57
DE.CM-1: The network is monitored to detect potential cybersecurity events	58
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	59
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	59
DE.CM-4: Malicious code is detected	60
DE.CM-5: Unauthorized mobile code is detected	60
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	61
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	61
DE.CM-8: Vulnerability scans are performed	62
DE.DP-2: Detection activities comply with all applicable requirements	63
DE.DP-3: Detection processes are tested	63
DE.DP-4: Event detection information is communicated	63
DE.DP-5: Detection processes are continuously improved	64
RESPOND	
RS.RP-1: Response plan is executed during or after an incident	65
RS.CO-1: Personnel know their roles and order of operations when a response is needed	66
RS.CO-2: Incidents are reported consistent with established criteria	66
RS.CO-3: Information is shared consistent with response plans	67
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	67
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	67
RS.AN-1: Notifications from detection systems are investigated	68
RS.AN-2: The impact of the incident is understood	68
RS.AN-3: Forensics are performed	69
RS.AN-4: Incidents are categorized and prioritized	69
RS.AN-5: Processes are established to ensure organizational resilience	69
RS.MI-1: Incidents are escalated	70
RS.MI-2: Incidents are mitigated	70
RS.MI-3: Newly identified vulnerabilities are reported	70
RS.MI-4: Response plans are updated	70
RS.MI-5: Response and recovery plans are updated	70
RS.MI-6: Response and recovery plans are updated	70
RS.MI-7: Response and recovery plans are updated	70
RS.MI-8: Response and recovery plans are updated	70
RS.MI-9: Response and recovery plans are updated	70
RS.MI-10: Response and recovery plans are updated	70
RS.MI-11: Response and recovery plans are updated	70
RS.MI-12: Response and recovery plans are updated	70
RS.MI-13: Response and recovery plans are updated	70
RS.MI-14: Response and recovery plans are updated	70
RS.MI-15: Response and recovery plans are updated	70
RS.MI-16: Response and recovery plans are updated	70
RS.MI-17: Response and recovery plans are updated	70
RS.MI-18: Response and recovery plans are updated	70
RS.MI-19: Response and recovery plans are updated	70
RS.MI-20: Response and recovery plans are updated	70
RS.MI-21: Response and recovery plans are updated	70
RS.MI-22: Response and recovery plans are updated	70
RS.MI-23: Response and recovery plans are updated	70
RS.MI-24: Response and recovery plans are updated	70
RS.MI-25: Response and recovery plans are updated	70
RS.MI-26: Response and recovery plans are updated	70
RS.MI-27: Response and recovery plans are updated	70
RS.MI-28: Response and recovery plans are updated	70
RS.MI-29: Response and recovery plans are updated	70
RS.MI-30: Response and recovery plans are updated	70
RS.MI-31: Response and recovery plans are updated	70
RS.MI-32: Response and recovery plans are updated	70
RS.MI-33: Response and recovery plans are updated	70
RS.MI-34: Response and recovery plans are updated	70
RS.MI-35: Response and recovery plans are updated	70
RS.MI-36: Response and recovery plans are updated	70
RS.MI-37: Response and recovery plans are updated	70
RS.MI-38: Response and recovery plans are updated	70
RS.MI-39: Response and recovery plans are updated	70
RS.MI-40: Response and recovery plans are updated	70
RS.MI-41: Response and recovery plans are updated	70
RS.MI-42: Response and recovery plans are updated	70
RS.MI-43: Response and recovery plans are updated	70
RS.MI-44: Response and recovery plans are updated	70
RS.MI-45: Response and recovery plans are updated	70
RS.MI-46: Response and recovery plans are updated	70
RS.MI-47: Response and recovery plans are updated	70
RS.MI-48: Response and recovery plans are updated	70
RS.MI-49: Response and recovery plans are updated	70
RS.MI-50: Response and recovery plans are updated	70
RS.MI-51: Response and recovery plans are updated	70
RS.MI-52: Response and recovery plans are updated	70
RS.MI-53: Response and recovery plans are updated	70
RS.MI-54: Response and recovery plans are updated	70
RS.MI-55: Response and recovery plans are updated	70
RS.MI-56: Response and recovery plans are updated	70
RS.MI-57: Response and recovery plans are updated	70
RS.MI-58: Response and recovery plans are updated	70
RS.MI-59: Response and recovery plans are updated	70
RS.MI-60: Response and recovery plans are updated	70
RS.MI-61: Response and recovery plans are updated	70
RS.MI-62: Response and recovery plans are updated	70
RS.MI-63: Response and recovery plans are updated	70
RS.MI-64: Response and recovery plans are updated	70
RS.MI-65: Response and recovery plans are updated	70
RS.MI-66: Response and recovery plans are updated	70
RS.MI-67: Response and recovery plans are updated	70
RS.MI-68: Response and recovery plans are updated	70
RS.MI-69: Response and recovery plans are updated	70
RS.MI-70: Response and recovery plans are updated	70
RS.MI-71: Response and recovery plans are updated	70
RS.MI-72: Response and recovery plans are updated	70
RS.MI-73: Response and recovery plans are updated	70
RS.MI-74: Response and recovery plans are updated	70
RS.MI-75: Response and recovery plans are updated	70
RS.MI-76: Response and recovery plans are updated	70
RS.MI-77: Response and recovery plans are updated	70
RS.MI-78: Response and recovery plans are updated	70
RS.MI-79: Response and recovery plans are updated	70
RS.MI-80: Response and recovery plans are updated	70
RS.MI-81: Response and recovery plans are updated	70
RS.MI-82: Response and recovery plans are updated	70
RS.MI-83: Response and recovery plans are updated	70
RS.MI-84: Response and recovery plans are updated	70
RS.MI-85: Response and recovery plans are updated	70
RS.MI-86: Response and recovery plans are updated	70
RS.MI-87: Response and recovery plans are updated	70
RS.MI-88: Response and recovery plans are updated	70
RS.MI-89: Response and recovery plans are updated	70
RS.MI-90: Response and recovery plans are updated	70
RS.MI-91: Response and recovery plans are updated	70
RS.MI-92: Response and recovery plans are updated	70
RS.MI-93: Response and recovery plans are updated	70
RS.MI-94: Response and recovery plans are updated	70
RS.MI-95: Response and recovery plans are updated	70
RS.MI-96: Response and recovery plans are updated	70
RS.MI-97: Response and recovery plans are updated	70
RS.MI-98: Response and recovery plans are updated	70
RS.MI-99: Response and recovery plans are updated	70
RS.MI-100: Response and recovery plans are updated	70

