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)

INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

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

Reference number
ISO/IEC 27001:2022(E)

Contents

Page

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)

Contents

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

CONTENTS

Click to navigate

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).

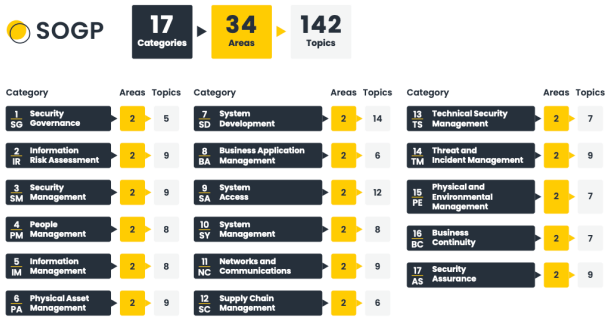


FIGURE 4: The structure of the SOGP

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

Table of Contents

List of Figures

List of Tables

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

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.

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

NIST Special Publication 800-53
Revision 5

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

National Institute of Standards and Technology
U.S. Department of Commerce

Table of Contents

CIS Critical Security Controls

CIS Critical Security Controls (CIS Controls)

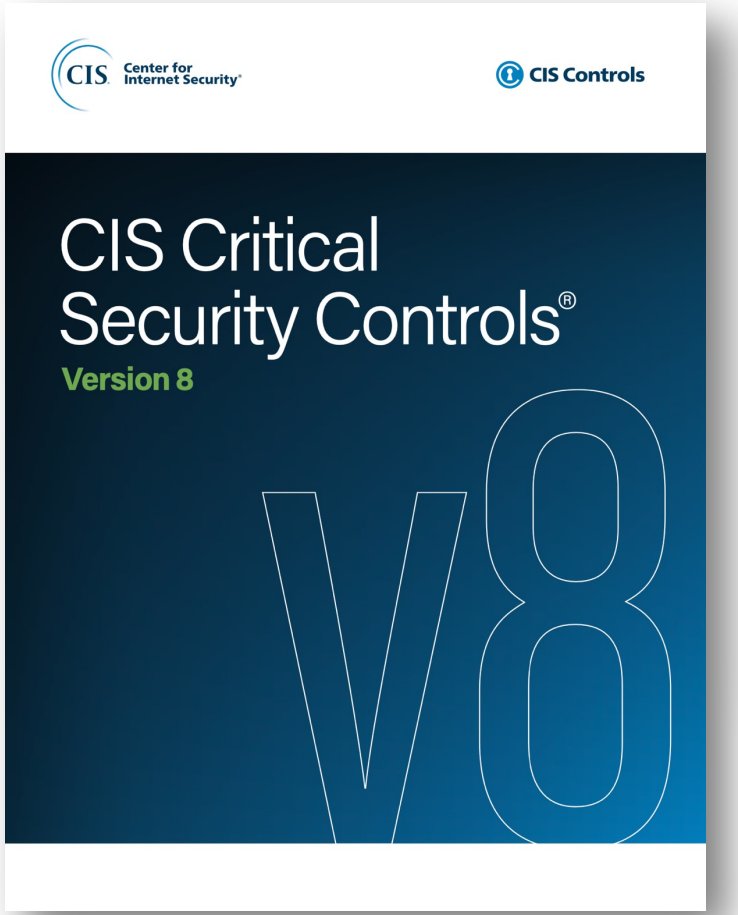
v.8, May 2021

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



Contents

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

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

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

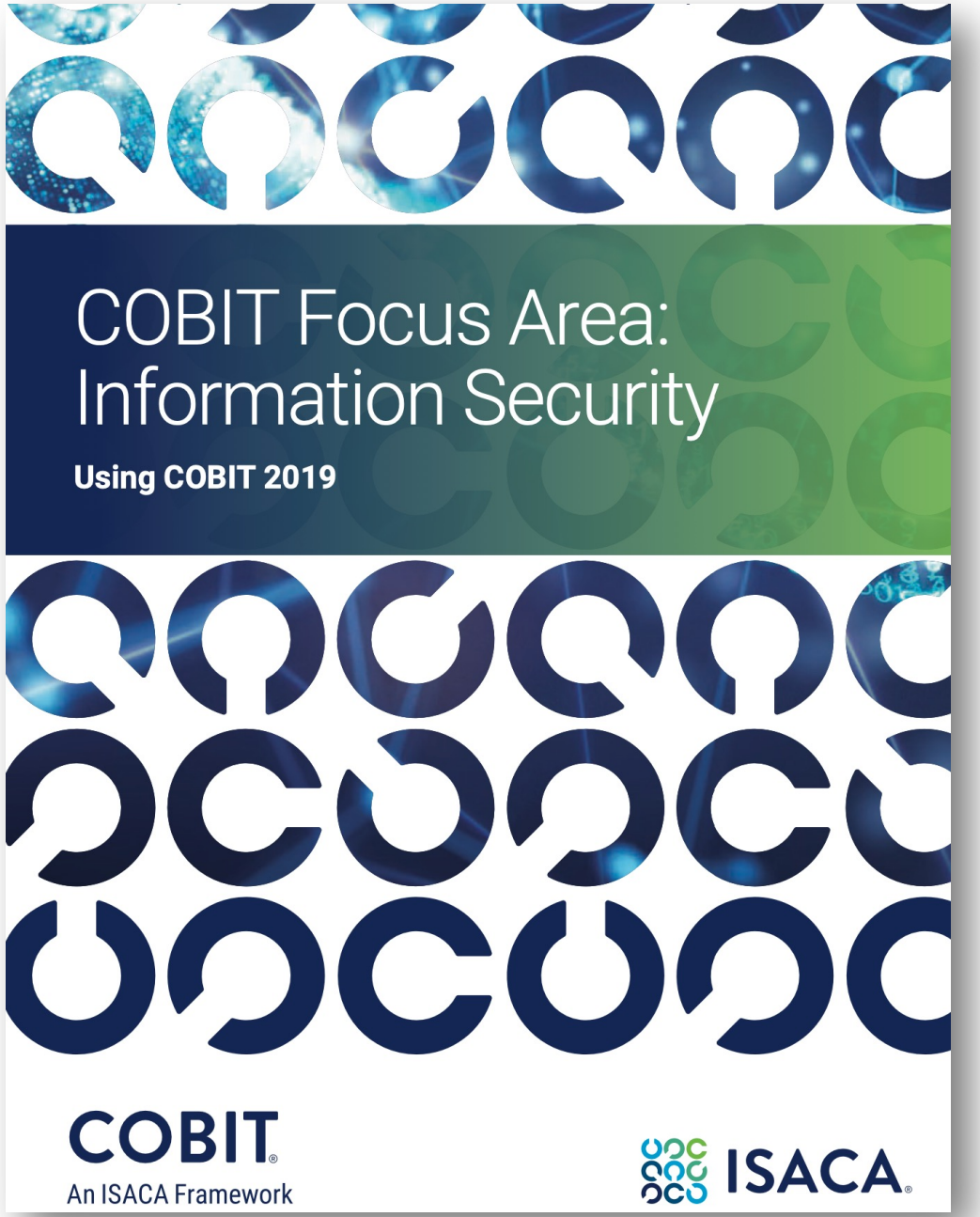


TABLE OF CONTENTS

Information Security Manual (ISM)

Information Security Manual (ISM)

