ETSI TS 103 305-1 V5.1.1 (2025-09)

TECHNICAL SPECIFICATION

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

Reference
RTS/CYBER-00159

Keywords
cyber security, cyber-defence,
information assurance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

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 [i.46].

The latest version of the Controls is found in the present document. It is the normative version of the ETSI Critical Security Controls. Parts of ETSI TR/TS 103 305, as well as related ETSI Technical Reports and Specifications, assist in the implementation. ETSI publishes derivative international versions. A global array of expert individuals and organizations contribute to provide ongoing development, support, adoption, and use of these Critical Security Controls.

The Controls reflect the combined knowledge of actual attacks and effective defences of experts from every part of the cyber security ecosystem and are implemented in a wide array of publicly available products worldwide, as well as mapped to the diverse sector and governmental cybersecurity frameworks and controls found globally. This ensures that the Controls continually evolve to remain current as an effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks. The most recent changes in the present iteration are described in Annex A.

Introduction

The Controls started as a simple grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and then share that information with a wider audience. The original goals were modest to help people and enterprises focus their attention and get started on the most important steps to defend themselves from the attacks that really mattered.

Under the leadership of the Center for Internet Security (CIS), the Controls initiative has matured into an international community of volunteer individuals and institutions that:

- Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action.
- Create and share tools, working aids, and stories of adoption and problem-solving.
- Map the Controls to regulatory and compliance frameworks in order to ensure alignment and bring collective priority and focus to them.
- Identify common problems and barriers (such as initial assessment and implementation roadmaps), and solve them as a community.

The Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, Information Technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defence, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the Controls.

Evolution of the Controls

The Controls have progressed on a multi-year path to bring more data, rigor, and transparency to the process of best practice recommendations consisting of both the specific Controls as well as ancillary material, especially benchmarks. All of these elements are essential to the maturation of a science to underlie cyber defence and all are necessary to allow the tailoring and "negotiation" of security actions applicable in specific cases, and as required through specific security frameworks, regulations, and similar oversight schemes.

In the earliest versions of the Controls, a standard list of publicly known attacks was used as a simple and informal test of the usefulness of specific recommendations. Starting in 2013, commercial Data Breach Investigations Reports (DBIRs) were used to map the results of their large-scale data analysis directly to the Controls, as a way to match their summaries of attacks into a standard program for defensive improvement.

The Community Defense Model (CDM) [i.15] represents the latest data-driven approach. The CDM combines information from the most recent Data Breach Investigations Reports (DBIRs), along with data from the U.S. Multi-State Information Sharing and Analysis Center (MS-ISAC®), to identify the five most important types of attacks. The attacks are described using the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) Framework to create attack patterns (or specific combinations of Tactics and Techniques used in those attacks). This approach allows analysis of the value of individual defensive actions (i.e. Safeguards) against those attacks. Previous versions of the Controls used the term "sub-controls" rather than "safeguards". This approach also provides a consistent and explainable way to look at the security value of a given set of defensive actions across the attacker's life cycle, and provide a basis for strategies like defence-in-depth. It represents a major step towards identifying the security value of the Controls, or any subset. These activities ensure that the Security Best Practices (which include the Controls and Benchmarks) are a prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements.

ETSI has also produced a set of related publications that facilitate the implementation of the Controls:

- Internet of Things Sector [i.4].
- Mobile Communications Sector [i.8].
- Cloud Sector [i.9].
- Facilitation Mechanisms, including Hardened Images, Compliance Control Mappings and Navigation, Guide for Small and Medium-sized Enterprises (SMEs), Control Assessment Mechanisms, Controls Assessment Specification (CAS), Controls Workbench, Risk Assessment Method (RAM), Community Defense Model, Critical Security Control benchmarks, Open Security Controls Assessment Language (OSCAL) [i.5].
- Privacy and personal data protection enhancement [i.6].
- Implementation of the Revised Network and Information Security (NIS2) Directive [i.7] and [i.10].

The Controls Ecosystem

Meaningful use of Controls, whether these Critical Security Controls or others, encompasses much more than focusing on a list of steps. There are many lists of ICT security controls. The ultimate value of these Controls is the ecosystem of individuals and enterprises who actually make security improvements through the sharing of ideas, tools, lessons, and collective action. The ecosystem includes unique assets including:

- a catalyst and clearinghouse blog;
- mappings to a very wide variety for formal Risk Management Frameworks;
- use cases of enterprise adoption;
- references to the Critical Security Controls in national and international standards, state and national legislation and regulation, trade and professional associations;
- information tailored for small and medium enterprises;
- measurement and metrics for the Controls;
- vendor white papers and other materials that support the Controls.

Historically, the Controls were ordered in sequence to focus enterprise cybersecurity activities, with a subset of the first six Controls referred to as "cyber hygiene". However, this proved to be too simplistic. Enterprises, especially small ones, could struggle with some of the early Safeguards and never implement additional Controls (for example, having a backup strategy to help recover from ransomware).

Beginning with Critical Security Controls ETSI TR 103 305-1 (V4.1.1) [i.47] in 2021 and their CIS equivalent, controls Implementation Groups (IGs) were developed to tailor and prioritize implementation. The IGs are self-assessed categories for enterprises. Each IG identifies a subset of the Controls that the community has broadly assessed to be applicable for an enterprise with a similar risk profile and resources to strive to implement. These IGs represent a horizontal look across the Controls tailored to different types of enterprises. IG1 has effectively become "basic cyber hygiene" that include the foundational set of cyber defence Safeguards that every enterprise should apply to guard against the most common attacks. Each IG then builds upon the previous one: IG2 includes IG1, and IG3 includes all Control Safeguards in IG1 and IG2.

The most recent changes in the present iteration are described in Annex A.

1 Scope

The present document describes a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber-attacks. The measures reflect the combined knowledge of actual attacks and effective defences.

The present document is technically equivalent and compatible with CIS Controls®, Version 8.1 of the Center for Internet Security [i.46].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] Void.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] NIST: "The NIST Cybersecurity Framework (CSF) 2.0", 26 February 2024.

[i.2] UK NCSC: "Cyber Assessment Framework".

[i.3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.4] ETSI TR 103 305-3: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 3: Internet of Things Sector".

[i.5] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.6] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.7] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.8] ETSI TR 103 954: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Mobile Communications Sector".

[i.9] ETSI TR 103 959: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Cloud Sector".

[i.10] ETSI TS 103 992: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.11] CIS: "Critical Security Controls ICS Companion Guide".

[i.12] NIST Special Publication 800-88 Revision 1: "Guides for Media Sanitization.

[i.13] NIST FIPS PUB 140-3: "Security Requirements for Cryptographic Modules".

[i.14] CIS: "CIS Benchmarks List".

[i.15] CIS: "CIS Community Defense Model 2.0".

[i.16] CIS: "CIS-CAT Lite".

[i.17] NIST: "Digital Identity Guidelines".

[i.18] CIS: "CIS Password Policy Guide".

[i.19] CVE: "CVE™ Program Mission".

[i.20] NIST: "Common Configuration Enumeration (CCE)".

[i.21] MITRE: "Open Vulnerability and Assessment Language (OVAL®)".

[i.22] MITRE: "Common Platform Enumeration (CPE)".

[i.23] FIRST: "Common Vulnerability Scoring System: Specification Document".

[i.24] NIST: "Extensible Configuration Checklist Description Format (XCCDF)".

[i.25] NIST Special Publication 800-126 Revision 3: "The Technical Specification for the Security Content Automation Protocol (SCAP)".

[i.26] CIS: "Living off the Land: Threats Looming From Within".

[i.27] CIS: "CIS Critical Security Controls v7.1 Telework and Small Office Network Security Guide".

[i.28] NIST Special Publication SP 800-50r1: "Building a Cybersecurity and Privacy Learning Program".

[i.29] National Cyber Security Centre (UK): "10 Steps to Cyber Security".

[i.30] EDUCAUSE: "Awareness Campaigns".

[i.31] National Cybersecurity Alliance (NCSA): "Empowering a more secure, interconnected world".

[i.32] SANS Security Awareness: "Resources".

[i.33] Void.

[i.34] SAFECode: "Application Software Security and the CIS Controls".

[i.35] NIST: "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)".

[i.36] The Software Alliance: "BSA Framework for Secure Software".

[i.37] OWASP®: "Explore the world of cyber security".

[i.38] CDC: "Health Insurance Portability and Accountability Act of 1996 (HIPAA)".

[i.39] Federal Financial Institutions Examination Council (FFIEC).

[i.40] ETSI TR 103 331: "Cyber Security (CYBER); Structured threat information sharing".

[i.41] ENISA: "Awareness and Cyber Hygiene".

[i.42] IEEE 802.1X™-2010: "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control".

[i.43] NIST: "National Checklist Program - Checklist Repository".

[i.44] National Cyber Security Centre: "Cyber Essentials".

[i.45] EDUCAUSE: "Higher Education Community Vendor Assessment Toolkit™ (HECVAT)".

[i.46] The Center for Internet Cybersecurity: "CIS Critical Security Controls®", Version 8.1, 2024.

[i.47] ETSI TR 103 305-1 (V4.1.1): "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

accounts: profile, identity, or membership created for a person, group, or machine entity that grant access to resources or functionalities within a computer system or network

NOTE: A system of accounts is important for managing permissions and security levels across an enterprise, and an individual may have access to multiple accounts depending on job roles and security requirements. User accounts are for individual users and are tailored for the specific tasks their roles and responsibilities require. User accounts, administrator accounts, and service accounts are subsets of accounts.

administrator accounts: dedicated accounts with escalated privileges and used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure

NOTE: Common administrator account subtypes include root accounts, local administrator and domain administrator accounts, and network or security appliance administrator accounts.

applications: program, or group of programs, hosted on enterprise assets and designed for end-users - which are considered a software asset in the present document, and include web, database, cloud-based, and mobile applications

NOTE: Applications are considered a software asset in the present document.

Application Programming Interface (API): set of rules and interfaces for software components to interact with each other in a standardized way

NOTE: APIs allow applications to access and communicate with both internal and external resources.

asset class: program, or group of programs, running on top of an operating system hosted on an enterprise asset

EXAMPLE: Application types include web, database, cloud-based, and mobile. Applications are considered a software asset in the present document.

authentication systems: system or mechanism used to identify a user through associating an incoming request with a set of identifying credentials

NOTE: The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system, user directory service, or within an authentication server.

EXAMPLE: Active directory, Multi-Factor Authentication (MFA), biometrics, and tokens.

authorization systems: system or mechanism used to determine access levels or user/client privileges related to system resources including files, services, computer programs, data, and application features

NOTE: An authorization system grants or denies access to a resource based on the user's identity.

EXAMPLE: Active directory, access control lists, and role-based access control lists.

bi-annually: every six months

NOTE: Any tasks that should be done bi-annually should also be repeated whenever significant change has occurred that would affect the network or devices in question, including changes such as hardware upgrades or mergers and acquisitions.

breach: loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:

- a person other than an authorized user accesses or potentially accesses sensitive or confidential information; or
- an authorized user accesses sensitive or confidential information for other than authorized purposes

cloud environment: virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services

NOTE: There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Critical Security Control (CSC): specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts

data: collection of facts that can be examined, considered, and used for decision-making

NOTE: Although data may be physical, the Critical Security Controls primarily provide protection for digital data that may be stored, transferred, and processed by enterprise assets.

data exposure: unintentional data breach

database: organized collection of data, generally stored and accessed electronically from a computer system

NOTE: Databases can reside remotely or on-site. Database Management Systems (DMSs) are used to administer databases, and are not considered part of a database for the present document.

devices: objects that physically or virtually exist and capable of interacting with an information network

NOTE: Devices may exist in physical spaces, virtual infrastructure, or cloud-based environments. Devices can remotely connect to these systems, and typically include a laptop, personal computer, and smartphone.

documentation: policies, processes, procedures, plans, diagrams, and other written material (e.g. compliance reports) either physical or digital

EXAMPLE: A methods of governance for an enterprise, processes that users follow, or describe network architecture.

dwell time: period of time between an initial attack and the detection of an intrusion when an attacker has unauthorized access to the data and the environment

end-user devices: Information Technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose

NOTE: End-user devices include mobile and portable devices such as laptops, smartphones and tablets, as well as desktops and workstations. For the purpose of the present document, end-user devices are a subset of enterprise assets.

enterprise: any business or organization that uses computer systems, networks and devices

enterprise assets: assets with the potential to store or process data

NOTE: For the purpose of the present document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments.

externally-exposed applications: applications that are public facing and discoverable through reconnaissance and network scanning from the public internet outside of the enterprise's network

externally-exposed enterprise assets: enterprise assets that are public facing and discoverable through domain name system reconnaissance and network scanning from the public internet outside of the enterprise's network

firmware: software stored within a device's non-volatile memory, such as ROM or flash memory, used to allow different types of hardware to communicate with the operating system

NOTE: Firmware is often updated outside of the enterprise's operating system and application software update process.

governance: security function that is a Control Safeguard attribute necessary to achieve an enterprise policy or plan

internal enterprise assets: non-public facing enterprise assets that can only be identified through network scans and reconnaissance from within an enterprise's network through authorized authenticated or unauthenticated access

Internet of Things (IoT): devices embedded with sensors, software, and other technologies

NOTE: These devices may connect, store, and exchange data with other devices and systems. The device's connection to the internet can be intermittent, non-existent, or persistent. For the purpose of the present document, IoT and non-computing devices are a subset of enterprise assets.

EXAMPLE: Smart watches and other wearables, printers, smart screens, smart home devices, speakers, industrial control systems, and physical security sensors.

library: shareable pre-compiled codebase to include classes, procedures, scripts, configuration data, and more, used to develop software programs and applications

NOTE: Libraries are designed to assist both the programmer and the programming language compiler in building and executing software more efficiently.

logs data: computer-generated data file that records the events occurring within the enterprise

EXAMPLE: Operating system, anti-malware detection, database, application, network, firewall, web server, or access control logs (e.g. electronic locks, alarm system).

mobile devices: small, enterprise issued end-user devices with intrinsic wireless capability, such as smartphones and tablets

NOTE: For the purposes of the present document, mobile devices are a subset of portable devices.

multi-factor authentication: authentication using two or more different factors to achieve authentication, and include something known (e.g. PIN, password), something possessed (e.g. cryptographic identification device, token), or a personal attribute (e.g. biometric)

network: group of interconnected devices that exchange data

NOTE: Network is a superset of network infrastructure and network architecture.

network architecture: how a network is designed, both physically and logically

NOTE 1: It defines how a network is organized, including the connections between devices and software as well as the data that is transmitted between them.

NOTE 2: This should include network architecture diagrams and security architecture diagrams.

network asset: group of interconnected devices that exchange data

NOTE: Enterprises may operate one or more networks that are managed together or independently.

network devices: electronic devices required for communication and interaction between devices on a computer network

NOTE: Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware, as well as virtual and cloud-based devices. For the purpose of the present document, network devices are a subset of enterprise assets.

network infrastructure: all of the resources of a network that make network or internet connectivity, management, business operations, and communication possible

NOTE: It consists of hardware and software, systems and devices, and it enables computing and communication between users, services, applications, and processes. Network infrastructure can be cloud, physical, or virtual.

non-computing/Internet of Things (IoT) devices: devices embedded with sensors, software, and other technologies for the purpose of connecting, storing, and exchanging data with other devices and systems over the internet

NOTE: While these devices are not used for computational processes, they support an enterprise's ability to conduct business processes. For the purpose of the present document, non-computing/IoT devices are a subset of enterprise assets.