© 2023 - Centre for Cybersecurity

ETSI Critical Security Controls

Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

v.4.1.2, April 2022

The present document captures and describes **the prioritized set of actions** that collectively form a defence-in-depth set of best practices that **mitigate the most common attacks against systems and networks**. These actions are specified by ETSI in the present document, the Critical Security Controls (CSCs), which are developed and maintained by the Center for Internet Security (CIS) as an independent, expert, global non-profit organization.

Organisation: ETSI

Price: Free



**Cyber Security (CYBER);
Critical Security Controls for Effective Cyber Defence;
Part 1: The Critical Security Controls**

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	5
Introduction	5
1 Scope.....	8
2 References	8
2.1 Normative references	8
2.2 Informative references.....	8
3 Definition of terms, symbols and abbreviations.....	9
3.1 Terms.....	9
3.2 Symbols.....	12
3.3 Abbreviations	12
4 Critical Security Controls.....	13
4.0 Structure of the Critical Security Controls	13
4.1 Control 1: Inventory and Control of Enterprise Assets	14
4.2 Control 2: Inventory and Control of Software Assets	16
4.3 Control 3: Data Protection.....	18
4.4 Control 4: Secure Configuration of Enterprise Assets and Software	20
4.5 Control 5: Account Management	22
4.6 Control 6: Access Control Management	24
4.7 Control 7: Continuous Vulnerability Management	25
4.8 Control 8: Audit Log Management	27
4.9 Control 9: Email and Web Browser Protections.....	29
4.10 Control 10: Malware Defences.....	31
4.11 Control 11: Data Recovery.....	32
4.12 Control 12: Network Infrastructure Management	33
4.13 Control 13: Network Monitoring and Defence.....	34
4.14 Control 14: Security Awareness and Skills Training	36
4.15 Control 15: Service Provider Management	38
4.16 Control 16: Application Software Security	40
4.17 Control 17: Incidence Response Management	44
4.18 Control 18: Penetration Testing.....	47
Annex A: Version changes to the Controls	49
Annex B: Graphical depiction of the Controls.....	50
History	59

HITRUST CSF

HITRUST Common Security Framework (CSF)

v.11.2.0, October 10, 2023

The HITRUST CSF provides the structure, transparency, guidance, and cross-references to authoritative sources that organizations globally need to be certain of their **data protection compliance**. The initial development of the HITRUST CSF leveraged nationally and internationally accepted security and privacy-related regulations, standards, and frameworks – including ISO, NIST, PCI, HIPAA, and GDPR – to ensure a comprehensive set of security and privacy controls. HITRUST continually incorporates additional authoritative sources as they are released and accepted in industry and global sectors. The HITRUST CSF standardizes these requirements across authoritative sources to provide clarity and consistency and reduce the burden of compliance.

The commitment and expertise demonstrated by HITRUST ensures that organizations leveraging the framework are prepared when new security and privacy regulations and risks are introduced.

Organisation: HITRUST

Price: Free



HITRUST CSF PDF v11.2.0

THE HITRUST CSF INCLUDED IN THE DOWNLOAD PACKAGE IS NOT A COMPREHENSIVE LISTING OF ALL REQUIREMENTS WITHIN THE HITRUST CSF. THE FULL AND COMPREHENSIVE HITRUST CSF IS AVAILABLE ONLY UPON REQUEST TO ELIGIBLE QUALIFIED ORGANIZATIONS OR QUALIFIED INDIVIDUALS AS SET FORTH IN THE LICENSE AGREEMENT.

Qualified Organizations or Qualified Individuals may request access to the full and comprehensive HITRUST CSF PDF by submitting a request to info@hitrustalliance.net.

HITRUST will review requests to confirm the Qualified Organization or Qualified Individual eligibility. HITRUST reserves the right to reject any request, for the full and comprehensive HITRUST CSF, at HITRUST's sole discretion.

© 2023 HITRUST. All rights reserved. Any commercial uses or creations of derivative works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronic or mechanical, without HITRUST's prior written permission.

