Guide to Asset Classes

CIS Critical Security Controls v8.1

September 2024

Center for Internet Security®

CIS Controls™

Contents

Introduction

The CIS Critical Security Controls® (CIS Controls®) are a set of best practices that are designed to protect an enterprise from the most common cyber attacks. In CIS Controls v8, enhancements were made to keep up with evolving technology, evolving threats, and the evolving workplace. A big part of v8's development involved simplifying the language, ensuring that practical guidance is given, and that each Safeguard is measurable.

CIS Controls version 8.1 (v8.1) is an iterative update to version 8. As part of our process to evolve the CIS Controls, we establish "design principles" that guide us through any minor or major updates to the document. Our 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 CIS Controls. Consistency maintains continuity for existing CIS Controls users, ensuring little to no change due to this update.

At the very foundation of the CIS Controls are a few critical actions that should be taken before any other Safeguards are implemented, which surround knowing your environment. In order to protect what you have, you first must know what you have. When implementing and auditing the CIS Controls, there are several references to terms such as enterprise assets, software, end-user devices, and more. CIS simplified the language in v8 to provide enterprises guidance on how enterprise assets and software are organized in the CIS Controls and to help explain what we mean when we say things like "Establish and Maintain Detailed Enterprise Asset Inventory." In v8.1, CIS restructured Asset Classes and their respective definitions to ensure consistency throughout the Controls.

Adopters of the CIS Controls should use this guide as a reference during activities such as implementation or auditing to verify that all in-scope assets are being accounted for and are secured.