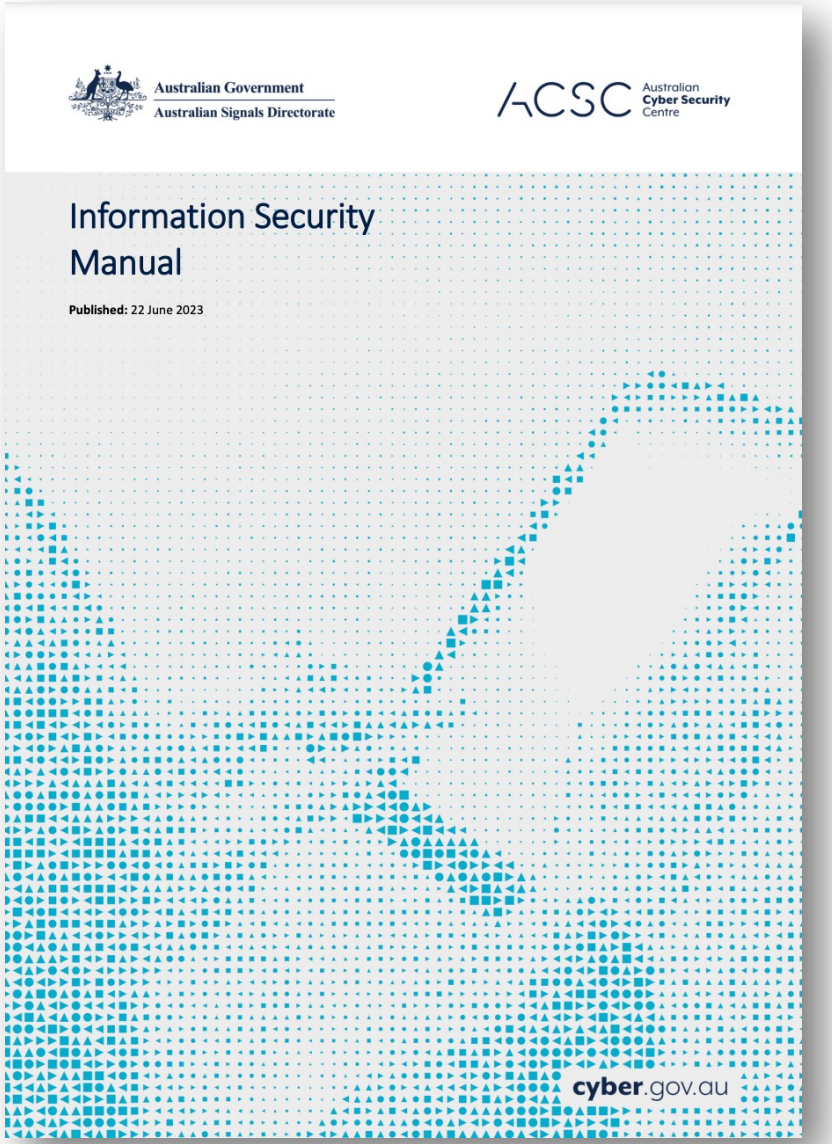
Published: 1 December 2023

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.

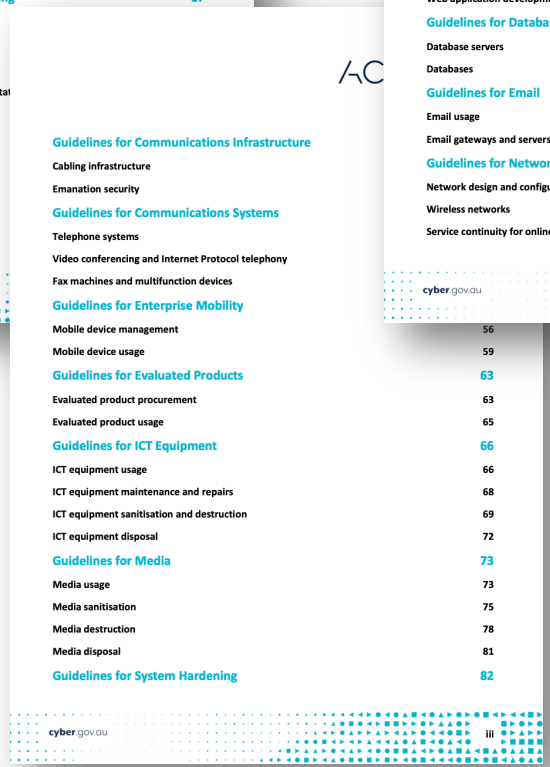
The ISM is intended for Chief Information Security Officers, Chief Information Officers, cyber security professionals and information technology managers.