Table of Contents

Control Category: 0.0 - Information Security Management Program.....	6
Objective Name: 0.01 Information Security Management Program.....	6
Control Reference: 0.0.a Information Security Management Program.....	6
Control Category: 0.1 - Access Control.....	12
Objective Name: 0.1 Business Requirement for Access Control.....	12
Control Reference: 0.1.a Access Control Policy.....	13
Objective Name: 0.1.02 Authorized Access to Information Systems.....	17
Control Reference: 0.1.a User Registration.....	17
Control Reference: 0.1.c Privilege Management.....	22
Control Reference: 0.1.d User Password Management.....	30
Control Reference: 0.1.e Review of User Access Rights.....	36
Objective Name: 0.1.03 User Responsibilities.....	39
Control Reference: 0.1.f Password Use.....	39
Control Reference: 0.1.g Unattended User Equipment.....	40
Control Reference: 0.1.h Clear Desk and Clear Screen Policy.....	42
Objective Name: 0.1.04 Network Access Control.....	43
Control Reference: 0.1.j User Authentication for External Connections.....	43
Control Reference: 0.1.k Equipment Identification in Networks.....	48
Control Reference: 0.1.l Remote Diagnostic and Configuration Port Protection.....	49
Control Reference: 0.1.m Segregation in Networks.....	52
Control Reference: 0.1.n Network Connection Control.....	56
Control Reference: 0.1.o Network Routing Control.....	61
Objective Name: 0.1.05 Operating System Access Control.....	65
Control Reference: 0.1.p Secure Log Procedures.....	65
Control Reference: 0.1.q User Identification and Authentication.....	68
Control Reference: 0.1.r Password Management System.....	76
Control Reference: 0.1.s Use of System Utilities.....	77
Control Reference: 0.1.t Session Time-out.....	78
Control Reference: 0.1.u Limitation of Connection Time.....	81
Objective Name: 0.1.06 Application and Information Access Control.....	81
Control Reference: 0.1.v Information Access Restriction.....	82
Control Reference: 0.1.w Sensitive System Isolation.....	84
Objective Name: 0.1.07 Mobile Computing and Teleworking.....	87
Control Reference: 0.1.x Mobile Computing and Communications.....	87
Control Reference: 0.1.y Teleworking.....	91
Control Category: 0.2 - Human Resources Security.....	95
Objective Name: 0.2.01 Prior to Employment.....	95
Control Reference: 0.2.a Roles and Responsibilities.....	95
Control Reference: 0.2.b Screening.....	97
Objective Name: 0.2.02 During On-Boarding.....	102
Control Reference: 0.2.c Terms and Conditions of Employment.....	102
Objective Name: 0.2.03 During Employment.....	105
Control Reference: 0.2.d Management Responsibilities.....	105
Control Reference: 0.2.e Information Security.....	105
Control Reference: 0.2.f Disciplinary Action.....	105
Objective Name: 0.2.04 Termination.....	105
Control Reference: 0.2.g Termination.....	105
Control Reference: 0.2.h Return of Assets.....	105
Control Reference: 0.2.i Removal of Access.....	105
Control Category: 0.3 - Risk Management.....	105
Objective Name: 0.3.01 Risk Management.....	105
Control Reference: 0.3.a Risk Management.....	105
Control Reference: 0.3.b Performing Risk Assessments.....	105
Control Reference: 0.3.c Risk Mitigation.....	105
Control Reference: 0.3.d Risk Evaluation.....	105
Control Reference: 0.3.e Removal of Assets.....	105
Control Category: 0.4 - Security Policy.....	105
Objective Name: 0.4.01 Information Security Policy.....	105
Control Reference: 0.4.a Information Security Policy Document.....	105
Control Reference: 0.4.b Review of the Information Security Policy.....	105
Control Category: 0.5 - Organization of Information Security.....	105
Objective Name: 0.5.01 Internal Organization.....	105
Control Reference: 0.5.a Management Commitment to Information Security.....	105
Control Reference: 0.5.b Information Security Coordination.....	105
Control Reference: 0.5.c Allocation of Information Security Responsibilities.....	105
Control Reference: 0.5.d Authorization Process for Information Assets and Facilities.....	105
Control Reference: 0.5.e Confidentiality Agreements.....	105
Control Reference: 0.5.f Contact with Authorities.....	105
Control Reference: 0.5.g Contact with Special Interest Groups.....	105
Control Reference: 0.5.h Independent Review of Information Security.....	105
Objective Name: 0.5.02 External Parties.....	105
Control Reference: 0.5.i Identification of Risks Related to External Parties.....	105
Control Reference: 0.5.j Addressing Security When Dealing with Customers.....	105
Control Reference: 0.5.k Addressing Security in Third Party Agreements.....	105
Control Category: 0.6 - Compliance.....	105
Objective Name: 0.6.01 Compliance with Legal Requirements.....	105
Control Reference: 0.6.a Identification of Applicable Legislation.....	105
Control Reference: 0.6.b Intellectual Property Rights.....	105
Control Reference: 0.6.c Protection of Organizational Records.....	105
Control Reference: 0.6.d Data Protection and Privacy of Covered Information.....	105
Control Reference: 0.6.e Prevention of Misuse of Information Assets.....	105
Control Reference: 0.6.f Regulation of Cryptographic Controls.....	105
Objective Name: 0.6.02 Compliance with Security Policies and Standards, and Technical Compliance.....	105
Control Reference: 0.6.g Compliance with Security Policies and Standards.....	105
Control Reference: 0.6.h Technical Compliance Checking.....	105
Objective Name: 0.6.03 Information System Audit Considerations.....	105
Control Reference: 0.6.i Information Systems Audit Controls.....	105
Control Reference: 0.6.j Protection of Information Systems Audit Tools.....	105
Control Category: 0.7 - Asset Management.....	105
Objective Name: 0.7.01 Responsibility for Assets.....	105
Control Reference: 0.7.a Inventory of Assets.....	105
Control Reference: 0.7.b Ownership of Assets.....	105
Control Reference: 0.7.c Acceptable Use of Assets.....	105
Objective Name: 0.7.02 Information Classification.....	105
Control Reference: 0.7.d Classification Guidelines.....	105
Control Reference: 0.7.e Information Labeling and Handling.....	105
Control Category: 0.8 - Physical and Environmental Security.....	105
Objective Name: 0.8.01 Secure Areas.....	105
Control Reference: 0.8.a Physical Security Perimeter.....	105
Control Reference: 0.8.b Physical Entry Controls.....	105
Control Reference: 0.8.c Securing Offices, Rooms, and Facilities.....	105
Control Reference: 0.8.d Protecting Against External and Environmental Threats.....	105
Control Reference: 0.8.e Working in Secure Areas.....	105
Control Reference: 0.8.f Public Access, Delivery, and Loading Areas.....	105
Objective Name: 0.8.02 Equipment Security.....	105
Control Reference: 0.8.g Equipment Siting and Protection.....	105
Control Reference: 0.8.h Supporting Utilities.....	105
Control Reference: 0.8.i Cabling Security.....	105
Control Reference: 0.8.j Equipment Maintenance.....	105