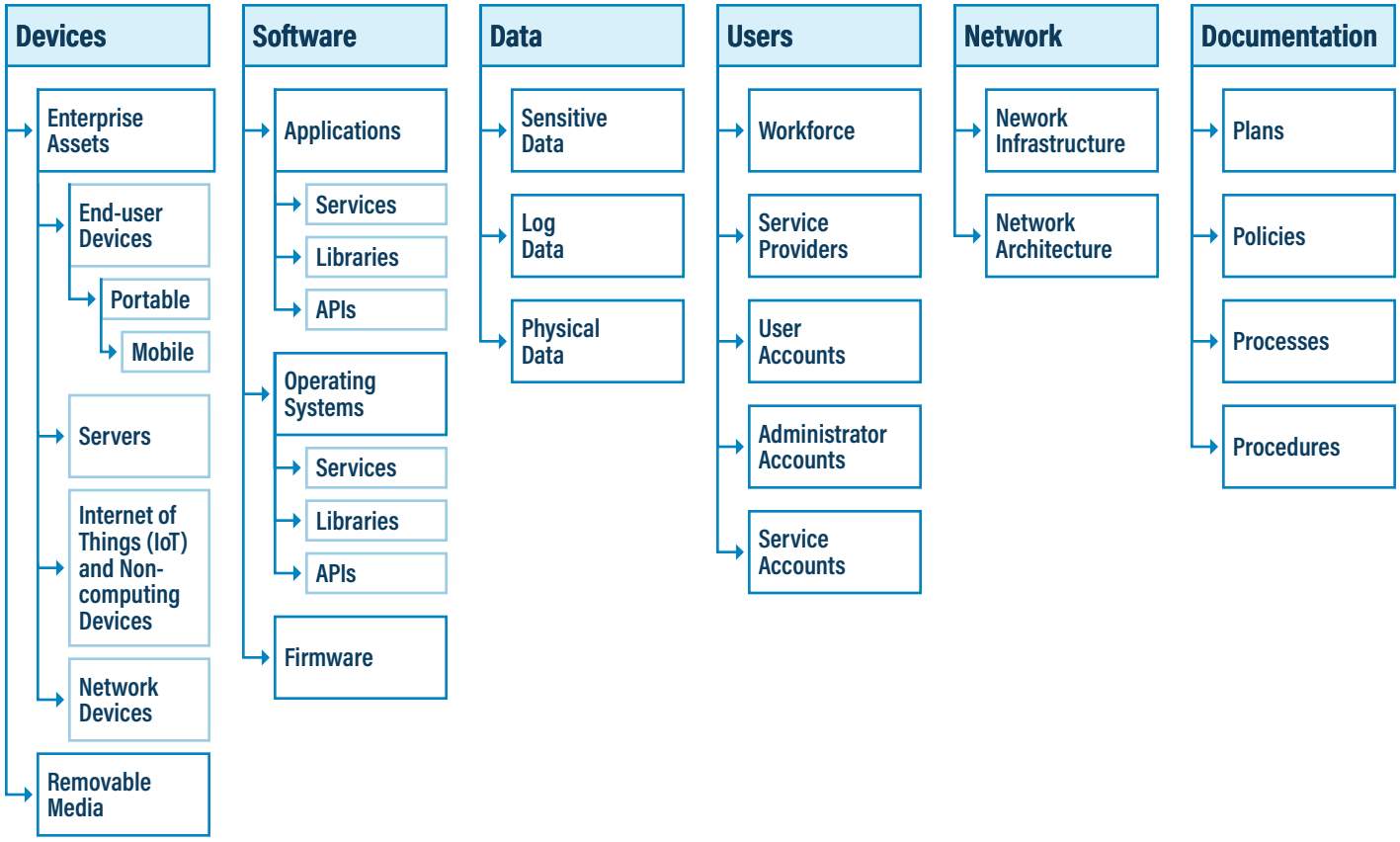
Asset Classes

What is an Asset Class?

Asset Classes can help to classify controls into different categories based on what assets they are protecting. An Asset Class is a group of information assets that are evaluated as one set based on their similarity. In Controls v8.1, the Asset Classes are broken into the following categories:

- Devices
- Software
- Data
- Users
- Network
- Documentation

Figure 1. Asset Classes



Devices

What are Devices?

Devices may exist in physical spaces, virtual infrastructure, or cloud-based environments. Devices can remotely connect to these systems. Devices consist of enterprise assets (including end-user devices, portable devices, and mobile devices; servers; Internet of Things (IoT) and non-computing devices; and network devices) and removable media.

What are enterprise assets?

Enterprise assets are assets with the potential to store or process data. Enterprise assets include *end-user devices, network devices, non-computing/Internet of Things (IoT) devices,* and *servers,* in virtual, cloud-based, and physical environments.

Where do remote devices fit into enterprise assets?

Any **enterprise asset** is generally capable of connecting to a network remotely, usually from public internet. This can include enterprise assets such as end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers.

What types of environments can enterprise assets exist in?

Enterprise assets can exist in physical, virtual, or cloud environments.

A **physical environment** consists of hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network.

A **cloud-based environment** provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. 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).

A **virtualized environment** simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many—with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work.

What are end-user devices?

End-user devices are information technology (IT) assets used among members of an enterprise during work hours, off-hours, or for any other purpose. End-user devices include desktops and workstations, as well as portable and mobile devices such as laptops, smartphones, and tablets. End-user devices are a *subset of enterprise assets.*

Are there subsets of end-user devices?

Yes. There are two subsets of end-user devices: **portable devices** and **mobile devices.**

Portable devices are 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, all of which are a *subset of enterprise assets.*

Mobile devices are small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile devices are a *subset of portable devices.*

What other types of enterprise assets are there?

Network devices are electronic devices required for communication and interaction between devices on a computer network. 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. Network devices are a *subset of enterprise assets.* Note that 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.

Non-computing and Internet of Things (IoT) devices are 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. While these devices are not used for computational processes, they support an enterprise's ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems, and information technology sensors. Non-computing/IoT devices are a *subset of enterprise assets.*

Servers are devices or systems that provide resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Servers can exist in datacenters, public/private/hybrid cloud environments, including temporal containers or serverless workloads. Examples include web servers, application servers, mail servers, and file servers. Servers are a *subset of enterprise assets.*

What is removable media?

Removable media is 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 compact discs (CDs), digital video discs (DVDs) and Blu-ray discs, tape backups, as well as diskettes and universal serial bus (USB) drives.

Figures 2 and 3 shows a high-level chart of how enterprise assets and removable media are categorized in CIS Controls v8.1. Cells in white are examples of the enterprise asset subsets and are not meant to represent an exhaustive list.