EXAMPLE: Printers, smart screens, physical security sensors, industrial control systems, and information technology sensors.

Operating System (OS): system software on enterprise assets that manages computer hardware and software resources, and provides common services for programs

phishing: such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person

physical data: data that is stored in physical documents or stored on physical types of removable devices (e.g. USB drives, tape backups)

NOTE: Physical data may be sensitive or not.

physical environment: physical hardware parts that make up a network, including cables and routers which is required for communication and interaction between devices on a network

plan: implements policies and may include groups of policies, processes, and procedures

policy: official governance statement that outlines specific objectives of an information security program and either dictate actions that should be taken or specify which actions are prohibited

portable devices: transportable, end-user devices that have the capability to wirelessly connect to a network

NOTE: Portable end-user devices can include laptops which may require external hardware for connectivity and mobile devices, such as smartphones and tablets. For the purpose of the present document, portable devices are a subset of end-user devices.

portable end-user devices: transportable, end-user devices that have the capability to wirelessly connect to a network

NOTE: For the purpose of the present document, portable end-user devices can include laptops and mobile devices such smartphones and tablets, all of which are a subset of enterprise assets.

pretexting: part of a social engineering attack that involves inventing a scenario to convince the victim to divulge information that should not be divulged, whose is to convince the victim of the legitimacy of the communication

NOTE: The method of this type of attack can be through any communication method or medium.

procedure: ordered set of steps that need to be followed to accomplish a specific task and provides the approved way of performing an action in a specific technological and organizational environment

process: set of general tasks and activities to achieve a series of security-related goals that is documented in a Plan, Policy, Procedure, or less formally

remote devices: any enterprise asset capable of connecting to a network remotely, usually from a public internet

EXAMPLE: End-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers.

remote file systems: systems enabling an application that runs on an enterprise asset to access files stored on a different asset

NOTE: Remote file systems often make other resources, such as remote non-computing devices, accessible from an asset. The remote file access takes place using some form of local area network, wide area network, point-to-point link, or other communication mechanism. These file systems are often referred to as network file systems or distributed file systems.

removable media: any type of storage device that can be removed from a computer while the system is running and allows data to be moved from one system to another

EXAMPLE: Compact Discs (CDs), Digital Versatile Discs (DVDs) and Blu-ray discs, tape backups, as well as diskettes and Universal Serial Bus (USB) drives.

safeguard: specific actions that enterprises should take to implement the Control consisting of four attributes:

- Asset Type;
- Security Function;
- Implementation Group;
- Specific Actions

script: uncompiled code that requires a software environment to execute

security function: attribute tag that enables mapping to cybersecurity compliance framework functions adopted by other parties

NOTE: See [i.1].

sensitive data: data stored, processed, or managed by the enterprise that need to be kept private (Confidential), accurate and reliable (Integrity), and/or available (Availability), and if released or destroyed in an unauthorized manner, would cause harm to the enterprise or its customers

NOTE: These impacts may be due to a data breach or a violation of a policy, contract, or regulation.

servers: device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network

NOTE: Servers can provide resources and use them from another system at the same time. Servers can exist in datacentres, public/private/hybrid cloud environments, including temporal containers or serverless workloads. For the purpose of the present document, servers are a subset of enterprise assets.

EXAMPLE: Web servers, application servers, mail servers, and file servers.

service accounts: accounts created specifically to run applications, services, and automated tasks on an operating system or created just to own data and configuration files

NOTE: Each service account should be used for a specific service or function, and should have an assigned owner who is responsible for how the account is used. Service accounts should not be used for general purpose computing.

services: specialized programs that perform well-defined critical tasks for the operating system

NOTE: Services often start with the operating system, run-in in the background, and can be stopped and started by users. Example services include managing network communications, users, file permissions, system security, and device interaction.

service provider: entities that offer platforms, software, and services to other enterprises.

EXAMPLE: IT contractors, Managed Service Providers (MSPs), and cloud service providers.

social engineering: broad range of malicious activities accomplished through human interactions on various platforms, such as email or phone, and which relies on psychological manipulation to trick users into making security mistakes or giving away sensitive information

software: sets of data and instructions used to direct a computer to complete a specific task, including operating systems and applications

NOTE: Both may contain services, libraries, or Application Programming Interfaces (APIs).

tailgating: physical security issue where an individual follows another into a secured area without properly authenticating or following established protocols for entering the area

third-party provider: Same as service provider, above.

users: employees, third-party vendors, contractors, service providers, consultants, or any other person who is authorized to access an enterprise asset, and includes user, administrator, and service accounts

user accounts: identity comprised of a set of credentials (e.g. username, password) that defines a user on a computer or computing system

NOTE: A user account keeps track of a user's information and settings, controls the files, folders, and resources a user is allowed to access, as well as the tasks a user is allowed to perform. For the purpose of the present document, user accounts refer to "standard" user accounts with limited privileges and are used for general tasks.

virtual environment: environment simulating hardware to allow a software environment to run without the need to use a lot of actual hardware which are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity, and allows cloud computing to work

workforce: all individuals who are employed or engaged by an organization and have access to its information systems, assets, or resources, and includes all employees both onside and remote, excluding service providers and contractors

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA	Authentication, Authorization and Auditing
ACL	Access Control List
AD	Active Directory
AoC	Attestation of Compliance
API	Application Programming Interface
ATT&CK®	Adversarial Tactics, Techniques and Common Knowledge
BASH	Bourne Again SHell
BEC	Business Email Compromise
C2	Command and Control
CAS	Controls Assessment Specification
CAT	Cyber Assessment Tool
CCE	Common Configuration Enumeration
CD	Compact Disc
CDM	Continuous Diagnostic and Mitigation
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
COTS	Commercial Off-The-Shelf
CPE	Common Platform Enumeration
CREST	Council of REgistered Security Testers
CSA	Cloud Security Alliance
CSAT	CIS Configuration Assessment Tool

CSC	Critical Security Control or Capability
CSF	CyberSecurity Framework
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DBIR	Data Breach Investigations Report
DEP	Data Execution Prevention
DG	Development Group
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DMS	Database Management System
DNS	Domain Name System
DPI	Deep Packet Inspection
DVD	Digital Video Disc
EDR	Endpoint Detection and Response
EOL	End-Of-Life
FFIEC	Federal Financial Institutions Examination Council
GRC	Governance Risk and Compliance
HECVAT	Higher Education Community Vendor Assessment Toolkit
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IG	Implementation Group
IOC	Indicator Of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
LotL	Living off the Land
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSP	Managed Service Provider
NaaS	Network as a Service
NCSA	National Cyber Security Alliance
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Protection System
NIS2	Network Information Security 2
NIST	National Institute of Standards and Technology
OS	Operating System
OSCAL	Open Security Controls Assessment Language
OSS	Open Source Software
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI	Payment Card Industry
RAM	Risk Assessment Method
SaaS	Software as a Service
SAFECode	Software Assurance Forum for Excellence in Code
SCADA	Supervisory Control And Data Acquisition
SCAP	Security Content Automation Protocol
SIEM	Security Information Event Management or Security Incident Event Management

SIP	System Integrity Protection
SLA	Service Level Agreement
SME	Small and Medium Enterprise
SMS	Short Messaging Service
SOC 2	Service Organization Control 2
SOC	Security Operations Centre
SPAM	Something Posing As Mail
SPF	Sender Policy Framework
SQL	Structured Query Language
SSDF	Secure Software Development Framework
SSH	Secure SHell
SSO	Single Sign-On
Telnet	Teletype Network
TLS	Transport Layer Security
TTPs	Tactics, Techniques and Procedures
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi® Protected Access 2
XCCDF	eXtensible Configuration Checklist Description Format

4 Critical Security Controls

4.0 Structure of the Critical Security Controls

4.0.1 Introduction

The presentation of each Control in the present document includes the following elements:

- **Overview:** A brief description of the intent of the Control and its utility as a defensive action.
- **Why is This Control Critical?** A description of the importance of this Control in blocking, mitigating, or identifying attacks, and an explanation of how attackers actively exploit the absence of this Control.
- **Procedures and Tools:** A technical description of the processes and technologies that enable implementation and automation of this Control.
- **Safeguards:** A list of the specific actions that enterprises should take to implement the Control. Each Safeguard consists of four attributes described in the clauses below:
  - Asset Type;
  - Security Function;
  - Implementation Group;
  - Specific Actions.

4.0.1a Asset Types

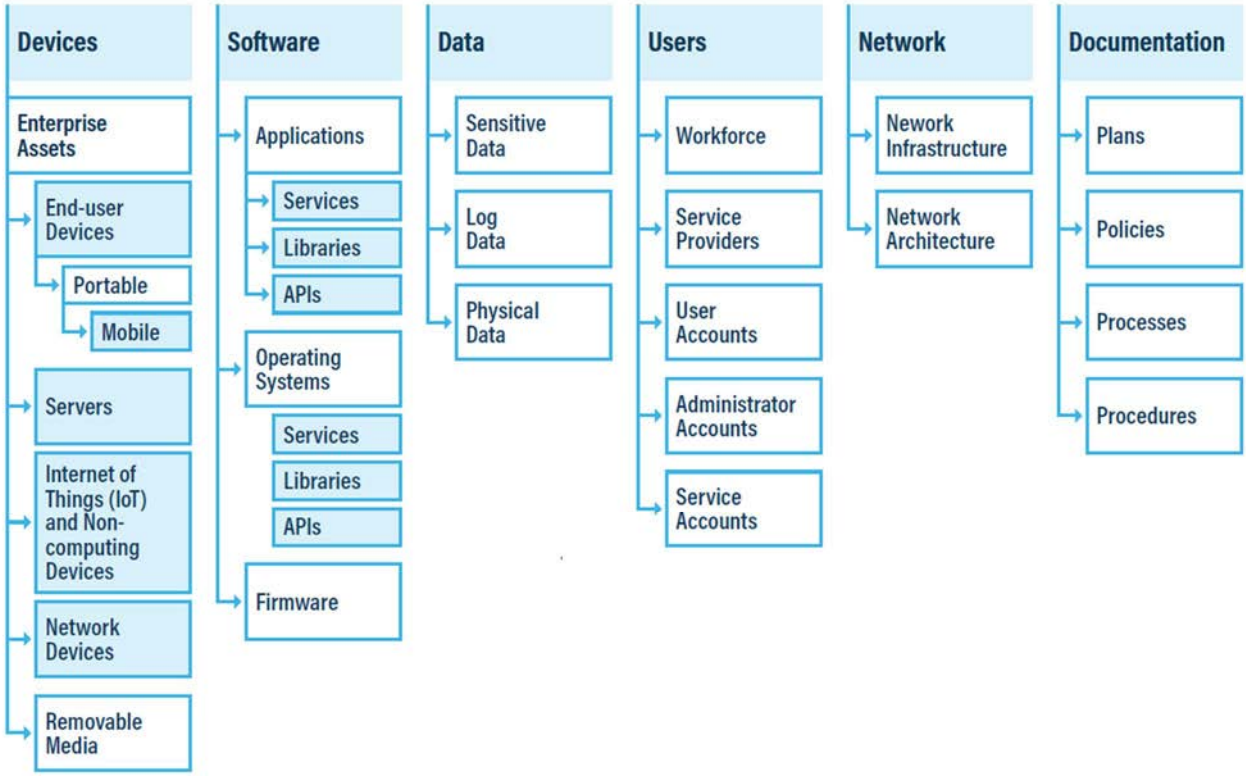

Figure 4.0-1

Devices: Devices may exist in physical spaces, virtual infrastructure, or cloud-based environments. Devices can remotely connect to these systems:

- **Enterprise Assets:** Assets with the potential to store or process data. For the purpose of the present document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments.
- **End-user Devices:** Information Technology (IT) assets used among members of an enterprise during work or off-hours. End-user devices include desktops and workstations, as well as portable and mobile devices such as laptops, smartphones, and tablets. For the purpose of the present document, end-user devices are a subset of enterprise assets.
    - **Portable Devices:** Transportable, end-user devices that have the capability to wirelessly connect to a network. Portable end-user devices can include laptops which may require external hardware for connectivity and mobile devices, such as smartphones and tablets. For the purpose of the present document, portable devices are a subset of end-user devices:
        - **Mobile Devices:** Small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. For the purpose of the present document, mobile devices are a subset of portable devices.
- **Servers:** A device or system that provides resources, data, services, or programs to other devices. Servers can exist in datacentres, public/private/hybrid cloud environments, including virtual machines, temporal containers, or serverless workloads. Examples of servers include web servers, application servers, mail servers, and file servers. For the purpose of the present document, servers are a subset of enterprise assets.
- **Internet of Things (IoT) and Non-computing Devices:** Devices embedded with sensors, software, and other technologies. These devices may connect, store, and exchange data with other devices and systems. The device's connection to the internet can be intermittent, non-existent, or persistent. Examples of these devices include smart watches and other wearables, printers, smart screens, smart home devices, speakers, industrial control systems, and physical security sensors. For the purpose of the present document, IoT and non-computing devices are a subset of enterprise assets.

- **Network Devices:** Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, switches, routers, and gateways, both physical and virtual. These devices consist of physical hardware, as well as virtual and cloud-based devices. For the purpose of the present document, network devices are a subset of enterprise assets. Network devices are listed under enterprise assets because they are managed much like other devices; however, they also play a dual role in the network asset class when related to the communication over a network.

- **Removable Media:** Any type of storage device that can be removed from a computer while the system is running and allows data to be moved from one system to another. Examples of removable media include CDs, DVDs, Blu-ray Discs, external hard drives, SD cards, tape backups, diskettes, and USB drives.

Software: Sets of data and instructions used to direct a computer to complete a specific task. Software assets include operating systems and applications. Both may contain services, libraries, or Application Programming Interfaces (APIs):

- **Applications:** A program, or a group of programs, running on top of an operating system hosted on an enterprise asset. Example application types include web, database, cloud-based, and mobile. Applications are considered a software asset in the present document.

- **Operating Systems:** Software on enterprise assets that manages computer hardware and software resources and provides common services for programs. Example operating systems include Windows, Ubuntu, MacOS, Android, and z/OS. Operating systems are considered a software asset:

    - **Services:** Specialized programs that perform well-defined critical tasks for the operating system. Services often start with the operating system, run-in in the background, and can be stopped and started by users. Example services include managing network communications, users, file permissions, system security, and device interaction.

    - **Library:** A shareable pre-compiled codebase to include classes, procedures, scripts, configuration data, and more, used to develop software programs and applications. Libraries are designed to assist both the programmer and the programming language compiler in building and executing software more efficiently.

    - **Application Programming Interface (API):** A set of rules and interfaces for software components to interact with each other in a standardized way. APIs allow applications to access and communicate with both internal and external resources.

- **Firmware:** Software stored within a device's non-volatile memory, such as ROM or flash memory, used to allow different types of hardware to communicate with the operating system. Firmware is often updated outside of the enterprise's operating system and application software update process.