Control Reference: 0.8.k Security of Equipment Off-Premises.....	274
Control Reference: 0.8.l Secure Disposal or Re-Use of Equipment.....	275
Control Reference: 0.8.m Removal of Property.....	279
Control Category: 0.9 - Communications and Operations Management.....	280
Objective Name: 0.9.01 Documented Operating Procedures.....	280
Control Reference: 0.9.a Documented Operations Procedures.....	280
Control Reference: 0.9.b Change Management.....	282
Control Reference: 0.9.c Segregation of Duties.....	283
Control Reference: 0.9.d Separation of Development, Test, and Operational Environments.....	287
Objective Name: 0.9.02 Control Third Party Service Delivery.....	289
Control Reference: 0.9.e Service Delivery.....	289
Control Reference: 0.9.f Monitoring and Review of Third Party Services.....	292
Control Reference: 0.9.g Managing Changes to Third Party Services.....	294
Objective Name: 0.9.03 System Planning and Acceptance.....	295
Control Reference: 0.9.h Capacity Management.....	295
Control Reference: 0.9.i System Acceptance.....	296
Objective Name: 0.9.04 Protection Against Malicious and Mobile Code.....	301
Control Reference: 0.9.j Controls Against Malicious Code.....	301
Control Reference: 0.9.k Controls Against Mobile Code.....	308
Objective Name: 0.9.05 Information Back-Up.....	309
Control Reference: 0.9.l Back-up.....	310
Objective Name: 0.9.06 Network Security Management.....	314
Control Reference: 0.9.m Network Controls.....	314
Control Reference: 0.9.n Security of Network Services.....	324
Objective Name: 0.9.07 Media Handling.....	327
Control Reference: 0.9.o Management of Removable Media.....	327
Control Reference: 0.9.p Disposal of Media.....	332
Control Reference: 0.9.q Information Handling Procedures.....	335
Control Reference: 0.9.r Security of System Documentation.....	338
Objective Name: 0.9.08 Exchange of Information.....	340
Control Reference: 0.9.s Information Exchange Policies and Procedures.....	340
Control Reference: 0.9.t Exchange Agreements.....	346
Control Reference: 0.9.u Physical Media in Transit.....	348
Control Reference: 0.9.v Electronic Messaging.....	350
Control Reference: 0.9.w Interconnected Business Information Systems.....	352
Objective Name: 0.9.09 On-line Transactions.....	354
Control Reference: 0.9.x Electronic Commerce Services.....	355
Control Reference: 0.9.y On-line Transactions.....	356
Control Reference: 0.9.z Publicly Available Information.....	358
Objective Name: 0.9.10 Monitoring.....	361
Control Reference: 0.9.aa Monitoring System Use.....	362
Control Reference: 0.9.ab Monitoring System Use.....	369
Control Reference: 0.9.ac Protection of Log Information.....	377
Control Reference: 0.9.ad Administration Operator Logs.....	380
Control Reference: 0.9.ae Fault Logging.....	381
Control Reference: 0.9.af Clock Synchronization.....	382
Control Category: 10.0 - Information Security Requirements.....	406
Objective Name: 10.01 Security Requirements.....	406
Control Reference: 10.0.a Security Requirements.....	406
Control Reference: 10.0.b Correct Procurement.....	406
Control Reference: 10.0.c Input Data Validation.....	406
Control Reference: 10.0.d Control of Information.....	406
Control Reference: 10.0.e Message Integrity.....	412
Control Reference: 10.0.f Output Data Protection.....	414
Objective Name: 10.05 Security in Development and Support Processes.....	415
Control Reference: 10.0.g Change Control Procedures.....	415
Control Reference: 10.0.h Outsourced Software Development.....	424
Objective Name: 10.06 Technical Vulnerability Management.....	426
Control Reference: 10.0.m Control of Technical Vulnerabilities.....	426
Control Category: 11.0 - Information Security Incident Management.....	434
Objective Name: 11.01 Reporting Information Security Incidents and Weaknesses.....	434
Control Reference: 11.a Reporting Information Security Events.....	434
Control Reference: 11.b Reporting Security Weaknesses.....	441
Objective Name: 11.02 Management of Information Security Incidents and Improvements.....	443
Control Reference: 11.c Responsibilities and Procedures.....	443
Control Reference: 11.d Learning from Information Security Incidents.....	452
Control Reference: 11.e Collection of Evidence.....	456
Control Category: 12.0 - Business Continuity Management.....	458
Objective Name: 12.01 Information Security Aspects of Business Continuity Management.....	458
Control Reference: 12.a Including Information Security in the Business Continuity Management Process.....	458
Control Reference: 12.b Business Continuity and Risk Assessment.....	460
Control Reference: 12.c Developing and Implementing Continuity Plans Including Information Security.....	462
Control Reference: 12.d Business Continuity Planning Framework.....	471
Control Reference: 12.e Testing, Maintaining and Re-Assessing Business Continuity Plans.....	473
Control Category: 13.0 - Privacy Practices.....	477
Objective Name: 13.01 Privacy Practices.....	477
Control Reference: 13.a Privacy Notices.....	477
Control Reference: 13.b Openness and Transparency.....	481
Control Reference: 13.c Accounting of Disclosures.....	483
Objective Name: 13.02 Individual Participation.....	484
Control Reference: 13.d Consent.....	485
Control Reference: 13.e Choice.....	487
Control Reference: 13.f Privacy Access.....	489
Objective Name: 13.03 Purpose Specification.....	492
Control Reference: 13.g Purpose Legitimacy.....	492
Control Reference: 13.h Purpose Specification.....	493
Objective Name: 13.04 Data Minimization.....	494
Control Reference: 13.i Collection Limitation.....	494
Control Reference: 13.j Data Minimization.....	496
Objective Name: 13.05 Use Limitation.....	498
Control Reference: 13.k Use and Disclosure.....	498
Control Reference: 13.l Retention and Disposal.....	504
Objective Name: 13.06 Data Quality and Integrity.....	505
Control Reference: 13.m Accuracy and Quality.....	505
Control Reference: 13.n Participation and Redress.....	506
Control Reference: 13.o Complaint Management.....	507
Objective Name: 13.07 Accountability & Auditing.....	509
Control Reference: 13.p Governance.....	509
Control Reference: 13.q Privacy and Impact Assessment.....	510
Control Reference: 13.r Privacy Requirements for Contractors and Processors.....	511
Control Reference: 13.s Privacy Monitoring and Auditing.....	513
Control Reference: 13.t Privacy Protection Awareness and Training.....	513
Control Reference: 13.u Privacy Protection Reporting.....	514