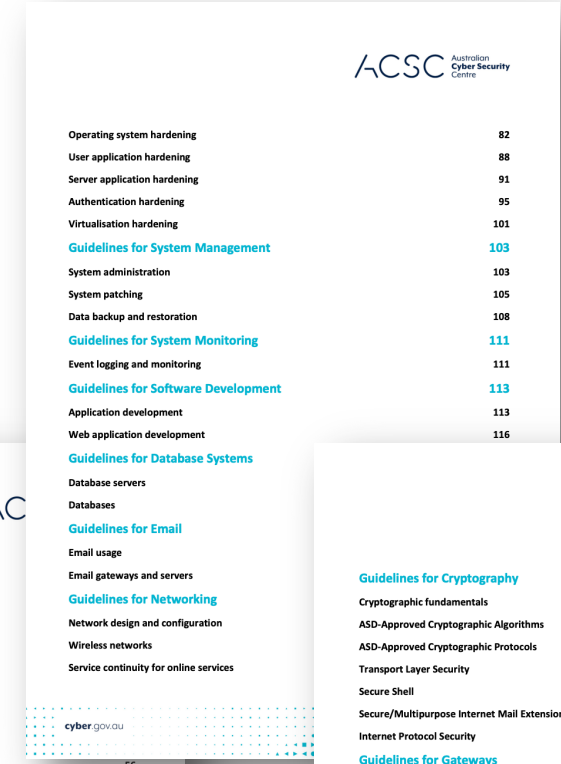
Organisation: Australian Signals Directorate (ASD) / Australian Cyber Security Centre (ACSC)

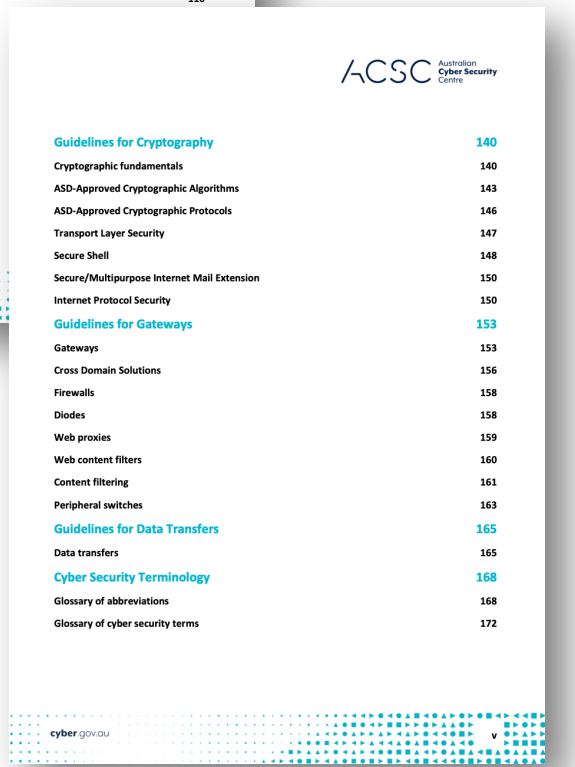
Price: Free


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 supply chain risk management
Managed services and cloud services
Guidelines for Security Documentation
Development and maintenance of security documentat
System-specific security documentation
Guidelines for Physical Security
Facilities and systems
ICT equipment and media
Guidelines for Personnel Security
Cyber security awareness training
Access to systems and their resources
cyber.gov.au


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
iii


ACSC Australian Cyber Security Centre
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
Guidelines for Cryptography 140
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 153
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
v