Data: A collection of facts that can be examined, considered, and used for decision-making. Enterprises often store and process data important to organizational operations but is not classified as sensitive; and this data still needs to be appropriately protected. Although data may be physical, the CIS Controls primarily provide protection for digital data that may be stored, transferred, and processed by a computing system:

- **Sensitive Data:** Physical or digital data stored, processed, or managed by the enterprise that needs to be kept private, accurate, reliable, and available. If released or destroyed in an unauthorized manner, it would cause harm to the enterprise or its customers. These impacts may be due to a data breach or a violation of a policy, contract, or regulation.

- **Log Data:** A computer-generated data file that records the events occurring within the enterprise. Examples of logs include operating system, anti-malware detection, database, application, network, firewall, web server, or access control logs (e.g. electronic locks, alarm system).

- **Physical Data:** Data that is stored in physical documents or stored on physical types of removable devices (e.g. USB drives, tape backups). Physical data may be sensitive or not.

Users: Employees, third-party vendors, contractors, service providers, consultants, or any other person who is authorized to access an enterprise asset. This also includes user, administrator, and service accounts:

- **Workforce:** All individuals who are employed or engaged by an organization and have access to its information systems, assets, or resources. It includes employees both on-site and remote. Contractors are often part of the workforce, whereas consultants and service providers are not, although this may vary based on the contract.
- **Service Providers:** Service providers are entities that offer platforms, software, and services to other enterprises. Examples include IT consultants, Managed Service Provider (MSPs), Software as a Service (SaaS) platforms, and cloud service providers. Third-party providers and vendors are also considered Service Providers. These services may be paid or free. Some relationships may or may not require a contract or SLA in place. Examples include data analysis, traffic blocking, and similar services.
- **User Accounts:** An identity comprised of a set of credentials (e.g. username, password) that defines a user on a computer or computing system. A user account keeps track of a user's information and settings, controls the files, folders, and resources a user is allowed to access, as well as the tasks a user is allowed to perform. For the purpose of the present document, user accounts refer to "standard" user accounts with limited privileges and are used for general tasks.
- **Administrator Accounts:** Accounts for users requiring escalated privileges. The accounts are used for managing aspects of a computer, domain, or the whole enterprise information technology infrastructure. Each administrator account should be assigned to a single user. Common administrator account subtypes include root accounts, local administrator, domain administrator accounts, and network or security appliance administrator accounts.
- **Service Accounts:** A service account is created specifically to run applications, services, and automated tasks on an operating system. Service accounts may also be created just to own data and configuration files. Each service account should be used for a specific service or function, and it should have an assigned owner who is responsible for how the account is used. Service accounts should not be used for general purpose computing.

Network: A group of interconnected devices that exchange data. Enterprises may operate one or more networks that are managed together or independently:

- **Network Infrastructure:** The collection of network resources that provide connectivity, management, business operations, and communication. It consists of hardware and software, systems and devices, and it enables computing and communication between users, services, applications, and processes. Network infrastructure can be in the cloud, physical, or virtual.
- **Network Architecture:** Refers to how a network is designed, both physically and logically. It defines how a network is organized, including the connections between devices and software as well as the data that is transmitted between them. This should include network architecture diagrams and security architecture diagrams.

Documentation: Policies, processes, procedures, plans, diagrams, and other written material (e.g. compliance reports) either physical or digital. Examples include methods of governance for an enterprise, processes that users follow, or describe network architecture:

- **Plan:** Implements policies and may include groups of policies, processes, and procedures.
- **Policy:** An official governance statement that outlines specific objectives of an information security program. A policy will either dictate actions that need to be taken or specify which actions are prohibited.
- **Process:** A set of general tasks and activities to achieve a series of security-related goals. A process should be documented, and can be documented in a Plan, Policy, Procedure, or less formally.
- **Procedure:** An ordered set of steps that need to be followed to accomplish a specific task. It provides the approved way of performing an action in a specific technological and organizational environment.

4.0.2 Security Functions

A considerable array of cybersecurity frameworks exist today which have been promulgated by different governmental agencies and industry organizations [i.1], [i.2] and [i.3]. Such frameworks provide guidance to industry, government agencies, and other organizations to manage cybersecurity risks and offer a taxonomy of high-level cybersecurity outcomes that can be used by any organization to better understand, assess, prioritize, and communicate its cybersecurity efforts. Enumerations of these frameworks with mappings to the controls are available and widely used [i.20].

The NIST CyberSecurity Framework (CSF) is one of the most widely referenced frameworks. Its implementation can be effected using Critical Security Control Safeguards - facilitated through the tagging of individual Safeguards with the six CSF core functions: govern, identify, protect, detect, respond and recover. Those functions are described as follows [i.1]:

- GOVERN - The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader Enterprise Risk Management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

- IDENTIFY - The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g. data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

- PROTECT - Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e. securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

- DETECT - Possible cybersecurity attacks and compromises are found and analysed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.

- RESPOND - Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

- RECOVER - Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

4.0.3 Implementation Groups

IG1. An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office Commercial Off-The-Shelf (COTS) hardware and software.

IG2 (Includes IG1). An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units can have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3 (Includes IG1 and IG2). An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g. risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise needs to address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

4.0.4 Specific action

The specific Controls community defensive action to streamline the process of designing, implementing, measuring, and managing enterprise security for each Safeguard is described.

4.1 Control 1: Inventory and Control of Enterprise Assets

4.1.0 Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Why Is This Control Critical?

Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.

External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to an enterprise's network. Attackers can take advantage of new assets that are installed, yet not securely configured and patched. Internally, unidentified assets can also have weak security configurations that can make them vulnerable to web- or email-based malware and adversaries can leverage weak security configurations for traversing the network, once they are inside.

Additional assets that connect to the enterprise's network (e.g. demonstration systems, temporary test systems, guest networks) should be identified and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. However, attackers have shown the ability, patience, and willingness to "inventory and control" assets at very large scale in order to support their opportunities.

Another challenge is that portable end-user devices will periodically join a network and then disappear, making the inventory of currently available assets very dynamic. Likewise, cloud environments and virtual machines can be difficult to track in asset inventories when they are shut down or paused.

Another benefit of complete enterprise asset management is supporting incident response, both when investigating the origination of network traffic from an asset on the network and when identifying all potentially vulnerable, or impacted, assets of similar type or location during an incident.

Procedures and Tools

This Control includes both technical and procedural actions, united in a process that accounts for, and manages the inventory of, enterprise assets and all associated data throughout its life cycle. It also links to business governance through establishing data/asset owners who are responsible for each component of a business process. Enterprises can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Smaller enterprises can leverage security tools already installed on enterprise assets or used on the network to collect this data. This includes doing a discovery scan of the network with a vulnerability scanner; reviewing anti-malware logs, logs from endpoint security portals, network logs from switches, or authentication logs; and managing the results in a spreadsheet or database.

Maintaining a current and accurate view of enterprise assets is an ongoing and dynamic process. Even for enterprises, there is rarely a single source of truth, as enterprise assets are not always provisioned or installed by the IT department. The reality is that a variety of sources need to be "crowd-sourced" to determine a high-confidence count of enterprise assets. Enterprises can actively scan on a regular basis, sending a variety of different packet types to identify assets connected to the network. In addition to asset sources mentioned above for small enterprises, larger enterprises can collect data from cloud portals and logs from enterprise platforms such as: Active Directory (AD), Single Sign-On (SSO), Multi-Factor Authentication (MFA), Virtual Private Network (VPN), Intrusion Detection Systems (IDSs) or Deep Packet Inspection (DPI), Mobile Device Management (MDM), and vulnerability scanning tools. Property inventory databases, purchase order tracking, and local inventory lists are other sources of data to determine which devices are connected. There are tools and methods that normalize this data to identify devices that are unique among these sources.

Specific guidance is available for the Cloud Data Centre sector [i.9], the mobile communications sector [i.8], Internet of Things sector [i.4], and Industrial Control Systems [i.11].

4.1.1 Establish and maintain detailed enterprise asset inventory

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
1.1	Devices	Identify	•	•	•

Enterprises **should** establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data.

The enterprise asset inventory **should** include end user devices, network devices, non-computing/IoT devices, and servers.

NOTE 1: End user devices include portable and mobile devices.

The enterprise asset inventory **should** record the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network.

NOTE 2: For mobile end-user devices, MDM type tools can support this process, where appropriate.

The enterprise asset inventory **should** include assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments.

The enterprise asset inventory **should** include assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise.

Enterprises **should** review and update the inventory of all enterprise assets bi-annually, or more frequently.

4.1.2 Address unauthorized assets

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
1.2	Devices	Respond	•	•	•

Enterprises **should** ensure that a process exists to address unauthorized assets on a weekly basis.

EXAMPLE: Enterprises can choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

4.1.3 Utilize an active discovery tool

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
1.3	Devices	Detect		•	•

Enterprises **should** utilize an active discovery tool to identify assets connected to the enterprise's network.

Enterprises **should** configure the active discovery tool to execute daily, or more frequently.

4.1.4 Use Dynamic Host Configuration Protocol (DHCP) logging to update enterprise asset inventory

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
1.4	Devices	Identify		•	•

Enterprises **should** use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise asset inventory.

Enterprises **should** review and use DHCP logs to update the enterprise asset inventory weekly, or more frequently.

4.1.5 Use a passive asset discovery tool

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
1.5	Devices	Detect			•

Enterprises **should** use a passive discovery tool to identify assets connected to the enterprise's network.

Enterprises **should** review and use scans to update the enterprise asset inventory at least weekly, or more frequently.

4.2 Control 2: Inventory and Control of Software Assets

4.2.0 Overview

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

Why Is This Control Critical?

A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defences against these attacks is updating and patching software. However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.

Even if a patch is not yet available, a complete software inventory list allows an enterprise to guard against known attacks until the patch is released. Some sophisticated attackers use "zero-day exploits", which take advantage of previously unknown vulnerabilities that have yet to have a patch released from the software vendor. Depending on the severity of the exploit, an enterprise can implement temporary mitigation measures to guard against attacks until the patch is released.

Management of software assets is also important to identify unnecessary security risks. An enterprise should review its software inventory to identify any enterprise assets running software that is not needed for business purposes. For example, an enterprise asset can come installed with default software that creates a potential security risk and provides no benefit to the enterprise. It is critical to inventory, understand, assess, and manage all software connected to an enterprise's infrastructure.

Procedures and Tools

Allowlisting can be implemented using a combination of commercial allowlisting tools, policies, or application execution tools that come with anti-virus suites and popular operating systems. Commercial software and asset inventory tools are widely available and in use in many enterprises today. The best of these tools provides an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the Common Platform Enumeration (CPE) specification.

Features that implement allowlists are included in many modern endpoint security suites and even natively implemented in certain versions of major operating systems. Moreover, commercial solutions are increasingly bundling together anti-virus, anti-spyware, personal firewall, and host-based Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs), along with application performing allow and deny listing. In particular, most endpoint security solutions can look at the name, file system location, and/or cryptographic hash of a given executable to determine whether the application should be allowed to run on the protected machine. The most effective of these tools offer custom allowlists based on executable path, hash, or regular expression matching. Some even include a suspicious list function that allows administrators to define rules for execution of specific programs only by certain users and at certain times of day.

Specific guidance is available for the Cloud Data Centre sector [i.9], the mobile communications sector [i.8], Internet of Things sector [i.4], and Industrial Control Systems [i.11].

4.2.1 Establish and maintain a software inventory

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
2.1	Software	Identify	•	•	•

Enterprises **should** establish and maintain a detailed inventory of all licensed software installed on enterprise assets.

The software inventory **shall** document the title, publisher, initial install/use date, and business purpose for each entry.

Where appropriate, the software inventory **should** include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.

Enterprises **should** review and update the software inventory bi-annually, or more frequently.

4.2.2 Ensure authorized software is currently supported

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
2.2	Software	Identify	•	•	•

Enterprises **should** ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets.

Enterprises **should** document an exception detailing mitigating controls and residual risk acceptance for any software that is unsupported, yet necessary for the fulfilment of the enterprise's mission.

Enterprises **should** designate as unauthorized any unsupported software without a documented exception.

Enterprises **should** review the software inventory to verify software support at least monthly, or more frequently.

4.2.3 Address unauthorized software

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
2.3	Software	Respond	•	•	•

Enterprises **should** ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception.

Enterprises **should** review the software inventory for unauthorized software monthly, or more frequently.

4.2.4 Utilize automated software inventory tools

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
2.4	Software	Detect		•	•

Enterprises **should** utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.

4.2.5 Allowlist authorized software

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
2.5	Software	Protect		•	•

Enterprises **should** use technical controls to ensure that only authorized software can execute or be accessed.

EXAMPLE: This can include application allowlisting,

Enterprises **should** review the technical controls bi-annually, or more frequently.

4.2.6 Allowlist authorized libraries

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
2.6	Software	Protect		•	•

Enterprises **should** use technical controls to ensure that only authorized software libraries are allowed to load into a system process.

NOTE: Software libraries can be specific .dll, .ocx, and .so files.

Enterprises **should** block unauthorized libraries from loading into a system process.

Enterprises **should** review the technical controls bi-annually, or more frequently.

4.2.7 Allowlist authorized scripts

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
2.7	Software	Protect			•

Enterprises **should** use technical controls to ensure that only authorized scripts are allowed to execute.

EXAMPLE: This can include digital signatures and version control.

NOTE: Scripts can be specific .ps1 and .py files.

Enterprises **should** block unauthorized scripts from executing.

Enterprises **should** review the technical controls bi-annually, or more frequently.

4.3 Control 3: Data Protection

4.3.0 Overview

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Why Is This Control Critical?

Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data needs to be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Once attackers have penetrated an enterprise's infrastructure, one of their first tasks is to find and exfiltrate data. Enterprises might not be aware that sensitive data is leaving their environment because they are not monitoring data outflows.

While many attacks occur on the network, others involve physical theft of portable end-user devices, attacks on service providers or other partners holding sensitive data. Other sensitive enterprise assets may also include non-computing devices that provide management and control of physical systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

The enterprise's loss of control over protected or sensitive data is a serious and often reportable business impact. While some data is compromised or lost as a result of theft or espionage, the vast majority are a result of poorly understood data management rules, and user error. The adoption of data encryption, both in transit and at rest, can provide mitigation against data compromise, and, even more important, it is a regulatory requirement for most controlled data.

Procedures and Tools

It is important for an enterprise to develop a data management process that includes a data management framework, data classification guidelines, and requirements for protection, handling, retention, and disposal of data. There should also be a data breach process that plugs into the incident response plan, and the compliance and communication plans. To derive data sensitivity levels, enterprises need to catalogue their key types of data and the overall criticality (impact to its loss or corruption) to the enterprise. This analysis would be used to create an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive", "Confidential" and "Public" and classify their data according to those labels.

Once the sensitivity of the data has been defined, a data inventory or mapping should be developed that identifies software accessing data at various sensitivity levels and the enterprise assets that house those applications. Ideally, the network would be separated so that enterprise assets of the same sensitivity level are on the same network and separated from enterprise assets with different sensitivity levels. If possible, firewalls need to control access to each segment, and have user access rules applied to only allow those with a business need to access the data.

Specific guidance is available for the Cloud Data Centre sector [i.9], the mobile communications sector [i.8]. Additional guidance is available on media security [i.12] and [i.13].

4.3.1 Establish and maintain a data management process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.1	Data	Govern	•	•	•

Enterprises **shall** establish and maintain a documented data management process.

The data management process **should** address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise.