Open Information Security Management Maturity Model (O-ISM3), v.2.0, 2017

O-ISM3

O-ISM3 is The Open Group framework for managing information security, and wider still to managing information in the wider context. It aims to ensure that security processes in any organization are implemented so as to operate at a level consistent with that organization's business requirements. O-ISM3 is technology-neutral. It defines a **comprehensive but manageable number of information security processes** sufficient for the needs of most organizations, with the relevant security control(s) being identified within each process as an essential subset of that process. In this respect, it is fully compatible with the well-established ISO/IEC 27000:2009, COBIT® , and ITIL® standards in this field. Additionally, as well as complementing the TOGAF® framework for Enterprise Architecture, O-ISM3 defines operational metrics and their allowable variances.

Organisation: The Open Group

Price: Free

Open Group Standard

Open Information Security Management Maturity Model (O-ISM3), Version 2.0



Contents

1	Introduction	1
1.1	Objective	1
1.2	Overview	1
1.2.1	Context for this Standard	2
1.3	Conformance	2
1.4	Normative References	3
1.5	Terminology	3
1.6	Future Directions	3
2	Key Concepts	4
2.1	Capability Levels	5
2.2	Maturity Levels	5
2.2.1	Maturity Levels and ROI	6
2.3	Processes	6
2.3.1	Process Levels	6
2.3.2	Selecting your Set of Processes	9
2.3.3	Process Definition	9
2.3.4	Process Roles and Responsibilities	11
2.3.5	Process Metrics Definition	15
2.3.6	Process Metrics Specification	17
2.3.7	Process Metrics Operational Use	19
2.4	Processes and Document Codes	21
2.5	Components of Information Systems	21
2.5.1	Structural Features	21
2.5.2	Transactional Features	22
2.6	Lifecycles and IT Managed Domains	23
3	O-ISM3 in Business Context	26
3.1	Business Context	26
3.2	Security-in-Context Model	26
3.3	Operational Approach	27
3.4	Operational Definitions	27
3.5	O-ISM3 Definition – Security-in-Context	28
3.6	Business Objectives, Security Objectives, and Security Targets	28
3.6.1	Business Objectives	28
3.6.2	Security Objectives	29
3.6.3	Security Targets	30
3.6.4	Examples	31
3.7	O-ISM3 Interpretation of Incidents, Success, and Failure	36
4	O-ISM3 Process Model	38
4.1	Security Management – O-ISM3 Basics	38
4.2	Generic Processes	40
4.2.1	GP-1: Knowledge Management	40