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

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

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

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

SAMA Cyber Security Framework

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

مؤسسة النقد العربي السعودي
Saudi Arabian Monetary Authority

Cyber Security Framework

Saudi Arabian Monetary Authority

Version 1.0

May 2017

Contents

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

National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

Cyber Essentials:

Requirements for IT infrastructure v3.1

April 2023

Contents

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

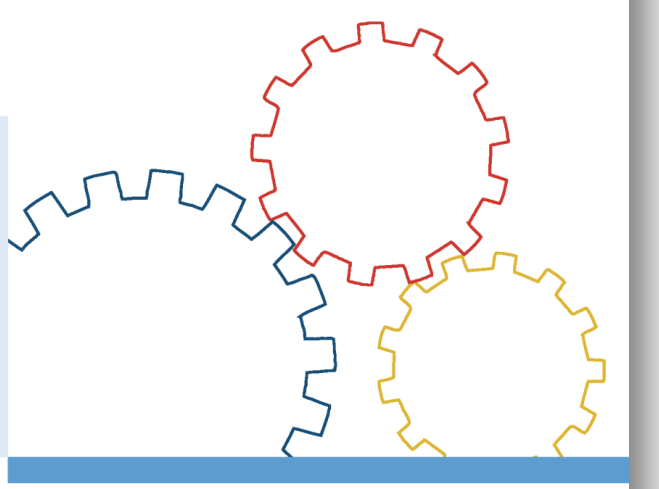
Organisation: Federal Office for Information Security (BSI), Germany

Price: Free

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 200-1

Information Security Management Systems (ISMS)



www.bsi.bund.de/grundschutz

Version 1.0

Table of contents

CSA Cloud Controls Matrix (CCM)

CSA Cloud Controls Matrix (CCM)