Enterprises **should** review and update the data management process annually, or when significant enterprise changes occur that could impact this Safeguard.

4.3.2 Establish and maintain a data inventory

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.2	Data	Identify	•	•	•

Enterprises **should** establish and maintain a data inventory based on the enterprise's data management process.

The data inventory **should** include sensitive data, at a minimum.

Enterprises **should** review and update the data inventory annually, or more frequently, with a priority on sensitive data.

4.3.3 Configure data access control lists

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.3	Data	Protect	•	•	•

Enterprises **should** configure data access control lists based on a user's need to know.

Enterprises **should** apply data access control lists to local and remote file systems, databases, and applications.

NOTE: Data access control lists are also known as access permissions.

4.3.4 Enforce data retention

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.4	Data	Protect	•	•	•

Enterprises **should** retain data according to the enterprise's documented data management process.

Data retention **shall** include both minimum and maximum timelines pursuant to the enterprise requirements.

4.3.5 Securely dispose of data

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.5	Data	Protect	•	•	•

Enterprises **should** securely dispose of data as outlined in the enterprise's documented data management process.

Enterprises **should** ensure the disposal process and method are commensurate with the data sensitivity.

4.3.6 Encrypt data on end-user devices

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.6	Data	Protect	•	•	•

Enterprises **should** encrypt data on end-user devices containing sensitive data.

4.3.7 Establish and maintain a data classification scheme

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.7	Data	Identify		•	•

Enterprises **should** establish and maintain an overall data classification scheme for the enterprise.

EXAMPLE: Enterprises can use labels, such as "Sensitive", "Confidential" and "Public" and classify their data according to those labels.

Enterprises **should** review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

4.3.8 Document data flows

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.8	Data	Identify		•	•

Enterprises **should** document data flows, including service provider data flows.

The data flow documentation **should** be based on the enterprise's data management process.

Enterprises **should** review and update the data flow documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

4.3.9 Encrypt data on removable media

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.9	Data	Protect		•	•

Enterprises **should** encrypt data on removable media.

4.3.10 Safeguard Encrypt sensitive data in transit

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.10	Data	Protect		•	•

Enterprises **should** encrypt sensitive data in transit.

EXAMPLE: Implementations can include Transport Layer Security (TLS) and Secure Shell (SSH).

4.3.11 Encrypt sensitive data at rest

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.11	Data	Protect		•	•

Enterprises **should** encrypt sensitive data at rest on servers, applications, and databases.

EXAMPLE 1: At a minimum, this can include storage-layer encryption, also known as server-side encryption.

EXAMPLE 2: Additional encryption methods can include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

4.3.12 Segment data processing and storage based on sensitivity

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.12	Data	Protect		•	•

Enterprises **should** segment data processing and storage based on the sensitivity of the data.

Enterprises **should not** process sensitive data on enterprise assets intended for lower sensitivity data.

4.3.13 Deploy a data loss prevention solution

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.13	Data	Protect			•

Enterprises **should** implement an automated tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider.

EXAMPLE: This can include a host-based Data Loss Prevention (DLP) tool.

Enterprises **should** use the automated tool to update the enterprise's data inventory.

4.3.14 Log sensitive data access

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
3.14	Data	Detect			•

Enterprises **should** log sensitive data access, including modification and disposal.

4.4 Control 4: Secure Configuration of Enterprise Assets and Software

4.4.0 Overview

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications.

Why Is This Control Critical?

As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Service providers play a key role in modern infrastructures, especially for smaller enterprises. They often are not set up by default in the most secure configuration to provide flexibility for their customers to apply their own security policies. Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations. These could introduce weaknesses that are under the responsibility of the enterprise that is using the software, rather than the service provider. This extends to ongoing management and updates, as some Platform as a Service (PaaS) only extend to the operating system, so patching and updating hosted applications are under the responsibility of the enterprise.

Even after a strong initial configuration is developed and applied, it needs to be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked" to allow the installation of new software or to support new operational requirements.

Procedures and Tools

There are many available security baselines for each system. Enterprises should start with these publicly developed, vetted, and supported security benchmarks, security guides, or checklists [i.14] and [i.43].

Enterprises should augment or adjust these baselines to satisfy enterprise security policies, and industry and government regulatory requirements. Deviations of standard configurations and rationale should be documented to facilitate future reviews or audits.

For a larger or more complex enterprise, there will be multiple security baseline configurations based on security requirements or classification of the data on the enterprise asset. Here is an example of the steps to build a secure baseline image:

1) Determine the risk classification of the data handled/stored on the enterprise asset (e.g. high, moderate, low risk).

2) Create a security configuration script that sets system security settings to meet the requirements to protect the data used on the enterprise asset. Use benchmarks, such as the ones described earlier in this clause.

3) Install the base operating system software.

4) Apply appropriate operating system and security patches.

5) Install appropriate application software packages, tool, and utilities.

6) Apply appropriate updates to software installed in Step 4.

7) Install local customization scripts to this image.

8) Run the security script created in Step 2 to set the appropriate security level.

9) Run a SCAP compliant tool to record/score the system setting of the baseline image [i.25].

10) Perform a security quality assurance test.

11) Save this base image in a secure location.

Commercial and/or free configuration management tools can be deployed to measure the settings of operating systems and applications of managed machines to look for deviations from the standard image configurations [i.16]. Commercial configuration management tools use some combination of an agent installed on each managed system, or agentless inspection of systems through remotely logging into each enterprise asset using administrator credentials. Additionally, a hybrid approach is sometimes used whereby a remote session is initiated, a temporary or dynamic agent is deployed on the target system for the scan, and then the agent is removed.

4.4.1 Establish and maintain a secure configuration process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.1	Documentation	Govern	•	•	•

Enterprises **shall** establish and maintain a documented secure configuration process for enterprise assets and software.

NOTE 1: Enterprise assets include end-user devices, including portable and mobile; non-computing/IoT devices; and servers.

NOTE 2: Software includes operating systems and applications.

Enterprises **shall** review and update the secure configuration process documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

4.4.2 Establish and maintain a secure configuration process for network infrastructure

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.2	Documentation	Govern	•	•	•

Enterprises **should** establish and maintain a documented secure configuration process for network devices.

Enterprises **should** review and update the secure configuration process documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

4.4.3 Configure automatic session locking on enterprise assets

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.3	Devices	Protect	•	•	•

Enterprises **shall** configure automatic session locking on enterprise assets after a defined period of inactivity.

For general purpose operating systems, the period **shall not** exceed 15 minutes.

For mobile end-user devices, the period **shall not** exceed 2 minutes.

4.4.4 Implement and manage a firewall on servers

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.4	Devices	Protect	•	•	•

Enterprises **should** implement and manage a firewall on servers, where supported.

EXAMPLE: This can be a virtual firewall, operating system firewall, or a third-party firewall agent.

4.4.5 Implement and manage a firewall on end-user devices

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.5	Devices	Protect	•	•	•

Enterprises **should** implement and manage a host-based firewall or port-filtering tool on end-user devices.

The host-based firewall or port-filtering tool **should** include a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

4.4.6 Securely manage enterprise assets and software

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.6	Devices	Protect	•	•	•

Enterprises **should** securely manage enterprise assets and software.

EXAMPLE 1: This can include managing configuration through version-controlled-Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS).

Enterprises **should not** use insecure management protocols unless operationally essential.

EXAMPLE 2: Insecure management protocols include Telnet (Teletype Network) and HTTP.

4.4.7 Manage default accounts on enterprise assets and software

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.7	Users	Protect	•	•	•

Enterprises **should** manage default accounts on enterprise assets and software.

NOTE: Default accounts include root, administrator, and other pre-configured vendor accounts.

EXAMPLE: This can include disabling default accounts or making them unusable.

4.4.8 Uninstall or disable unnecessary services on enterprise assets and software

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.8	Devices	Protect		•	•

Enterprises **should** uninstall or disable unnecessary services on enterprise assets and software.

NOTE: Unnecessary services can include an unused file sharing service, web application module, or service function.

4.4.9 Configure trusted DNS servers on enterprise assets

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.9	Devices	Protect		•	•

Enterprises **should** configure trusted DNS servers on network infrastructure.

EXAMPLE: This can include configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

4.4.10 Enforce automatic device lockout on portable end-user devices

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.10	Devices	Protect		•	•

Enterprises **should** enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported.

For laptops, enterprises **should not** allow more than 20 failed authentication attempts.

For tablets and smartphones, enterprises **should not** allow more than 10 failed authentication attempts.

4.4.11 Enforce remote wipe capability on portable end-user devices

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.11	Data	Protect		•	•

Enterprises **should** remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate.

EXAMPLE: Lost or stolen devices, or when an individual no longer supports the enterprise.

4.4.12 Separate enterprise workspaces on mobile end-user devices

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
4.12	Data	Protect			•

Enterprises **should** ensure separate enterprise workspaces are used on mobile end-user devices, where supported.

4.5 Control 5: Account Management

4.5.0 Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Why Is This Control Critical?

It is easier for an external or internal threat actor to gain unauthorized access to enterprise assets or data through using valid user credentials than through "hacking" the environment. There are many ways to covertly obtain access to user accounts, including: weak passwords, accounts still valid after a user leaves the enterprise, dormant or lingering test accounts, shared accounts that have not been changed in months or years, service accounts embedded in applications for scripts, a user having the same password as one they use for an online account that has been compromised (in a public password dump), social engineering a user to give their password, or using malware to capture passwords or tokens in memory or over the network.

Administrative, or highly privileged, accounts are a particular target, because they allow attackers to add other accounts, or make changes to assets that could make them more vulnerable to other attacks. Service accounts are also sensitive, as they are often shared among teams, internal and external to the enterprise, and sometimes not known about, only to be revealed in standard account management audits.

Finally, account logging and monitoring is a critical component of security operations. While account logging and monitoring are covered in Control 8 (Audit Log Management), it is important in the development of a comprehensive Identity and Access Management (IAM) program.

Procedures and Tools

Accounts also need to be tracked; any account that is dormant needs to be disabled and eventually removed from the system. There should be periodic audits to ensure all active accounts are traced back to authorized users of the enterprise asset. Look for new accounts added since previous review, especially administrator and service accounts. Close attention should be made to identify and track administrative, or high-privileged accounts and service accounts.

Users with administrator or other privileged access should have separate accounts for those higher authority tasks. These accounts would only be used when performing those tasks or accessing especially sensitive data, to reduce risk in case their normal user account is compromised. For users with multiple accounts, their base user account, used day-to-day for non-administrative tasks, should not have any elevated privileges.

Single Sign-On (SSO) is convenient and secure when an enterprise has many applications, including cloud applications, which helps reduce the number of passwords a user needs to manage. Users should use password manager applications to securely store their passwords, and should be instructed not to keep them in spreadsheets or text files on their computers. MFA should be used for remote access.

Users also need to be automatically logged out of the system after a period of inactivity, and be trained to lock their screen when they leave their device to minimize the possibility of someone else in physical proximity around the user accessing their system, applications, or data.

Additional guidance on digital identity and passwords is available [i.17] and [i.18].

4.5.1 Establish and maintain an inventory of accounts

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
5.1	Users	Identify	•	•	•

Enterprises **shall** establish and maintain an inventory of all accounts managed in the enterprise.

The account inventory **shall** at a minimum include user, administrator and service accounts.

The account inventory, at a minimum, **should** contain the person's name, username, start/stop dates, and department.

Enterprises **should** validate that all active accounts are authorized, on a recurring schedule quarterly, or more frequently.

4.5.2 Use unique passwords

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
5.2	Users	Protect	•	•	•

Enterprises **should** use unique passwords for all enterprise assets.

NOTE: Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.

4.5.3 Disable dormant accounts

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
5.3	Users	Protect	•	•	•

Enterprises **shall** delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.

4.5.4 Restrict administrator privileges to dedicated administrator accounts

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
5.4	Users	Protect	•	•	•

Enterprises **should** restrict administrator privileges to dedicated administrator accounts on enterprise assets.

Users **should** conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

4.5.5 Establish and maintain an inventory of service accounts

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
5.5	Users	Identify		•	•

Enterprises **should** establish and maintain an inventory of service accounts.

The service account inventory, at a minimum, **shall** contain department owner, review date, and purpose.

Enterprises **should** perform service account reviews to validate that all active accounts are authorized, on a recurring schedule quarterly, or more frequently.

4.5.6 Centralize account management

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
5.6	Users	Govern		•	•

Enterprises **should** centralize account management through a directory or identity service.

4.6 Control 6: Access Control Management

4.6.0 Overview

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Why Is This Control Critical?

Where Control 5 deals specifically with account management, Control 6 focuses on managing what access these accounts have, ensuring users only have access to the data or enterprise assets appropriate for their role, and ensuring that there is strong authentication for critical or sensitive enterprise data or functions. Accounts should only have the minimal authorization needed for the role. Developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

There are some user activities that pose greater risk to an enterprise, either because they are accessed from untrusted networks, or performing administrator functions that allow the ability to add, change, or remove other accounts, or make configuration changes to operating systems or applications to make them less secure. This also enforces the importance of using MFA and Privileged Access Management (PAM) tools.

Some users have access to enterprise assets or data they do not need for their role; this might be due to an immature process that gives all users all access, or lingering access as users change roles within the enterprise over time. Local administrator privileges to users' laptops are also an issue, as any malicious code installed or downloaded by the user can have greater impact on the enterprise asset running as administrator. User, administrator, and service account access should be based on enterprise role and need.

Procedures and Tools

There should be a process where privileges are granted and revoked for user accounts. This ideally is based on enterprise role and need through role-based access. Role-based access is a technique to define and manage access requirements for each account based on: need to know, least privilege, privacy requirements, and/or separation of duties. There are technology tools to help manage this process. However, there might be more granular or temporary access based on circumstance.

MFA should be universal for all privileged or administrator accounts. There are many tools that have smartphone applications to perform this function, and are easy to deploy. Using the number-generator feature is more secure than just sending a Short Messaging Service (SMS) message with a one-time code, or prompting a "push" alert for a user to accept. However, neither is recommended for privileged account MFA. PAM tools are available for privileged account control, and provide a one-time password that needs to be checked out for each use. For additional security in system administration, "jump-boxes" or out of band terminal connections should be used.

Comprehensive account de-provisioning is important. Many enterprises have repeatable consistent processes for removing access when employees leave the enterprise. However, that process is not always consistent for contractors, and needs to be included in the standard de-provisioning process. Enterprises should also inventory and track service accounts, as a common error is leaving clear text tokens or passwords in code, and posting to public cloud-based code repositories.

High-privileged accounts should not be used for day-to-day use, such as web surfing and email reading. Administrators should have separate accounts that do not have elevated privileges for daily office use, and should log into administrator accounts only when performing administrator functions requiring that level of authorization. Security personnel should periodically gather a list of running processes to determine whether any browsers or email readers are running with high privileges.

Additional guidance on digital identity is available [i.17].

4.6.1 Establish an access granting process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
6.1	Documentation	Govern	•	•	•

Enterprises **should** establish and follow a process for granting access to enterprise assets upon new hire or role change of a user.

NOTE: An automated process is preferred.

4.6.2 Establish an access revoking process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
6.2	Documentation	Govern	•	•	•

Enterprises **shall** establish and follow a process, preferably automated, for revoking access to enterprise assets.

NOTE 1: An automated process is preferred.

Accounts **should** be disabled immediately upon termination, rights revocation, or role change of a user.