4.2.2	GP-2: ISMS and Business Audit	42
4.2.3	Implementing O-ISM3	43
4.3	Specific Processes – Strategic Management	46
4.3.1	SSP-1: Report to Stakeholders	46
4.3.2	SSP-2: Coordination	47
4.3.3	SSP-4: Define Division of Duties Rules	48
4.3.4	SSP-6: Allocate Resources for Information Security	48
4.4	Specific Processes – Tactical Management	49
4.4.1	TSP-1: Report to Strategic Management	49
4.4.2	TSP-2: Manage Allocated Resources	50
4.4.3	TSP-3: Define Security Targets and Security Objectives	51
4.4.4	TSP-4: Service Level Management	52
4.4.5	TSP-6: Security Architecture	53
4.4.6	TSP-13: Insurance Management	54
4.4.7	Personnel Security	55
4.4.8	TSP-14: Information Operations	59
4.5	Specific Processes – Operational Management	60
4.5.1	OSP-1: Report to Tactical Management	60
4.5.2	OSP-2: Security Procurement	60
4.5.3	Lifecycle Control	61
4.5.4	Access and Environmental Control	70
4.5.5	Availability Control	74
4.5.6	Testing and Auditing	78
4.5.7	Monitoring	82
4.5.8	Incident Handling	85
5	Outsourcing	88
5.1	Introduction	88
5.2	Service-Level Agreements	88
5.3	Guidelines	89
6	Implementing O-ISM3	92
6.1	Top-Down or Bottom-Up	92
6.2	No One Solution Fits All	92
6.3	Selecting the Processes to Implement	92
6.4	Processes Fundamental to any O-ISM3 Implementation	93
6.5	Guidance on the Role of Key Groups of O-ISM3 Processes	93
6.6	Top-Down Implementation	94
6.7	Bottom-Up Implementation	96
6.8	Examples of O-ISM3 Maturity Levels	96
6.8.1	General	97
6.8.2	Strategic Management	97
6.8.3	Tactical Management	97
6.8.4	Operational Management	98
A	Index of Processes	100
B	Compatibility with other Standards and Frameworks	102
B.1	Compatibility with ISO 9000 Quality Management	102

B.2	Compatibility with ISO/IEC 27000	102
B.3	Compatibility with NIST Cybersecurity Framework	102
B.4	Compatibility with COBIT®	103
B.5	Compatibility with ITIL®	103
B.6	Compatibility with the TOGAF® Standard	103
C	Rationale (Informative)	104
C.1	Conformance	104

Secure Controls Framework (SCF)

Secure Controls Framework (SCF), 2023.2

The SCF focuses on internal controls. These are the cybersecurity & data privacy-related policies, standards, procedures, technologies and associated processes that are designed **to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented, detected and corrected.** The concept is to address the broader People, Processes, Technology and Data (PPTD) that are what controls fundamentally exists to govern. Using the SCF should be viewed as a long-term tool to not only help with compliance-related efforts but to ensure cybersecurity & data privacy principles are properly designed, implemented and maintained. The SCF helps implement a holistic approach to protecting the Confidentiality, Integrity, Availability and Safety (CIAS) of your data, systems, applications and other processes. The SCF can be used to assist with strategic planning down to tactical needs that impact the people, processes and technologies directly impacting your organization.

Organisation: SCF Council

Price: Free

Cybersecurity & Data Privacy by Design Principles (C|P)

The C|P establishes 33 common-sense principles to guide the development and oversight of a modern cybersecurity & data privacy program. The C|P is sourced from the Secure Controls Framework (SCF), which is a free resource for businesses. The SCF's comprehensive listing of over 1,000 cybersecurity & data privacy controls is categorized into 33 domains that are mapped to over 100 statutory, regulatory and contractual frameworks. Those applicable SCF controls can operationalize the C|P principles to help an organization ensure that secure practices are implemented by design and by default. Those 33 C|P principles are listed below:



1. Cybersecurity & Data Protection Governance (GOV)

Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses applicable statutory, regulatory and contractual obligations.



2. Artificial Intelligence and Autonomous Technology (AAT)

Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.



3. Asset Management (AST)

Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.



4. Business Continuity & Disaster Recovery (BCD)

Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.



5. Capacity & Performance Planning (CAP)

Govern the current and future capacities and performance of technology assets.



6. Change Management (CHG)

Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.



7. Cloud Security (CLD)

Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity & data privacy controls.



8. Compliance (CPL)

Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.



9. Configuration Management (CFG)

Enforce secure configurations according to vendor-recommended and industry-recognized secure practices that enforce the concepts of "least privilege" and "least functionality" for all systems, applications and services.



10. Continuous Monitoring (MON)

Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.



11. Cryptographic Protections (CRY)

Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.



12. Data Classification & Handling (DCH)

Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.



13. Embedded Technology (EMB)

Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.



14. Endpoint Security (END)

Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.



15. Human Resources Security (HRS)

Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.



16. Identification & Authentication (IAC)

Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.



17. Incident Response (IRO)

Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).



18. Information Assurance (IAO)

Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.



19. Maintenance (MNT)

Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.



20. Mobile Device Management (MDM)

Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.



21. Network Security (NET)

Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.



22. Physical & Environmental Security (PES)

Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.



23. Data Privacy (PRI)

Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.



24. Project & Resource Management (PRM)

Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.