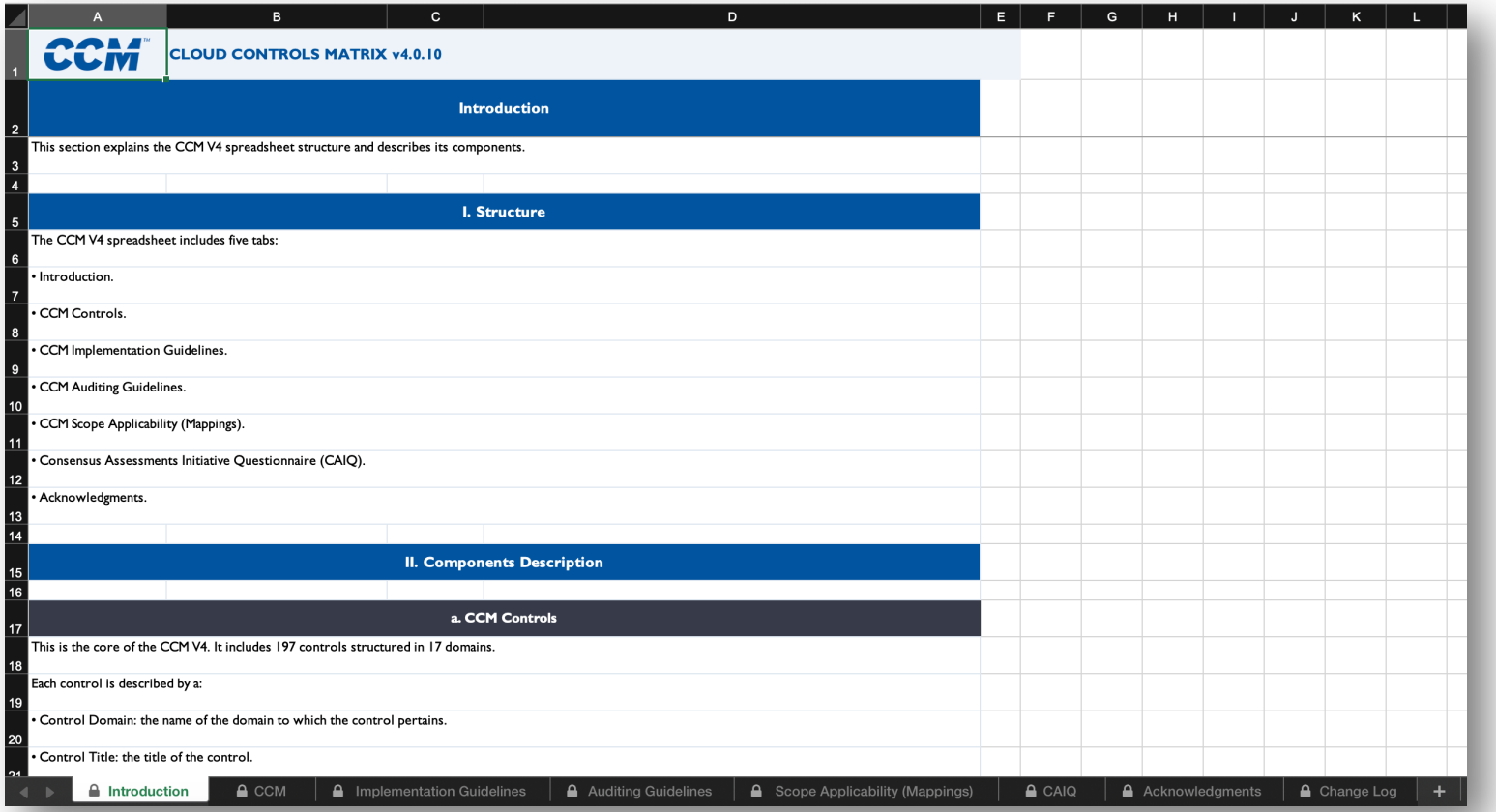
Release Date: 07.06.2021, v.4

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



CCM CLOUD CONTROLS MATRIX v4.0.10

Introduction

This section explains the CCM V4 spreadsheet structure and describes its components.

I. Structure

The CCM V4 spreadsheet includes five tabs:

- Introduction.
- CCM Controls.
- CCM Implementation Guidelines.
- CCM Auditing Guidelines.
- CCM Scope Applicability (Mappings).
- Consensus Assessments Initiative Questionnaire (CAIQ).
- Acknowledgments.

II. Components Description

a. CCM Controls

This is the core of the CCM V4. It includes 197 controls structured in 17 domains.

Each control is described by a:

- Control Domain: the name of the domain to which the control pertains.
- Control Title: the title of the control.

Introduction | CCM | Implementation Guidelines | Auditing Guidelines | Scope Applicability (Mappings) | CAIQ | Acknowledgments | Change Log

"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 Association Germany

TeleTrusT
Pioneers in IT security.