NOTE 2: Disabling accounts, instead of deleting accounts, might be necessary to preserve audit trails.

4.6.3 Implement MFA for externally-exposed applications

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
6.3	Users	Protect	•	•	•

Enterprises **should** configure all externally-exposed enterprise or third-party applications to enforce MFA, where supported.

EXAMPLE: Enterprises can enforce MFA through a directory service or SSO provider.

4.6.4 Implement MFA for remote network access

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
6.4	Users	Protect	•	•	•

Enterprises **should** implement MFA for remote network access.

4.6.5 Implement MFA for administrative access

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
6.5	Users	Protect	•	•	•

Enterprises **should** implement MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.

4.6.6 Establish and maintain an inventory of authentication and authorization systems

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
6.6	Software	Identify		•	•

Enterprises **should** establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider.

Enterprises **should** review and update the inventory of authentication and authorization systems, annually, or more frequently.

4.6.7 Centralize access control

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
6.7	Users	Protect		•	•

Enterprises **should** centralize access control for all enterprise assets through a directory service or SSO provider, where supported.

4.6.8 Define and maintain role-based access control

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
6.8	Users	Govern			•

Enterprises **should** define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties.

Enterprises **should** perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule annually, or more frequently.

4.7 Control 7: Continuous Vulnerability Management

4.7.0 Overview

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Why Is This Control Critical?

Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders need to have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate. While there is a gap in time from a vulnerability being known to when it is patched, defenders can prioritize which vulnerabilities are most impactful to the enterprise, or likely to be exploited first due to ease of use. For example, when researchers or the community report new vulnerabilities, vendors develop and deploy patches, Indicators Of Compromise (IOCs), and updates. Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches, and install the patch.

There is never perfection in this process. Attackers might be using an exploit to a vulnerability that is not known within the security community. They might have developed an exploit to this vulnerability referred to as a "zero-day" exploit. Once the vulnerability is known in the community, the process mentioned above starts. Therefore, defenders need to keep in mind that an exploit might already exist when the vulnerability is widely socialized. Sometimes vulnerabilities might be known within a closed community (e.g. vendor still developing a fix) for weeks, months, or years before it is disclosed publicly. Defenders have to be aware that there might always be vulnerabilities they cannot remediate, and therefore need to use other controls to mitigate.

Enterprises that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their enterprise assets compromised. Defenders face particular challenges in scaling remediation across an entire enterprise, and prioritizing actions with conflicting priorities, while not impacting the enterprise's business or mission.

Procedures and Tools

A large number of vulnerability scanning tools are available to evaluate the security configuration of enterprise assets. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities across an enterprise, it is preferable to use vulnerability scanning tools that map vulnerabilities to one or more of the following industry-recognized vulnerability, configuration and platform classification schemes and languages, such as Common Vulnerabilities and Exposures (CVE®) [i.19], Common Configuration Enumeration (CCE) [i.20], Open Vulnerability and Assessment Language (OVAL®) [i.21], Common Platform Enumeration (CPE) [i.22], Common Vulnerability Scoring System (CVSS) [i.23], and/or Extensible Configuration Checklist Description Format (XCCDF) [i.24] using the Security Content Automation Protocol (SCAP) [i.25].

The frequency of scanning activities should increase as the diversity of an enterprise's assets increases to account for the varying patch cycles of each vendor. Advanced vulnerability scanning tools can be configured with user credentials to authenticate into enterprise assets and perform more comprehensive assessments. These are called "authenticated scans".

In addition to the scanning tools that check for vulnerabilities and misconfigurations across the network, various free and commercial tools can evaluate security settings and configurations of enterprise assets. Such tools can provide fine-grained insight into unauthorized changes in configuration or the inadvertent introduction of security weaknesses from administrators.

Effective enterprises link their vulnerability scanners with problem-ticketing systems that track and report progress on fixing vulnerabilities. This can help highlight unmitigated critical vulnerabilities to senior management to ensure they are resolved. Enterprises can also track how long it took to remediate a vulnerability, after identified, or a patch has been issued. These can support internal or industry compliance requirements. Some mature enterprises will go over these reports in IT security steering committee meetings, which bring leaders from IT and the business together to prioritize remediation efforts based on business impact.

In selecting which vulnerabilities to fix, or patches to apply, an enterprise should augment Forum of Incident Response and Security Teams, Inc.'s (FIRST) CVSS [i.23] with data concerning the likelihood of a threat actor using a vulnerability, or potential impact of an exploit to the enterprise. Information on the likelihood of exploitation should also be periodically updated based on the most current threat information. For example, the release of a new exploit, or new intelligence relating to exploitation of the vulnerability, should change the priority through which the vulnerability should be considered for patching. Various commercial systems are available to allow an enterprise to automate and maintain this process in a scalable manner.

The most effective vulnerability scanning tools compare the results of the current scan with previous scans to determine how the vulnerabilities in the environment have changed over time. Security personnel use these features to conduct vulnerability trending from month to month.

Finally, there should be a quality assurance process to verify configuration updates, or that patches are implemented correctly and across all relevant enterprise assets.

Additional guidance on structured threat information sharing is available [i.40].

4.7.1 Establish and maintain a vulnerability management process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
7.1	Documentation	Govern	•	•	•

Enterprises **should** establish and maintain a documented vulnerability management process for enterprise assets.

Enterprises **should** review and update the vulnerability management process annually, or when significant enterprise changes occur that could impact this Safeguard.

4.7.2 Establish and maintain a remediation process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
7.2	Documentation	Govern	•	•	•

Enterprises **should** establish and maintain a risk-based remediation strategy documented in a remediation process.

Enterprises **should** review the remediation process monthly, or more frequently.

4.7.3 Perform automated operating system patch management

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
7.3	Software	Protect	•	•	•

Enterprises **should** perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

4.7.4 Perform automated application patch management

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
7.4	Software	Protect	•	•	•

Enterprises **should** perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

4.7.5 Perform automated vulnerability scans of internal enterprise assets

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
7.5	Software	Identify		•	•

Enterprises **should** perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis.

Enterprises **should** conduct both authenticated and unauthenticated scans.

4.7.6 Perform automated vulnerability scans of externally-exposed enterprise assets

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
7.6	Software	Identify		•	•

Enterprises **should** perform automated vulnerability scans of externally-exposed enterprise assets on a monthly, or more frequent, basis.

4.7.7 Remediate detected vulnerabilities

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
7.7	Software	Respond		•	•

Enterprises **should** remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

4.8 Control 8: Audit Log Management

4.8.0 Overview

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Why Is This Control Critical?

Log collection and analysis is critical for an enterprise's ability to detect malicious activity quickly. Sometimes audit records are the only evidence of a successful attack. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyse them. Attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or non-existent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing.

There are two types of logs that are generally treated and often configured independently: system logs and audit logs. System logs typically provide system-level events that show various system process start/end times, crashes, etc. These are native to systems, and take less configuration to turn on. Audit logs typically include user-level events - when a user logged in, accessed a file, etc. - and take more planning and effort to set up.

Logging records are also critical for incident response. After an attack has been detected, log analysis can help enterprises understand the extent of an attack. Complete logging records can show, for example, when and how the attack occurred, what information was accessed, and if data was exfiltrated. Retention of logs is also critical in case a follow-up investigation is required or if an attack remained undetected for a long period of time.

Procedures and Tools

Most enterprise assets and software offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (Virtual Private Network (VPN), dial-up, etc.) should all be configured for verbose logging where beneficial. Retention of logging data is also important in the event an incident investigation is required.

Furthermore, all enterprise assets should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an enterprise should periodically scan through its logs and compare them with the enterprise asset inventory assembled as part of Control 1, in order to ensure that each managed asset actively connected to the network is periodically generating logs.

4.8.1 Establish and maintain an audit log management process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.1	Documentation	Govern	•	•	•

Enterprises **should** establish and maintain a documented audit log management process that defines the enterprise's logging requirements.

The audit log management process **should**, at a minimum, address the collection, review, and retention of audit logs for enterprise assets.

Enterprises **should** review and update the audit log management process annually, or when significant enterprise changes occur that could impact this Safeguard.

4.8.2 Collect audit logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.2	Data	Detect	•	•	•

Enterprises **should** collect audit logs.

Enterprises **should** ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.

4.8.3 Ensure adequate audit log storage

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.3	Data	Protect	•	•	•

Enterprises **should** ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

4.8.4 Standardize time synchronization

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.4	Data	Protect		•	•

Enterprises **should** standardize time synchronization.

Enterprises **should** configure at least two synchronized time sources across enterprise assets, where supported.

4.8.5 Collect detailed audit logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.5	Data	Detect		•	•

Enterprises **should** configure detailed audit logging for enterprise assets containing sensitive data.

EXAMPLE: This can include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.

4.8.6 Collect DNS query audit logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.6	Data	Detect		•	•

Enterprises **should** collect DNS query audit logs on enterprise assets, where appropriate and supported.

4.8.7 Collect URL request audit logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.7	Data	Detect		•	•

Enterprises **should** collect URL request audit logs on enterprise assets, where appropriate and supported.

4.8.8 Collect command-line audit logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.8	Data	Detect		•	•

Enterprises **should** collect command-line audit logs.

EXAMPLE: This can include collecting audit logs from PowerShell, BASH, and remote administrative terminals.

4.8.9 Centralize audit logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.9	Data	Detect		•	•

Enterprises **should** centralize, to the extent possible, audit log collection and retention across enterprise assets in accordance with the documented audit log management process.

EXAMPLE: This can include leveraging a SIEM tool to centralize multiple log sources.

4.8.10 Retain audit logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.10	Data	Protect		•	•

Enterprises **should** retain audit logs across enterprise assets for a minimum of 90 days.

4.8.11 Conduct audit log reviews

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.11	Data	Detect		•	•

Enterprises **should** conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat.

Enterprises **should** conduct audit log reviews on a weekly, or more frequent, basis.

4.8.12 Collect service provider logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
8.12	Data	Detect			•

Enterprises **should** collect service provider logs, where supported.

EXAMPLE: This can include collecting authentication and authorization events, data creation and disposal events, and user management events.

4.9 Control 9: Email and Web Browser Protections

4.9.0 Overview

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.

Why Is This Control Critical?

Web browsers and email clients are very common points of entry for attackers because of their direct interaction with users inside an enterprise. Content can be crafted to entice or spoof users into disclosing credentials, providing sensitive data, or providing an open channel to allow attackers to gain access, thus increasing risk to the enterprise. Since email and web are the main means that users interact with external and untrusted users and environments, these are prime targets for both malicious code and social engineering. Additionally, as enterprises move to web-based email, or mobile email access, users no longer use traditional full-featured email clients, which provide embedded security controls like connection encryption, strong authentication, and phishing reporting buttons.

Web Browser

Cybercriminals can exploit web browsers in multiple ways. If they have access to exploits of vulnerable browsers, they can craft malicious webpages that can exploit those vulnerabilities when browsed with an insecure, or unpatched, browser. Alternatively, they can try to target any number of common web browser third-party plugins that may allow them to hook into the browser or even directly into the operating system or application. These plugins, much like any other software within an environment, need to be reviewed for vulnerabilities, kept up-to-date with latest patches or versions, and controlled. Many come from untrusted sources, and some are even written to be malicious. Therefore, it is best to prevent users from intentionally or unintentionally installing malware that might be hiding in some of these plugins, extensions, and add-ons. Simple configuration updates to the browser can make it much harder for malware to get installed through reducing the ability of installing add-ons/plugins/extensions and preventing specific types of content from automatically executing.

Most popular browsers employ a database of phishing and/or malware sites to protect against the most common threats. A best practice is to enable these content filters and turn on the pop-up blockers. Pop-ups are not only annoying; they can also host embedded malware directly or lure users into clicking links using social engineering tricks. To help enforce blocking of known malicious domains, also consider subscribing to DNS filtering services to block attempts to access these websites at the network level.

Email

Email represents one the most interactive ways humans work with enterprise assets; training and encouraging the right behaviour is just as important as the technical settings. Email is the most common threat vector against enterprises through tactics such as phishing and Business Email Compromise (BEC).

Using a spam-filtering tool and malware scanning at the email gateway reduces the number of malicious emails and attachments that come into the enterprise's network. Initiating Domain-based Message Authentication, Reporting and Conformance (DMARC) helps reduce spam and phishing activities. Installing an encryption tool to secure email and communications adds another layer of user and network-based security. In addition to blocking based on the sender, it is also worthwhile to only allow certain file types that users need for their jobs. This will require coordination with different business units to understand what types of files they receive via email to ensure that there is not an interruption to their processes.

Since phishing email techniques are ever evolving to get past Something Posing as Mail (SPAM) filter rules, it is important to train users on how to identify phishing, and to notify IT Security when they see one. There are many platforms that perform phishing tests against users to help educate them on different examples, and track their improvement over time. Crowd-sourcing this knowledge into notifying IT Security teams of phishing helps improve the protections and detections of email-based threats.

4.9.1 Ensure use of only fully supported browsers and email clients

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
9.1	Software	Protect	•	•	•

Enterprises **should** ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.

4.9.2 Use DNS filtering services

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
9,2	Devices	Protect	•	•	•

Enterprises **should** use DNS filtering services on all end user devices, including remote and on-enterprise assets, to block access to known malicious domains.

4.9.3 Maintain and enforce network-based URL filters

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
9.3	Network	Protect		•	•

Enterprises **should** enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites.

EXAMPLE: This can include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

4.9.4 Restrict unnecessary or unauthorized browser and email client extensions

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
9.4	Software	Protect		•	•

Enterprises **should** restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

4.9.5 Implement DMARC

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
9.5	Network	Protect		•	•

Enterprises **should** implement DMARC policy and verification to lower the chance of spoofed or modified emails from valid domains.

EXAMPLE: At a minimum, this includes implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

4.9.6 Block unnecessary file types

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
9.6	Network	Protect		•	•

Enterprises **should** block unnecessary file types attempting to enter the enterprise's email gateway.

4.9.7 Deploy and maintain email server anti-malware protections

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
9.7	Network	Protect			•

Enterprises **should** deploy and maintain email server anti malware protections.

EXAMPLE: This can include attachment scanning and/or sandboxing.

4.10 Control 10: Malware Defences

4.10.0 Overview

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Why Is This Control Critical?

Malicious software (sometimes categorized as viruses or Trojans) is an integral and dangerous aspect of internet threats. They can have many purposes, from capturing credentials, stealing data, identifying other targets within the network, and encrypting or destroying data. Malware is ever-evolving and adaptive, as modern variants leverage machine learning techniques.

Malware enters an enterprise through vulnerabilities within the enterprise on end-user devices, email attachments, webpages, cloud services, mobile devices, and removable media. Malware often relies on insecure end-user behaviour, such as clicking links, opening attachments, installing software or profiles, or inserting Universal Serial Bus (USB) flash drives. Modern malware is designed to avoid, deceive, or disable defences.

Malware defences need to be able to operate in this dynamic environment through automation, timely and rapid updating, and integration with other processes like vulnerability management and incident response. They need to be deployed at all possible entry points and enterprise assets to detect, prevent spread, or control the execution of malicious software or code.

Procedures and Tools

Effective malware protection includes traditional endpoint malware prevention and detection suites. To ensure malware IOCs are up-to-date, enterprises can receive automated updates from the vendor to enrich other vulnerability or threat data. These tools are best managed centrally to provide consistency across the infrastructure.