C|P 2023.4



25. Risk Management (RSK)

Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.



26. Secure Engineering & Architecture (SEA)

Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.



27. Security Operations (OPS)

Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.



28. Security Awareness & Training (SAT)

Foster a cybersecurity & data privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.



29. Technology Development & Acquisition (TDA)

Develop and/or acquire systems, applications and services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design flaws.



30. Third-Party Management (TPM)

Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.



31. Threat Management (THR)

Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.



32. Vulnerability & Patch Management (VPM)

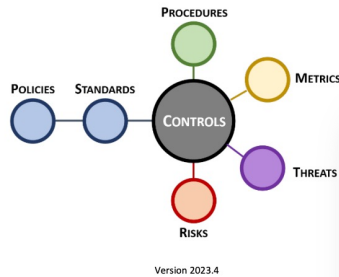
Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.



33. Web Security (WEB)

Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.

Integrated Controls Management (ICM) Overview



Version 2023.4

Disclaimer: This document is provided for educational purposes only. This document does not constitute a substitute for professional services. If you have compliance questions, you are encouraged to consult with a competent cybersecurity professional.

Copyright © 2023 by Compliance Forge, LLC (ComplianceForge). All rights reserved.

Table of Contents

- Executive Summary 3
- Integrated Controls Management (ICM) 4
- Defining What It Means To Be "Secure & Compliant"..... 4
 - IT General Controls (ITGC)..... 4
- ICM Principles..... 5
 - Principle 1: Establish Context..... 5
 - Principle 2: Define Applicable Controls..... 5
 - Principle 3: Assign Maturity-Based Criteria..... 5
 - Principle 4: Publish Policies & Standards..... 6
 - Principle 5: Assign Stakeholder Accountability..... 6
 - Principle 6: Maintain Situational Awareness..... 6
 - Principle 7: Manage Risk..... 6
 - Principle 8: Evolve Processes..... 6
- Practical Risk Management Considerations 7
- Understanding The Differences Between: Risks vs Threats 7
 - Risk Management Options..... 7
 - What Is A Risk?..... 8
 - What Is A Threat?..... 8
- Understanding The Differences Between: Risk Tolerance vs Risk Threshold vs Risk Appetite..... 9
 - What Is A Risk Appetite?..... 9
 - What Is A Risk Tolerance?..... 9
 - What Is A Risk Threshold?..... 12
- Defining A Risk Determination 12
 - Conforms..... 13
 - Significant Deficiency..... 13
 - Material Weakness..... 14
- Materiality: Criteria To Establish Risk Thresholds 14
 - Historical Context For Cybersecurity & Data Privacy Materiality Usage..... 14
- Applying ICM To Governance, Risk Management & Compliance (GRC) Functions 16
 - GRC Is A Plan, Do, Check & Act (PDCA) Adventure – That Is A Concept that Should Be Embraced, Not Fought Against..... 16
 - Chicken vs Egg Debate: The Logical Order of GRC Functions..... 17
 - Compliance..... 17
 - Governance..... 17
 - Risk Management..... 18
 - GRC Integrations..... 19
- Practical Solutions To Implement ICM 20
 - Cybersecurity & Data Protection Controls..... 20
 - Maturity-Based Control Criteria..... 20
 - Documented Policies, Standards & Procedures..... 21
 - Assign Stakeholder Accountability..... 21
 - Maintain Situational Awareness..... 21
 - Manage Risk..... 21
 - Evolve Processes..... 22

CYBERSECURITY & DATA PRIVACY CAPABILITY MATURITY MODEL (C|P-CMM) OVERVIEW

version 2023.4

con·trol
/kən trol/

A control is the power to influence or direct behaviors and the practices within organizations so that both cybersecurity and privacy are implemented and managed in an efficient and sustainable manner.

NOTE: This guide is for educational purposes only. You are highly encouraged to work with a cybersecurity and/or data privacy professional to validate any compliance-related assumptions. For more information, please visit www.SecureControlsFramework.com.

Table of Contents

- Executive Summary 3
- Objectives of the C|P-CMM 3
- Not Just Another CMM 3
- Nested Approach To Maturity 3
- Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) Overview 4
- Maintaining The Integrity of Maturity-Based Criteria 4
- Divining A Maturity Level Decision From Control-Level Maturity Criteria 4
- Maturity (Governance) + Assurance (Security) 5
- Defining C|P-CMM Levels 5
 - C|P-CMM Level 0 (L0) - Not Performed..... 5
 - C|P-CMM Level 1 (L1) - Performed Informally..... 5
 - C|P-CMM Level 2 (L2) - Planned & Tracked..... 6
 - C|P-CMM Level 3 (L3) - Well Defined..... 6
 - C|P-CMM Level 4 (L4) - Quantitatively Controlled..... 7
 - C|P-CMM Level 5 (L5) - Continuously Improving..... 7
- Defining A Capability Maturity "Sweet Spot" 9
 - Negligence Considerations 9
 - Risk Considerations 9
 - Process Review Lag Considerations 9
 - Stakeholder Value Considerations 9
 - Analog Example – Sit / Crawl / Walk / Run / Sprint / Hurdle 10
- Expected C|P-CMM Use Cases 11
 - Use Case #1 – Objective Criteria To Build A Cybersecurity & Privacy Program 11
 - Identifying The Problem..... 11
 - Considerations..... 11
 - Identifying A Solution..... 12
 - Use Case #2 – Assist Project Teams To Appropriately Plan & Budget Secure Practices 13
 - Identifying The Problem..... 13
 - Considerations..... 13
 - Identifying A Solution..... 13
 - Use Case #3 – Provide Objective Criteria To Evaluate Third-Party Service Provider Security..... 14
 - Identifying The Problem..... 14
 - Considerations..... 14
 - Identifying A Solution..... 14
 - Use Case #4 – Due Diligence In Mergers & Acquisitions (M&A) 15
 - Identifying The Problem..... 15
 - Considerations..... 15
 - Identifying A Solution..... 15