Figure 2. Enterprise Assets

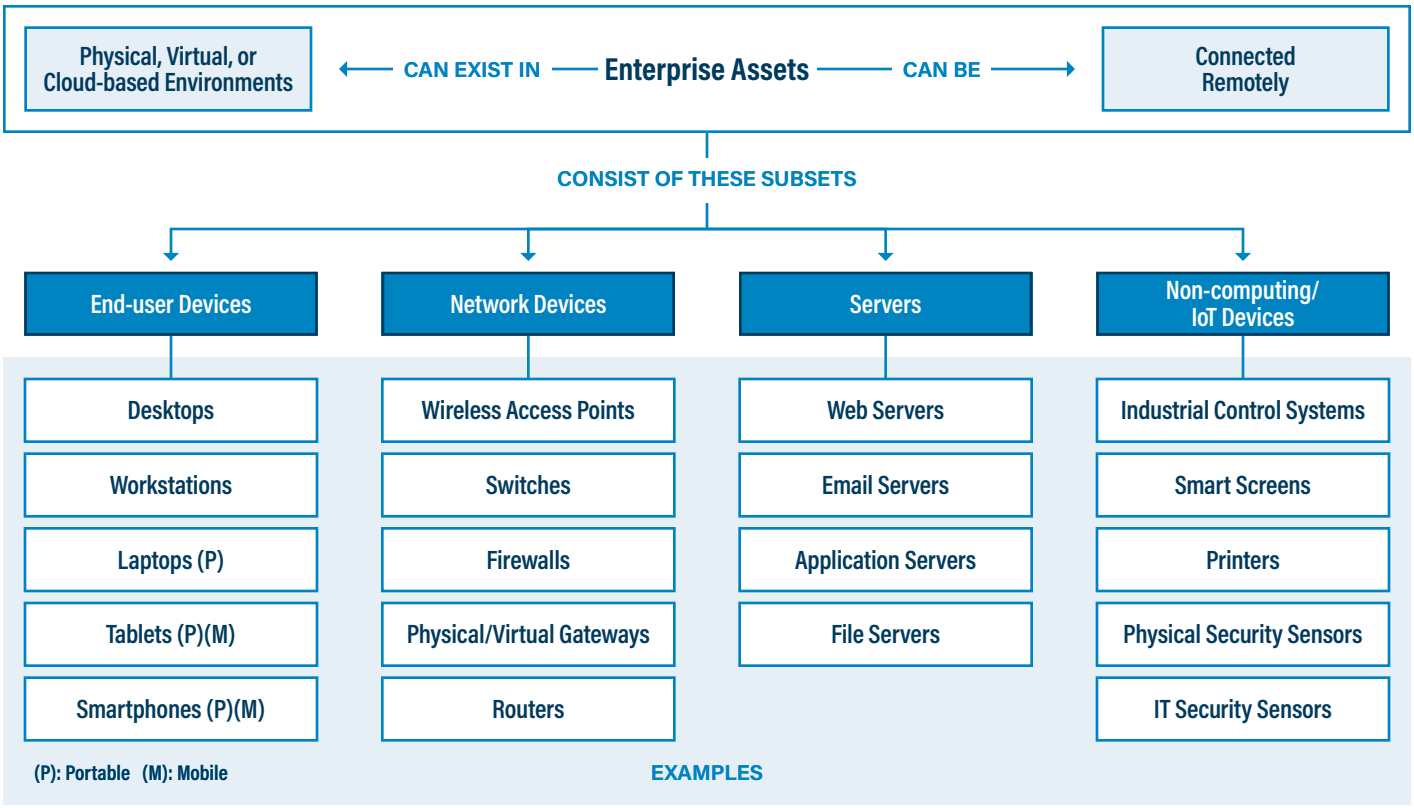
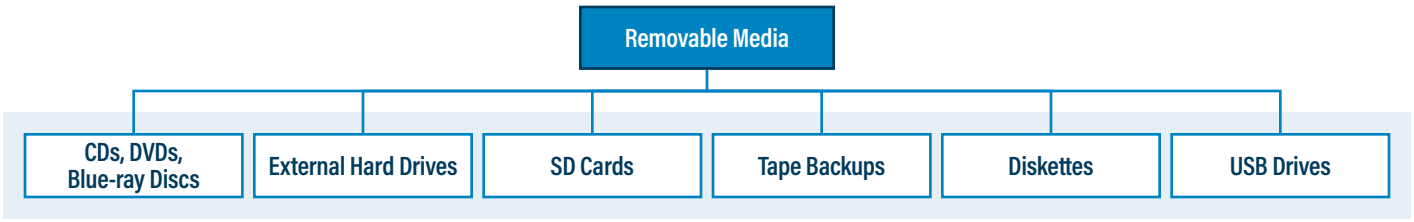


Figure 3. Removable Media



Software

What are software assets?