Being able to block or identify malware is only part of this Control; there is also a focus on centrally collecting the logs to support alerting, identification, and incident response. As malicious actors continue to develop their methodologies, many are starting to take a "Living off the-Land" (LotL) approach to minimize the likelihood of being caught [i.26]. This approach refers to attacker behaviour that uses tools or features that already exist in the target environment. Enabling logging, as per the Safeguards in Control 8, will make it significantly easier for the enterprise to follow the events to understand what happened and why it happened.

4.10.1 Deploy and maintain anti-malware software

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
10.1	Devices	Detect	•	•	•

Enterprises **shall** deploy and maintain anti malware software on all enterprise assets.

4.10.2 Configure automatic anti-malware signature updates

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
10.2	Devices	Protect	•	•	•

Enterprises **shall** configure automatic updates for anti-malware signature files on all enterprise assets.

4.10.3 Disable autorun and autoplay for removable media

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
10.3	Devices	Protect	•	•	•

Enterprises **should** disable autorun and autoplay auto-execute functionality for removable media.

4.10.4 Configure automatic anti-malware scanning of removable media

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
10.4	Devices	Detect		•	•

Enterprises **should** configure anti-malware software to automatically scan removable media.

4.10.5 Enable anti-exploitation features

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
10.5	Devices	Protect		•	•

Enterprises **should** enable anti-exploitation features on enterprise assets and software.

EXAMPLE: This can include DEP, WDEG SIP or Gatekeeper where possible.

4.10.6 Centrally manage anti-malware software

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
10.6	Devices	Protect		•	•

Enterprises **should** centrally manage anti-malware software.

4.10.7 Use behaviour-based anti-malware software

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
10.7	Devices	Detect		•	•

Enterprises **should** use behaviour-based anti-malware software.

4.11 Control 11: Data Recovery

4.11.0 Overview

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Why Is This Control Critical?

In the cybersecurity triad - Confidentiality, Integrity and Availability (CIA) - the availability of data is, in some cases, more critical than its confidentiality. Enterprises need many types of data to make business decisions, and when that data is not available or is untrusted, then it could impact the enterprise. An easy example is weather information to a transportation enterprise.

When attackers compromise assets, they make changes to configurations, add accounts, and often add software or scripts. These changes are not always easy to identify, as attackers might have corrupted or replaced trusted applications with malicious versions, or the changes might appear to be standard-looking account names. Configuration changes can include adding or changing registry entries, opening ports, turning off security services, deleting logs, or other malicious actions that make a system insecure. These actions do not have to be malicious; human error can cause each of these as well. Therefore, it is important to have an ability to have recent backups or mirrors to recover enterprise assets and data back to a known trusted state.

There has been an exponential rise in ransomware over the last few years. It is not a new threat, though it has become more commercialized and organized as a reliable method for attackers to make money. If an attacker encrypts an enterprise's data and demands ransom for its restoration, having a recent backup to recover to a known, trusted state can be helpful. However, as ransomware has evolved, it has also become an extortion technique, where data is exfiltrated before being encrypted, and the attacker asks for payment to restore the enterprise's data, as well as to keep it from being sold or publicized. In this case, restoration would only solve the issue of restoring systems to a trusted state and continuing operations. Leveraging the guidance within the CSC will help reduce the risk of ransomware through improved cyber hygiene, as attackers usually use older or basic exploits on insecure systems.

Procedures and Tools

Data recovery procedures should be defined in the data management process described in Control 3, Data Protection. This should include backup procedures based on data value, sensitivity, or retention requirements. This will assist in developing backup frequency and type (full vs. incremental).

Once per quarter (or whenever a new backup process or technology is introduced), a testing team should evaluate a random sampling of backups and attempt to restore them on a test bed environment. The restored backups should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

4.11.1 Establish and maintain a data recovery process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
11.1	Documentation	Govern	•	•	•

Enterprises **should** establish and maintain a documented data recovery process.

The data recovery process **should** address the scope of data recovery activities, recovery prioritization, and the security of backup data.

Enterprises **should** review and update the data recovery process annually, or when significant enterprise changes occur that could impact this Safeguard.

4.11.2 Perform automated backups

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
11.2	Data	Recover	•	•	•

Enterprises **should** perform automated backups of in-scope enterprise assets.

Enterprises **should** run backups weekly, or more frequently, based on the sensitivity of the data.

4.11.3 Protect recovery data

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
11.3	Data	Protect	•	•	•

Enterprises **should** protect recovery data with equivalent controls to the original data.

EXAMPLE: This includes reference encryption or data separation, based on requirements.

4.11.4 Establish and maintain an isolated instance of recovery data

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
11.4	Data	Recover	•	•	•

Enterprises **should** establish and maintain an isolated instance of recovery data.

EXAMPLE: This can include version controlling backup destinations through offline, cloud, or off-site systems or services.

4.11.5 Test data recovery

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
11.5	Data	Recover		•	•

Enterprises **should** test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.

4.12 Control 12: Network Infrastructure Management

4.12.0 Overview

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Why Is This Control Critical?

Secure network infrastructure is an essential defence against attacks. This includes an appropriate security architecture, addressing vulnerabilities that are, often times, introduced with default settings, monitoring for changes, and reassessment of current configurations. Network infrastructure includes devices such as physical and virtualized gateways, firewalls, wireless access points, routers, and switches. Default configurations for network devices are geared for ease-of-deployment and ease-of-use - not security. Potential default vulnerabilities include open services and ports, default accounts and passwords (including service accounts), support for older vulnerable protocols, and pre-installation of unneeded software. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defences. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept data while in transmission.

Network security is a constantly changing environment that necessitates regular re-evaluation of architecture diagrams, configurations, access controls, and allowed traffic flows. Attackers take advantage of network device configurations becoming less secure over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed, but not removed when they are no longer applicable to the business's needs. In some cases, the security risk of an exception is neither properly analysed nor measured against the associated business need and can change over time.

Procedures and Tools

Enterprises should ensure network infrastructure is fully documented and architecture diagrams are kept up-to-date. It is important for key infrastructure components to have vendor support for patches and feature upgrades. Upgrade End-Of-Life (EOL) components before the date they will be out of support or apply mitigating controls to isolate them. Enterprises need to monitor their infrastructure versions and configurations for vulnerabilities that would require them to upgrade the network devices to the latest secure and stable version that does not impact the infrastructure.

An up-to-date network architecture diagram, including security architecture diagrams, are an important foundation for infrastructure management. Next is having complete account management for access control, logging, and monitoring. Finally, infrastructure administration should only be performed over secure protocols, with strong authentication (MFA for PAM), and from dedicated administrative devices or out-of-band networks.

Commercial tools can be helpful to evaluate the rule sets of network filtering devices to determine whether they are consistent or in conflict. This provides an automated sanity check of network filters. These tools search for errors in rule sets or Access Controls Lists (ACLs) that may allow unintended services through the network device. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.

Additional guidance for telework and small office networks is available [i.27].

4.12.1 Ensure network infrastructure is up-to-date

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
12.1	Network	Protect	•	•	•

Enterprises **should** ensure network infrastructure is kept up-to-date.

EXAMPLE: This can include running the latest stable release of software and/or using currently supported Network as a Service (NaaS) offerings.

Enterprises **should** review software versions monthly, or more frequently, to verify software support.

4.12.2 Establish and maintain a secure network architecture

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
12.2	Network	Protect		•	•

Enterprises **should** establish and maintain a secure network architecture.

The secure network architecture **shall** address segmentation, least privilege, and availability, at a minimum.

NOTE: This will not solely include documentation, but also policy and design components.

4.12.3 Securely manage network infrastructure

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
12.3	Network	Protect		•	•

Enterprises **should** securely manage network infrastructure.

EXAMPLE: This can include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.

4.12.4 Establish and maintain architecture diagram(s)

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
12.4	Documentation	Govern		•	•

Enterprises **should** establish and maintain architecture diagram(s) and/or other network system documentation.

Enterprises **should** review and update the network system documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

4.12.5 Centralize network Authentication, Authorization, and Auditing (AAA)

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
12.5	Network	Protect		•	•

Enterprises **should** centralize network AAA.

4.12.6 Use of secure network management and communication protocols

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
12.6	Network	Protect		•	•

Enterprises **should** use secure network management and communication protocols.

EXAMPLE: This can include IEEE 802.1X™-2010 [i.42] Wi-Fi® Protected Access 2 (WPA2) Enterprise or greater.

4.12.7 Ensure remote devices utilize a VPN and are connecting to an enterprise's AAA infrastructure

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
12.7	Devices	Protect		•	•

Enterprises **should** require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end user devices.

4.12.8 Establish and maintain dedicated computing resources for all administrative work

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
12.8	Devices	Protect			•

Enterprises **should** establish and maintain dedicated computing resources for all administrative tasks or tasks requiring administrative access.

NOTE: The computing resources can either physically or logically separated.

The computing resources **should** be segmented from the enterprise's primary network and not be allowed internet access.

4.13 Control 13: Network Monitoring and Defence

4.13.0 Overview

Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.

Why Is This Control Critical?

Network defences are not perfect. Adversaries continue to evolve and mature, as they share, or sell, information among their community on exploits and bypasses to security controls. Even if security tools work "as advertised", it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective. Often, misconfigurations due to human error or lack of knowledge of tool capabilities give enterprises a false sense of security.

Security tools can only be effective if they are supporting a process of continuous monitoring that allows staff the ability to be alerted and respond to security incidents quickly. Enterprises that adopt a purely technology-driven approach will also experience more false positives, due to their over-reliance on alerts from tools. Identifying and responding to these threats requires visibility into all threat vectors of the infrastructure and leveraging humans in the process of detection, analysis, and response. It is critical for large or heavily targeted enterprises to have a security operations capability to prevent, detect, and quickly respond to cyber threats before they can impact the enterprise. This process will generate activity reports and metrics that will help enhance security policies, and support regulatory compliance for many enterprises.

As has been seen many times in the press, enterprises have been compromised for weeks, months, or years before discovery. The primary benefit of having comprehensive situational awareness is to increase the speed of detection and response. This is critical to respond quickly when malware is discovered, credentials are stolen, or when sensitive data is compromised to reduce impact to the enterprise.

Through good situational awareness (i.e. security operations), enterprises will identify and catalogue Tactics, Techniques and Procedures (TTPs) of attackers, including their IOCs that will help the enterprise become more proactive in identifying future threats or incidents. Recovery can be achieved faster when the response has access to complete information about the environment and enterprise structure to develop efficient response strategies.

Procedures and Tools

Most enterprises do not need to stand up a Security Operations Centre (SOC) to gain situational awareness. This starts with first understanding critical business functions, network and server architectures, data and data flows, vendor service and business partner connection, and end-user devices and accounts. This informs the development of a security architecture, technical controls, logging, monitoring, and response procedures.

At the core of this process is a trained and organized team that implements processes for incident detection, analysis, and mitigation. These capabilities could be conducted internally, or through consultants or a managed service provider. Enterprises should consider network, enterprise asset, user credential, and data access activities. Technology will play a crucial role to collect and analyse all of the data, and monitor networks and enterprise assets internally and externally to the enterprise. Enterprises should include visibility to cloud platforms that might not be in line with on-premises security technology.

Forwarding all important logs to analytical programs, such as Security Information and Event Management (SIEM) solutions, can provide value; however, they do not provide a complete picture. Weekly log reviews are necessary to tune thresholds and identify abnormal events. Correlation tools can make audit logs more useful for subsequent manual inspection. These tools are not a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

As this process matures, enterprises will create, maintain, and evolve a knowledge base that will help to understand and assess the business risks, developing an internal threat intelligence capability. Threat intelligence is the collection of TTPs from incidents and adversaries. To accomplish this, a situational awareness program will define and evaluate which information sources are relevant to detect, report, and handle attacks. Most mature enterprises can evolve to threat hunting, where trained staff manually review system and user logs, data flows, and traffic patterns to find anomalies.

4.13.1 Centralize security event alerting

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.1	Network	Detect		•	•

Enterprises **should** centralize security event alerting across enterprise assets for log correlation and analysis.

EXAMPLE 1: Best practice implementation implies the use of a SIEM, which includes vendor-defined event correlation alerts.

EXAMPLE 2: A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

4.13.2 Deploy a host-based intrusion detection solution

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.2	Devices	Detect		•	•

Enterprises **should** deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

4.13.3 Deploy a network intrusion detection solution

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.3	Network	Detect		•	•

Enterprises **should** deploy a network intrusion detection solution on enterprise assets, where appropriate.

EXAMPLE: This can include the use of a Network Intrusion Detection System (NIDS) or equivalent Cloud Service Provider (CSP) service.

4.13.4 Perform traffic filtering between network segments

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.4	Network	Protect		•	•

Enterprises **should** perform traffic filtering between network segments, where appropriate.

4.13.5 Manage access control for remote assets

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.5	Devices	Protect		•	•

Enterprises **should** manage access control for assets remotely connecting to enterprise resources.

Enterprises **should** determine the amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

4.13.6 Collect network traffic flow logs

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.6	Network	Detect		•	•

Enterprises **should** collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

4.13.7 Deploy a host-based intrusion prevention solution

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.7	Devices	Protect			•

Enterprises **should** deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported.

EXAMPLE: This can include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

4.13.8 Deploy a network intrusion prevention solution

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.8	Network	Protect			•

Enterprises **should** deploy a network intrusion prevention solution, where appropriate.

EXAMPLE: This can include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

4.13.9 Deploy port-level access control

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.9	Network	Protect			•

Enterprises **should** deploy port-level access control.

NOTE: Port-level access control utilizes IEEE 802.1X™-2010 [i.2], or similar network access control protocols, such as certificates, and can incorporate user and/or device authentication.

4.13.10 Perform application layer filtering

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.10	Network	Protect			•

Enterprises **should** perform application layer filtering.

EXAMPLE: This can include a filtering proxy, application layer firewall, or gateway.

4.13.11 Tune security event alerting thresholds

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
13.11	Network	Detect			•

Enterprises **should** tune security event alerting thresholds monthly, or more frequently.

4.14 Control 14: Security Awareness and Skills Training

4.14.0 Overview

Establish and maintain a security awareness program to influence behaviour among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Why Is This Control Critical?

The actions of people play a critical part in the success or failure of an enterprise's security program. It is easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise, than to find a network exploit to do it directly.

Users themselves, both intentionally and unintentionally, can cause incidents as a result of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password they use on public sites.

No security program can effectively address cyber risk without a means to address this fundamental human vulnerability. Users at every level of the enterprise have different risks. For example: executives manage more sensitive data; system administrators have the ability to control access to systems and applications; and users in finance, human resources, and contracts all have access to different types of sensitive data that can make them targets.

The training should be updated regularly. This will increase the culture of security and discourage risky workarounds.

Procedures and Tools

An effective security awareness training program should not just be a canned, once-a-year training video coupled with regular phishing testing. While annual training is needed, there should also be more frequent, topical messages and notifications about security. This might include messages about: strong password-use that coincides with a media report of password dump, the rise of phishing during tax time, or increased awareness of malicious package delivery emails during the holidays.

Training should also consider the enterprise's different regulatory and threat posture. Financial firms might have more compliance-related training on data handling and use, healthcare enterprises on handling healthcare data, and merchants for credit card data.