IEC 62443-2-1

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

IEC 62443-2-1:2010 defines the elements necessary to establish a **cyber security management system (CSMS) for industrial automation and control systems (IACS)** and provides guidance on how to develop those elements. This standard uses the broad definition and scope of what constitutes an IACS described in IEC/TS 62443-1-1.

The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

Organisation: International Electrotechnical Commission (IEC)

Price: CHF 380 (\$140)

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Industrial communication networks – Network and system security –
Part 2-1: Establishing an industrial automation and control system security
program**

**Réseaux industriels de communication – Sécurité dans les réseaux et les
systèmes –
Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes
d'automatisation et de commande industrielles**



CONTENTS

FOREWORD.....	5
0 INTRODUCTION	7
0.1 Overview	7
0.2 A cyber security management system for IACS	7
0.3 Relationship between this standard and ISO/IEC 17799 and ISO/IEC 27001	7
1 Scope.....	9
2 Normative references	9
3 Terms, definitions, abbreviated terms, acronyms, and conventions.....	9
3.1 Terms and definitions	9
3.2 Abbreviated terms and acronyms	14
3.3 Conventions	16
4 Elements of a cyber security management system.....	16
4.1 Overview	16
4.2 Category: Risk analysis.....	18
4.2.1 Description of category.....	18
4.2.2 Element: Business rationale	18
4.2.3 Element: Risk identification, classification and assessment	18
4.3 Category: Addressing risk with the CSMS.....	20
4.3.1 Description of category.....	20
4.3.2 Element group: Security policy, organization and awareness	20
4.3.3 Element group: Selected security countermeasures.....	25
4.3.4 Element group: Implementation	32
4.4 Category: Monitoring and improving the CSMS.....	36
4.4.1 Description of category.....	36
4.4.2 Element: Conformance	36
4.4.3 Element: Review, improve and maintain the CSMS.....	37
Annex A (informative) Guidance for developing the elements of a CSMS.....	39
Annex B (informative) Process to develop a CSMS.....	140
Annex C (informative) Mapping of requirements to ISO/IEC 27001	148
Bibliography.....	156
Figure 1 – Graphical view of elements of a cyber security management system	17
Figure 2 – Graphical view of category: Risk analysis.....	18
Figure 3 – Graphical view of element group: Security policy, organization and awareness	20
Figure 4 – Graphical view of element group: Selected security countermeasures	25
Figure 5 – Graphical view of element group: Implementation	32
Figure 6 – Graphical view of category: Monitoring and improving the CSMS	36
Figure A.1 – Graphical view of elements of a cyber security management system.....	40
Figure A.2 – Graphical view of category: Risk analysis	40
Figure A.3 – Reported attacks on computer systems through 2004 (source: CERT)	44
Figure A.4 – Sample logical IACS data collection sheet	57
Figure A.5 – Example of a graphically rich logical network diagram	59

1. ISO 27001 - www.iso.org/standard/270012
2. ISO 27002 - www.iso.org/standard/75652.html
3. ISF SoGP - www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security
4. NIST CSF - www.nist.gov/cyberframework/framework
5. NIST SP 800-53 - csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
6. CIS Controls - www.cisecurity.org/controls
7. PCI DSS - www.pcisecuritystandards.org/document_library
8. Katakri - www.um.fi/information-security-auditing-tool-for-authorities-katakri
9. COBIT Focus Area: Information Security - store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9hEAC10
10. Information Security Manual (ISM) - www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism
11. New Zealand Information Security Manual (NZISM) - nzism.gcsb.govt.nz
12. Essential Cybersecurity Controls (ECC) - nca.gov.sa/en/legislation
13. SAMA Cyber Security Framework - www.sama.gov.sa/en-us/rulesinstructions/pages/cybersecurity.aspx
14. Cyber Essentials - www.ncsc.gov.uk/cyberessentials
15. IT-Grundschutz - www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
16. CSA Cloud Controls Matrix (CCM) - cloudsecurityalliance.org/research/cloud-controls-matrix
17. State of the art - www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security
18. C2M2 - www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2
19. CyberFundamentals Framework - atwork.safeonweb.be/tools-resources/cyberfundamentals-framework
20. ETSI Standards - www.etsi.org/standards-search
21. HITRUST CSF - hitrustalliance.net/product-tool/hitrust-csf
22. O-ISM3 – www.publications.opengroup.org/c17b
23. Secure Controls Framework (SCF) - securecontrolsframework.com
24. IEC 62443-2-1 - webstore.iec.ch/publication/7030



Thanks, and good luck!

www.linkedin.com/in/andreyprozorov

www.patreon.com/AndreyProzorov

Related presentations



www.patreon.com/posts/my-presentation-88795477



www.patreon.com/posts/12-best-privacy-89048414