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

enisa
European Network and Information Security Agency

Contents

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

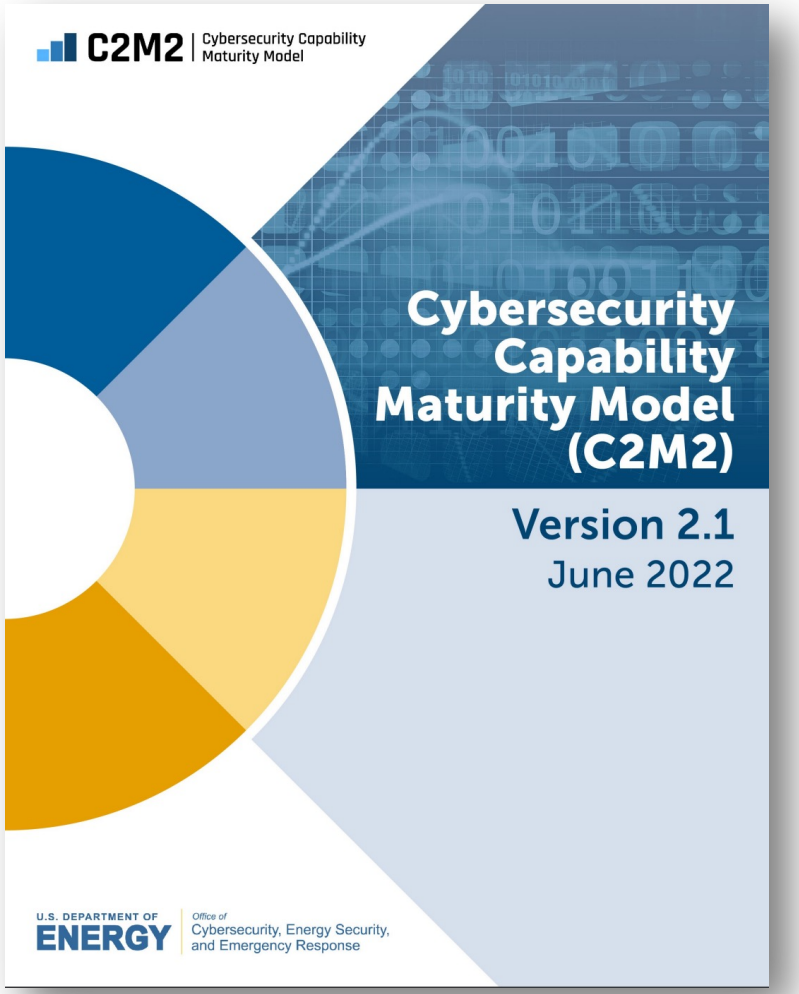


TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

CyberFundamentals Framework

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

Safeonweb @Work

AN INITIATIVE BY

CENTRE FOR CYBER SECURITY BELGIUM

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

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

ETSI TR 103 305-1 V4.1.2 (2022-04)

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

Contents

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®

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.