Social engineering training, such as phishing tests, should also include awareness of tactics that target different roles. For example, the financial team will receive BEC attempts posing as executives asking to wire money, or receive emails from compromised partners or vendors asking to change the bank account information for their next payment. A variety of resources are available for building an effective security awareness programme [i.27], [i.28], [i.29], [i.30], [i.31], [i.32], [i.40] and [i.41].

4.14.1 Establish and maintain a security awareness program

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.1	Documentation	Govern	•	•	•

Enterprises **should** establish and maintain a security awareness program.

NOTE: The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner.

Enterprises **should** conduct training at hire and, at a minimum, annually.

Enterprises **should** review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.

4.14.2 Train workforce members to recognize social engineering attacks

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.2	Users	Protect	•	•	•

Enterprises **should** train workforce members to recognize social engineering attacks.

EXAMPLE: Topics can include phishing, Business Email Compromise (BEC), pre-texting, and tailgating.

4.14.3 Train workforce members on authentication best practices

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.3	Users	Protect	•	•	•

Enterprises **should** train workforce members on authentication best practices.

EXAMPLE: Topics can include MFA, password composition, and credential management.

4.14.4 Train workforce on data handling best practices

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.4	Users	Protect	•	•	•

Enterprises **should** train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data.

NOTE: This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.

4.14.5 Train workforce members on causes of unintentional data exposure

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.5	Users	Protect	•	•	•

Enterprises **should** train workforce members to be aware of causes for unintentional data exposure.

EXAMPLE: Topics can include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

4.14.6 Train workforce members on recognizing and reporting security incidents

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.6	Users	Protect	•	•	•

Enterprises **should** train workforce members to be able to recognize a potential incident and be able to report such an incident.

4.14.7 Train workforce on how to identify and report if their enterprise assets are missing security updates

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.7	Users	Protect	•	•	•

Enterprises **should** train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools.

This training **should** include notifying IT personnel of any failures in automated processes and tools.

4.14.8 Train workforce on the dangers of connecting to and transmitting enterprise data over insecure networks

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.8	Users	Protect	•	•	•

Enterprises **should** train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities.

If the enterprise has remote workers, this training **shall** include guidance to ensure that all users securely configure their home network infrastructure.

4.14.9 Conduct role-specific security awareness and skills training

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
14.9	Users	Protect		•	•

Enterprises **should** conduct role-specific security awareness and skills training.

EXAMPLE: This can include secure system administration courses for IT professionals, OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles [i.37].

4.15 Control 15: Service Provider Management

4.15.0 Overview

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Why Is This Control Critical?

In our modern, connected world, enterprises rely on vendors and partners to help manage their data or rely on third-party infrastructure for core applications or functions.

There have been numerous examples where third-party breaches have significantly impacted an enterprise; for example, as early as the late 2000s, payment cards were compromised after attackers infiltrated smaller third-party vendors in the retail industry. More recent examples include ransomware attacks that impact an enterprise indirectly, due to one of their service providers being locked down, causing disruption to business. Or worse, if directly connected, a ransomware attack could encrypt data on the main enterprise.

Most data security and privacy regulations require their protection extend to service providers, such as with Health Insurance Portability and Accountability Act (HIPAA) Business Associate agreements in healthcare [i.38], Federal Financial Institutions Examination Council (FFIEC) [i.39] requirements for the financial industry, and the United Kingdom (UK) Cyber Essentials [i.44]. Third-party trust is a core Governance Risk and Compliance (GRC) function, as risks that are not managed within the enterprise are transferred to entities outside the enterprise. While reviewing the security of third-parties has been a task performed for decades, there is not a universal standard for assessing security; and many service providers are being audited by their customers multiple times a month, causing impacts to their own productivity. Every enterprise typically has a different "checklist" or set of standards to grade the service provider. There are only a few industry standards, such as in finance, with the Shared Assessments program, or in higher education, with their Higher Education Community Vendor Assessment Toolkit (HECVAT) [i.45]. Insurance companies selling cybersecurity policies also have their own measurements.

While an enterprise might put a lot of scrutiny into large cloud or application hosting companies because they are hosting their email or critical business applications, smaller firms are often a greater risk. Often, a third-party service provider contracts with additional parties to provide other plugins or services, such as when a third-party uses a fourth-party platform or product to support the main enterprise.

Procedures and Tools

Most enterprises have traditionally used standard checklists, such as ones from ISO or the Critical Security Controls. Often, this process is managed through spreadsheets; however, there are online platforms now that allow central management of this process. The focus of this Control though is not on the checklist; instead it is on the fundamentals of the program. Make sure to revisit annually, as relationships and data may change.

No matter what the enterprise's size is, there should be a policy about reviewing service providers, an inventory of these vendors, and a risk rating associated with their potential impact to the business in case of an incident. There should also be language in the contracts to hold them accountable if there is an incident that impacts the enterprise.

There are third-party assessment platforms that have an inventory of thousands of service providers, which attempt to provide a central view of the industry, to help enterprises make more informed risk decisions. These platforms often have a dynamic risk score for service providers, based (usually) on passive technical assessments, or enriched through other firms' third-party assessments.

When performing reviews, focus on the services or departments of the provider that are supporting the enterprise. A third-party that has a managed security service contract, or retainer, and holds cybersecurity insurance, can also help with risk reduction.

It is also important to securely decommission service providers when contracts are completed or terminated. Decommission activities may include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

Specific guidance is available for media sanitization [i.12].

4.15.1 Establish and maintain an inventory of service providers

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
15.1	Users	Identify	•	•	•

Enterprises **should** establish and maintain an inventory of service providers.

The service provider inventory **should** list all known service providers, include classification(s), and designate an enterprise contact for each service provider.

Enterprises **should** review and update the service provider inventory annually, or when significant enterprise changes occur that could impact this Safeguard.

4.15.2 Establish and maintain a service provider management policy

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
15.2	Documentation	Govern		•	•

Enterprises **should** establish and maintain a service provider management policy.

The service provider management policy **should** address the classification, inventory, assessment, monitoring, and decommissioning of service providers.

Enterprises **should** review and update the service provider management policy annually, or when significant enterprise changes occur that could impact this Safeguard.

4.15.3 Classify service providers

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
15.3	Users	Govern		•	•

Enterprises **should** classify service providers.

EXAMPLE: Classification considerations can include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk.

Enterprises **should** review and update service provider classifications annually, or when significant enterprise changes occur that could impact this Safeguard.

4.15.4 Ensure service provider contracts include security requirements

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
15.4	Documentation	Govern		•	•

Enterprises **should** ensure service provider contracts include security requirements.

EXAMPLE: The requirements can include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments.

The security requirements **shall** be consistent with the enterprise's service provider management policy.

Enterprises **should** review service provider contracts annually to ensure contracts are not missing security requirements.

4.15.5 Assess service providers

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
15.5	Users	Govern			•

Enterprises **should** assess whether service providers are consistent with the enterprise's service provider management policy.

NOTE: Assessment scope can vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes.

Enterprises **should** reassess service providers annually, at a minimum, or with new and renewed contracts.

4.15.6 Monitor service providers

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
15.6	Data	Govern			•

Enterprises **should** monitor that service providers are consistent with the enterprise's service provider management policy.

EXAMPLE: Monitoring can include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.

4.15.7 Securely decommission service providers

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
15.7	Data	Protect			•

Enterprises **should** securely decommission service providers.

EXAMPLE: Considerations can include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

4.16 Control 16: Application Software Security

4.16.0 Overview

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Why Is This Control Critical?

Applications provide a human-friendly interface to allow users to access and manage data in a way that is aligned to business functions. They also minimize the need for users to deal directly with complex (and potentially error-prone) system functions, like logging into a database to insert or modify files. Enterprises use applications to manage their most sensitive data and control access to system resources. Therefore, an attacker can use the application itself to compromise the data, instead of an elaborate network and system hacking sequence that attempts to bypass network security controls and sensors. This is why protecting user credentials (specifically application credentials) defined in Control 6 is so important.

Lacking credentials, application flaws are the attack vector of choice. However, today's applications are developed, operated, and maintained in a highly complex, diverse, and dynamic environment. Applications run on multiple platforms: web, mobile, cloud, etc., with application architectures that are more complex than legacy client-server or database-web server structures. Development life cycles have become shorter, transitioning from months or years in long waterfall methodologies, to DevOps cycles with frequent code updates. Also, applications are rarely created from scratch, and are often "assembled" from a complex mix of development frameworks, libraries, existing code, and new code. There are also modern and evolving data protection regulations dealing with user privacy. These can require compliance to regional or sector-specific data protection requirements.

These factors make traditional approaches to security, like control (of processes, code sources, run-time environment, etc.), inspection, and testing, much more challenging. Also, the risk that an application vulnerability introduces might not be understood, except in a specific operational setting or context.

Application vulnerabilities can be present for many reasons: insecure design, insecure infrastructure, coding mistakes, weak authentication, and failure to test for unusual or unexpected conditions. Attackers can exploit specific vulnerabilities, including buffer overflows, exposure to Structured Query Language (SQL) injection, cross-site scripting, cross-site request forgery, and click-jacking of code to gain access to sensitive data, or take control over vulnerable assets within the infrastructure as a launching point for further attacks.

Applications and websites can also be used to harvest credentials, data, or attempt to install malware onto the users who access them.

Finally, it is now more common to acquire Software as a Service (SaaS) platforms, where software is developed and managed entirely through a third-party. These might be hosted anywhere in the world. This brings challenges to enterprises that need to know what risks they are accepting with using these platforms; and, they often do not have visibility into the development and application security practices of these platforms. Some of these SaaS platforms allow for customizing of their interfaces and databases. Enterprises that extend these applications should follow this Control, similar to if they were doing ground-up customer development.

Procedures and Tools

For the previous version of the Controls, SAFECode [i.34] helped develop the procedures and Safeguards for this updated Application Software Security Control. However, application software security is a large topic on its own, and so (consistent with the principles of the overall Controls), the focus here is on the most critical Safeguards. These were derived from a companion paper on application software security that SAFECode developed (referenced below), which provides a more in-depth treatment of the topic, and is consistent with SAFECode's existing body of content.

SAFECode developed a three-tiered approach to help implementers identify which Development Group (DG) is most applicable as a maturity scale for development programs. The three Implementation Group levels used within the Safeguards guided their approach for the DGs below:

Development Group 1

The enterprise largely relies on off-the-shelf or Open Source Software (OSS) and packages with only the occasional addition of small applications or website coding. The enterprise is capable of applying basic operational and procedural best practices and of managing the security of its vendor-supplied software as a result of following the guidance of the Controls.

Development Group 2

The enterprise relies on some custom (in-house or contractor-developed) web and/or native code applications integrated with third-party components and runs on-premises or in the cloud. The enterprise has a development staff that applies software development best practices. The enterprise is attentive to the quality and maintenance of third-party open source or commercial code on which it depends.

Development Group 3

The enterprise makes a major investment in custom software that it requires to run its business and serve its customers. It can host software on its own infrastructure, in the cloud, or both, and can integrate a large range of third-party open source and commercial software components. Software vendors and enterprises that deliver SaaS should consider Development Group 3 as a minimum set of requirements.

The first step in developing an application security program is implementing a vulnerability management process. This process needs to integrate into the development life cycle, and should be lightweight to insert into the standard bug-fixing progress. The process should include root cause analysis to fix underlying flaws so as to reduce future vulnerabilities, and a severity rating to prioritize remediation efforts.

Developers need to be trained in application security concepts and secure coding practices. This includes a process to acquire or evaluate third-party software, modules, and libraries used in the application to ensure they do not introduce security flaws. The developers should be taught what types of modules they can securely use, where they can be safely acquired, and which components they can, or should not, develop themselves (e.g. encryption).

Weaknesses in the infrastructure that supports these applications can introduce risk. The Critical Security Controls and the concept of minimizing the attack surface can help secure networks, systems, and accounts that are used within the application. Specific guidance can be found in Controls 1-7, 12, and 13.

The ideal application security program is one that introduces security as early into the software development life cycle as possible. The management of security problems should be consistent and integrated with standard software flaw/bug management, as opposed to a separate process that competes for development resources. Larger or more mature development teams should consider the practice of threat modelling in the design phase. Design-level vulnerabilities are less common than code-level vulnerabilities; however, they often are very severe and much harder to fix quickly. Threat modelling is the process of identifying and addressing application security design flaws before code is created. Threat modelling requires specific training, technical, and business knowledge. It is best conducted through internal "security champions" in each development team, to lead threat modelling practices for that team's software. It also provides valuable context to downstream activities, such as root cause analysis and security testing.

Larger, or commercial, development teams may also consider a bug bounty program where individuals are paid for finding flaws in their applications. Such a program is best used to supplement an in-house secure development process and can provide an efficient mechanism for identifying classes of vulnerabilities that the process needs to focus on.

In 2020, NIST published its Secure Software Development Framework (SSDF) [i.35], which brought together what the industry has learned about software security over the past two decades and created a secure software development framework for planning, evaluating, and communicating about software security activities. Enterprises acquiring software or services can use this framework to build their security requirements and understand whether a software provider's development process follows best practices. Guidance is available for application security [i.34], [i.35], [i.36] and [i.37].

4.16.1 Establish and maintain a secure application development process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.1	Documentation	Govern		•	•

Enterprises **shall** establish and maintain a secure application development process.

The secure application development process **should** address secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures.

Enterprises **should** review and update the secure application development process annually, or when significant enterprise changes occur that could impact this Safeguard.

4.16.2 Establish and maintain a process to accept and address software vulnerabilities

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.2	Documentation	Govern		•	•

Enterprises **should** establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report.

The vulnerability remediation process **should** include a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing.

The vulnerability remediation process **should** use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities.

Enterprises **should** review and update the vulnerability remediation process annually, or when significant enterprise changes occur that could impact this Safeguard.

NOTE: Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

4.16.3 Perform root cause analysis on security vulnerabilities

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.3	Software	Protect		•	•

Enterprises **should** perform root cause analysis on security vulnerabilities.

NOTE: When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

4.16.4 Establish and manage an inventory of third-party software components

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.4	Software	Identify		•	•

Enterprises **should** establish and manage an updated inventory of third-party components used in development as well as components slated for future use.

NOTE: An inventory of third-party components used in development is often referred to as a "bill of materials",

The third-party component inventory **should** include any risks that each third-party component could pose.

Enterprises **should** review the third-party component inventory at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

4.16.5 Use up-to-date and trusted third-party software components

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.5	Software	Protect		•	•

Enterprises **should** use up-to-date and trusted third-party software components.

When possible, enterprises **should** choose established and proven frameworks and libraries that provide adequate security.

Enterprises **should** acquire third-party software components from trusted sources or evaluate the software for vulnerabilities before use.

4.16.6 Establish and maintain a severity rating system and process for application vulnerabilities

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.6	Documentation	Govern		•	•

Enterprises **should** establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed.

This vulnerability severity rating process **should** include setting a minimum level of security acceptability for releasing code or applications.

NOTE: Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first.

Enterprises **should** review and update the vulnerability severity system and process annually.

4.16.7 Use standard hardening configuration templates for application infrastructure

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.7	Software	Protect		•	•

Enterprises **should** use standard, industry-recommended hardening configuration templates for application infrastructure components.

NOTE: Application infrastructure components include underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components.

Enterprises **should not** allow in-house developed software to weaken configuration hardening.

4.16.8 Separate production and non-production systems

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.8	Network	Protect		•	•

Enterprises **should** maintain separate environments for production and non-production systems.

4.16.9 Train developers in application security concepts and secure coding

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.9	Users	Protect		•	•

Enterprises **should** ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.

EXAMPLE: Training can include general security principles and application security standard practices.

The secure software development training **should** be designed to promote security within the development team and build a culture of security among the developers.

Enterprises **should** conduct secure software development training at least annually.

4.16.10 Apply secure design principles in application architectures

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.10	Software	Protect		•	•

Enterprises **should** apply secure design principles in application architectures.

NOTE 1: Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input".

EXAMPLE 1: Validating user input can include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.

NOTE 2: Secure design also means minimizing the application infrastructure attack surface.

EXAMPLE 2: Minimizing the application infrastructure attack surface can include turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

4.16.11 Leverage vetted modules or services for application security components

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.11	Software	Identify		•	•

Enterprises **should** leverage vetted modules or services for application security components.

NOTE 1: Application security components can include identity management, encryption, and auditing and logging.

NOTE 2: Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors.

EXAMPLE: Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Operating systems also provide mechanisms to create and maintain secure audit logs.

Enterprises **should** use only standardized, currently accepted, and extensively reviewed encryption algorithms.

4.16.12 Implement code-level security checks

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.12	Software	Protect			•

Enterprises **should** apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

4.16.13 Conduct application penetration testing

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.13	Software	Detect			•

Enterprises **should** conduct application penetration testing.

NOTE: For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

4.16.14 Conduct threat modelling

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
16.14	Software	Protect			•

Enterprises **should** conduct threat modelling.

NOTE: Threat modelling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

4.17 Control 17: Incidence Response Management

4.17.0 Overview

Establish a program to develop and maintain an incident response capability (e.g. policies, plans, procedures, defined roles, training and communications) to prepare, detect, and quickly respond to an attack.

Why Is This Control Critical?

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to original state, and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

Protections are not effective 100 % of the time. When an incident occurs, if an enterprise does not have a documented plan - even with good people - it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

Along with detection, containment, and eradication, communication to stakeholders is key. If the probability of material impact due to a cyber event is to be reduced, the enterprise's leadership needs to know what potential impact there could be, so that they can help prioritize remediation or restoration decisions that best support the enterprise. These business decisions could be based on regulatory compliance, disclosure rules, service-level agreements with partners or customers, revenue, or mission impacts.

Dwell time from when an attack happens to when it is identified can be days, weeks, or months. The longer the attacker is in the enterprise's infrastructure, the more embedded they become and they will develop more ways to maintain persistent access for when they are eventually discovered. With the rise of ransomware, which is a stable moneymaker for attackers, this dwell time is critical, especially with modern tactics of stealing data before encrypting it for ransom.

Procedures and Tools

Even if an enterprise does not have resources to conduct incident response within an enterprise, it is still critical to have a plan. This would include the sources for protections and detections, a list of who to call upon for assistance, and communication plans about how to convey information to leadership, employees, regulators, partners, and customers.

After defining incident response procedures, the incident response team, or a third-party, should engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and potential impacts the enterprise faces. These scenarios help ensure that enterprise leadership and technical team members understand their role in the incident response process to help prepare them to handle incidents. It is inevitable that exercise and training scenarios will identify gaps in plans and processes, and unexpected dependencies, which can then be updated into the plan.

More mature enterprises should include threat intelligence and/or threat hunting into their incident response process. This will help the team become more proactive, identifying key or primary attackers to their enterprise or industry to monitor or search for their TTPs. This will help focus detections and define response procedures to identify and remediate more quickly.

The actions in Control 17 provide specific, high-priority steps that can improve enterprise security, and should be a part of any comprehensive incident and response plan [i.10].

4.17.1 Designate personnel to manage incident handling

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.1	Users	Respond	•	•	•

Enterprises **should** designate one key person, and at least one backup, who will manage the enterprise's incident handling process.

NOTE: Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach.

If using a service vendor, enterprises **should** designate at least one person internal to the enterprise to oversee any third-party work.

Enterprises **should** review designations annually, or when significant enterprise changes occur that could impact this Safeguard.

4.17.2 Establish and maintain contact information for reporting security incidents

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.2	Documentation	Govern	•	•	•

Enterprises **should** establish and maintain contact information for parties that need to be informed of security incidents.

EXAMPLE: Contacts can include internal staff, service providers, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders.

Enterprises **should** verify contacts annually to ensure that information is up-to-date.

4.17.3 Establish and maintain an enterprise process for reporting incidents

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.3	Documentation	Govern	•	•	•

Enterprises **should** establish and maintain a documented enterprise process for the workforce to report security incidents.

The incident response process **should** include reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported.

Enterprises **should** ensure the incident reporting process is publicly available to all of the workforce.

Enterprises **should** review the incident reporting process annually, or when significant enterprise changes occur that could impact this Safeguard.

4.17.4 Establish and maintain an incident response process

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.4	Documentation	Govern		•	•

Enterprises **shall** establish and maintain a documented incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan.

Enterprises **should** review the incident response process annually, or when significant enterprise changes occur that could impact this Safeguard.

4.17.5 Assign key roles and responsibilities

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.5	Users	Respond		•	•

Enterprises **should** assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts.

Enterprises **should** review the incident response roles and responsibilities annually, or when significant enterprise changes occur that could impact this Safeguard.

4.17.6 Define mechanisms for communicating during incident response

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.6	Users	Respond		•	•

Enterprises **should** determine which primary and secondary mechanisms will be used to communicate and report during a security incident.

EXAMPLE: Mechanisms can include phone calls, emails, secure chat, or notification letters.

NOTE: Keep in mind that certain mechanisms, such as emails, can be affected during a security incident.

Enterprises **should** review the incident response communication mechanisms annually, or when significant enterprise changes occur that could impact this Safeguard.

4.17.7 Conduct routine incident response exercises

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.7	Users	Recover		•	•

Enterprises **should** plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents.

The incident response exercises **should** test communication channels, decision-making, and workflows.

Enterprises **should** conduct incident response exercises on an annual basis, or more frequently.

4.17.8 Conduct post-incident reviews

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.8	Users	Recover		•	•

Enterprises **should** conduct post-incident reviews.

NOTE: Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.

4.17.9 Establish and maintain security incident thresholds

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
17.9	Documentation	Recover			•

Enterprises **should** establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event.

NOTE: Security incidents can include abnormal activity, security vulnerabilities, security weaknesses, data breaches, or privacy incidents.

Enterprises **should** review the security incident thresholds annually, or when significant enterprise changes occur that could impact this Safeguard.

4.18 Control 18: Penetration Testing

4.18.0 Overview

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Why Is This Control Critical?

A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defences, combined with appropriate action from people. However, it is rarely perfect. In a complex environment where technology is constantly evolving and new attacker tradecraft appears regularly, enterprises should periodically test their controls to identify gaps and to assess their resiliency. This test may be from external network, internal network, application, system, or device perspective. It may include social engineering of users, or physical access control bypasses.

Often, penetration tests are performed for specific purposes:

- As a "dramatic" demonstration of an attack, usually to convince decision-makers of their enterprise's weaknesses.
- As a means to test the correct operation of enterprise defences ("verification").

- To test that the enterprise has built the right defences in the first place ("validation").

Independent penetration testing can provide valuable and objective insights about the existence of vulnerabilities in enterprise assets and humans, and the efficacy of defences and mitigating controls to protect against adverse impacts to the enterprise. They are part of a comprehensive, ongoing program of security management and improvement. They can also reveal process weaknesses, such as incomplete or inconsistent configuration management, or end-user training.

Penetration testing differs from vulnerability testing, described in Control 7. Vulnerability testing just checks for presence of known, insecure enterprise assets, and stops there. Penetration testing goes further to exploit those weaknesses to see how far an attacker could get, and what business process or data might be impacted through exploitation of that vulnerability. This is an important detail, and often penetration testing and vulnerability testing are incorrectly used interchangeably. Vulnerability testing is exclusively automated scanning with sometimes manual validation of false positives, whereas penetration testing requires more human involvement and analysis, sometimes supported through the use of custom tools or scripts. However, vulnerability testing is often a starting point for a penetration test.

Another common term is "Red Team" exercises. These are similar to penetration tests in that vulnerabilities are exploited; however, the difference is the focus. Red Teams simulate specific attacker TTPs to evaluate how an enterprise's environment would withstand an attack from a specific adversary, or category of adversaries.

Procedures and Tools

Penetration testing starts with the reconnaissance of the enterprise and environment, and scanning to identify the vulnerabilities that can be used as entries into the enterprise. It is important to make sure all enterprise assets are discovered that are in-scope, and not just rely on a static list, which might be outdated or incomplete. Next, vulnerabilities will be identified in these targets. Exploits to these vulnerabilities are executed to demonstrate specifically how an adversary can either subvert the enterprise's security goals (e.g. the protection of specific sensitive data) or achieve specific adversarial objectives (e.g. the establishment of a covert Command and Control (C2) infrastructure). The results provide deeper insight, through demonstration, into the business risks of various vulnerabilities. This can be against physical access controls, network, system, or application layers, and often includes social engineering components.

Penetration tests are expensive, complex, and potentially introduce their own risks. Experienced people from reputable vendors need to conduct them. Some risks include unexpected shutdown of systems that might be unstable, exploits that might delete or corrupt data or configurations, and the output of a testing report that needs to be protected itself, because it gives step-by-step instructions on how to break into the enterprise to target critical assets or data.

Each enterprise should define a clear scope and rules of engagement for penetration testing. The scope of such projects should include, at a minimum, enterprise assets with the highest valued information and production processing functionality. Other lower-value systems may also be tested to see if they can be used as pivot points to compromise higher-value targets. The rules of engagement for penetration test analyses should describe, at a minimum, times of day for testing, duration of test(s), and the overall test approach. Only a few people in the enterprise should know when a penetration test is performed, and a primary point of contact in the enterprise should be designated if problems occur. Increasingly popular recently is having penetration tests conducted through third-party legal counsel to protect the penetration test report from disclosure.

The Safeguards in this Control provide specific, high-priority steps that can improve enterprise security, and should be a part of any penetration testing. In addition, use of the many excellent comprehensive resources dedicated to this topic to support security test planning, management, and reporting are recommended.

4.18.1 Establish and maintain a penetration testing program

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
18.1	Documentation	Govern		•	•

Enterprises **should** establish and maintain a penetration testing program appropriate to the size, complexity, industry, and maturity of the enterprise.

NOTE: Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

4.18.2 Perform periodic external penetration tests

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
18.2	Network	Detect		•	•

Enterprises **should** perform periodic external penetration tests based on penetration testing program requirements, no less than annually.

External penetration testing **shall** include enterprise and environmental reconnaissance to detect exploitable information.

External penetration testing **shall** be conducted through a qualified party.

NOTE 1: Penetration testing requires specialized skills and experience.

NOTE 2: The testing may be clear box or opaque box.

4.18.3 Remediate penetration test findings

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
18.3	Network	Protect		•	•

Enterprises **should** remediate penetration test findings based on the enterprise's documented vulnerability remediation process.

Remediation **should** include determining a timeline and level of effort based on the impact and prioritization of each identified finding.

4.18.4 Validate security measures

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
18.4	Network	Protect			•

Enterprises **should** validate security measures after each penetration test.

If deemed necessary, enterprises **should** modify rulesets and capabilities to detect the techniques used during testing.

4.18.5 Perform periodic internal penetration tests

Safeguard	Asset Type	Security Function	IG1	IG2	IG3
18.5	Network	Detect			•

Enterprises **should** perform periodic internal penetration tests based on penetration testing program requirements, no less than annually.

NOTE: The testing may be clear box or opaque box.

Annex A:
Version changes to the Controls

This version of the controls is an iterative update. As part of the process to evolve the Controls, "design principles" are established that guide any minor or major updates to the present document. The design principles for this revision are context, clarity, and consistency. Context enhances the scope and practical applicability of Safeguards by incorporating specific examples and additional explanations. Clarity aligns with other major security frameworks to the extent practical, while preserving the unique features of the Critical Security Controls. Consistency maintains continuity for existing Critical Security Control users, ensuring little to no change due to this update. The broad changes made for each design principle include:

Context: The Controls are updated with new asset classes to better match the specific parts of an enterprise's infrastructure each Safeguard applies to. New definitions are included together with enhanced the descriptions of several Safeguards for greater detail, practicality, and clarity.

Coexistence: The Critical Security Controls have always maintained alignment with evolving industry standards and frameworks. This assists all users of the Controls and is a core principle of how the Controls operate. The release of NIST CSF 2.0 [i.1] necessitated updated mappings and updated security functions.

Consistency: Traditionally any iterative update to the Controls should minimize disruption to Controls users. This means that no Implementation Groups were modified in this update, and the spirit of any given Safeguard remains the same. Additionally, the new asset classes and definitions needed to be consistently applied throughout the Controls, and in doing so some minor updates were added.

With these principles in mind, specific updates include:

- Realigned NIST CSF security function mappings to match NIST CSF 2.0 [i.1].
- A new and expanded glossary definitions for reserved words used throughout the Controls (e.g. plan, process, sensitive data).
- Revised asset classes, alongside new mappings to Safeguards.
- Fixed minor typos in Safeguard descriptions.
- Added clarification to several Safeguard descriptions.
- Added additional reference guidance for each Control.

One key improvement to the Security Functions is the addition of "Governance". Effective governance provides the structure needed to steer a cybersecurity program toward achieving their enterprise goals. The Controls were designed to be comprehensive enough to protect and defend cybersecurity programs for any size enterprise, while being prescriptive enough to ease implementation. With the latest update to the Controls, governance topics are now specifically identified as recommendations that can be implemented to enhance the governance of a cybersecurity program. This will help adopters better identify the governing pieces of the program as well as equip them with the evidence needed to demonstrate compliance.

The Controls aim to streamline the process of designing, implementing, measuring, and managing enterprise security. This involves simplifying language to reduce duplication, focusing on measurable actions with defined metrics, and ensuring each Safeguard is clear and concise. The need to address current cybersecurity challenges is continuously balanced with maintaining a stable, foundational cyber defence strategy, steering clear of overly complex or inaccessible technologies. Technology is constantly shifting, and the Controls reflect awareness of the developments in Artificial Intelligence, augmented reality, and ambient computing working to reshape enterprise infrastructure in subtle and radical ways that will be reflected in future versions.

Annex B: Bibliography

- CIS: "CIS Controls Assessment Specification".
- CIS: "Configuration Assessment Tool (CAT)".
- CIS: "CIS Controls Self Assessment Tool (CSAT)".
- CIS: "CIS Risk Assessment Method (RAM)".
- Council of Registered Security Testers (CREST): "Cyber Security Incident Response Guide".
- CSA: "AI Controls".

History

Document history		
V1.1.1	May 2015	Publication as ETSI TR 103 305
V2.1.1	August 2016	Publication as ETSI TR 103 305-1
V3.1.1	September 2018	Publication as ETSI TR 103 305-1
V4.1.1	December 2021	Publication as ETSI TR 103 305-1
V4.1.2	April 2022	Publication as ETSI TR 103 305-1
V4.2.1	October 2024	Publication as ETSI TR 103 305-1
V5.1.1	September 2025	Publication