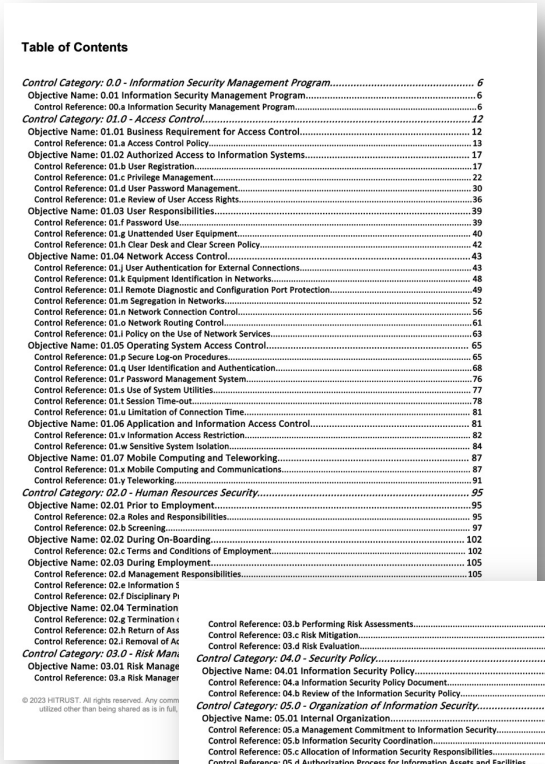
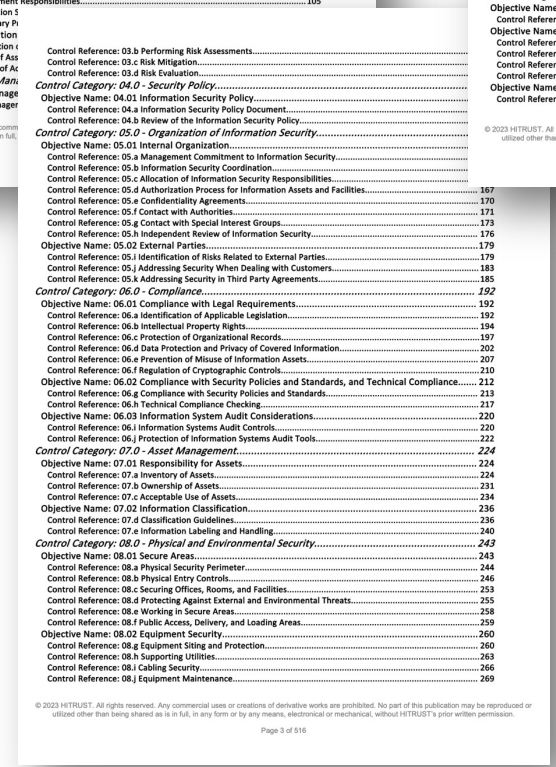
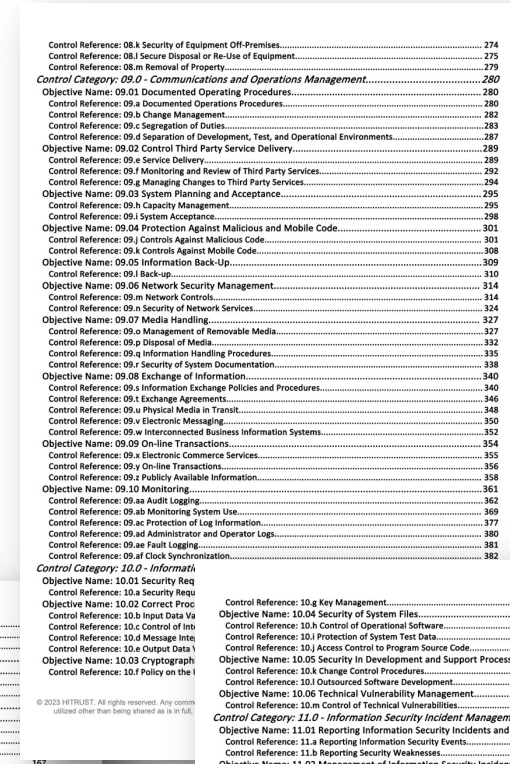
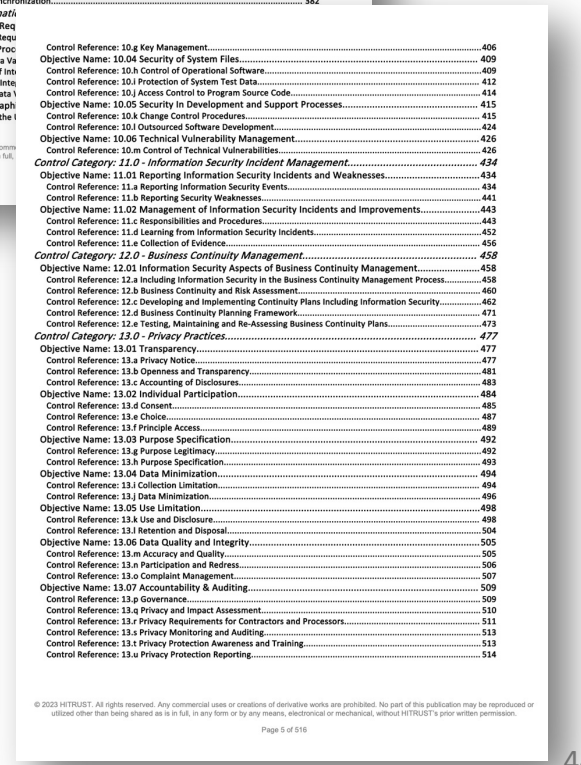


Table of Contents







O-ISM3

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

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

THE Open GROUP

Contents

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

SCF SECURE CONTROLS FRAMEWORK

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

Table of Contents

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 precisely why the Secure Controls Framework™ (SCF) was developed – w practices within organizations so that both cybersecurity and privac 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, to validate any compliance-related assumptions. For more information, please visit www.SecureControlsFram

Table of Contents

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)

IEC

IEC 62443-2-1

Edition 1.0 2010-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

IEC 62443-2-1:2010

CONTENTS

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