Also referred to as software in CIS Controls v8.1, these are 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). Software assets include operating systems, applications, and firmware. Enterprise assets contain software assets.

Are there subsets of software assets?

Yes. There are three subsets of software assets: **applications**, **operating systems**, and **firmware**.

An **application** is a program, or group of programs, running on top of an operating system hosted on enterprise assets. Applications are considered a software asset in this document. Examples include web, database, cloud-based, and mobile applications. Applications are a *subset of software*.

An **operating system** is software on enterprise assets that manages computer hardware and software resources, and provides common services for programs. Operating systems are considered a software asset and can be single- and multi-tasking, single- and multi-user, distributed, templated, embedded, real-time, and library. Operating systems are a *subset of software*.

Firmware is 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. Firmware is a *subset of software*.

Are there components of applications and operating systems?

Yes. While there are multiple components that make up applications and operating systems, CIS Controls v8.1 focuses on two key areas that are most vulnerable to exploitation: **services** and **libraries**.

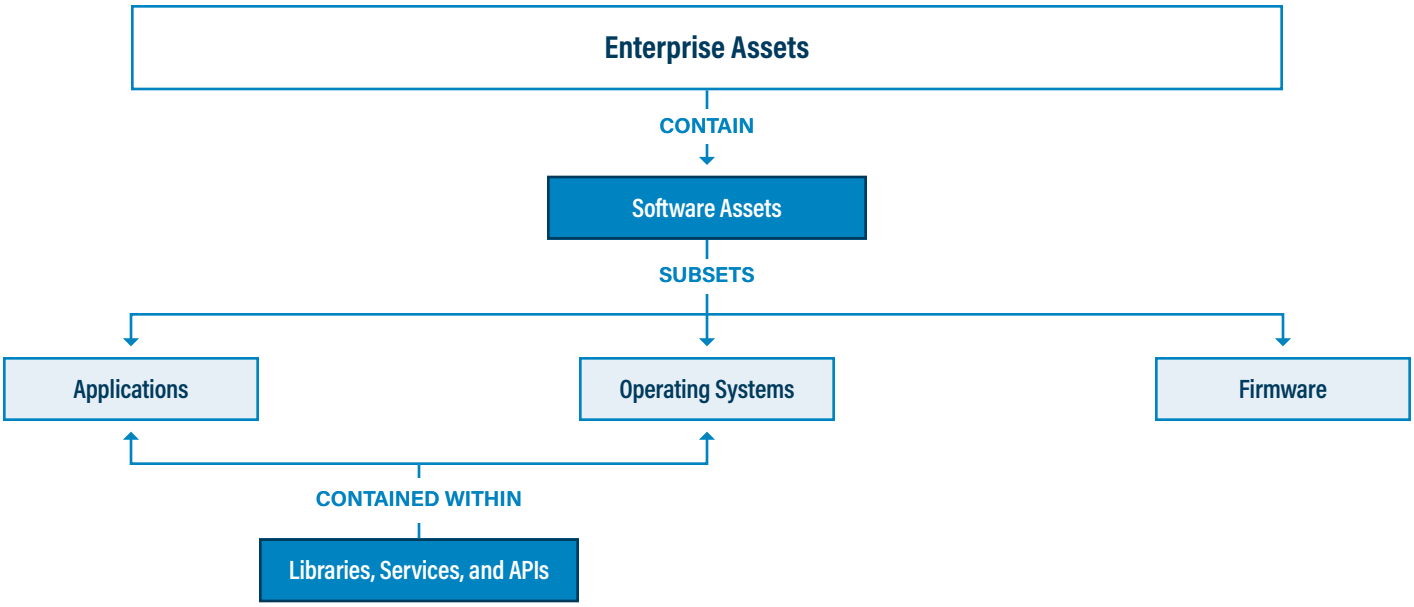
A **service** refers to specialized programs that perform well-defined critical tasks for the operating system. Services often start with the operating system, run in the background, and can be stopped and started by users. Example services include managing network communications, users, file permissions,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

A **library** is 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.

An **Application Programming Interface (API)** is 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.

Figure 4 shows a high-level chart of how software assets are categorized in v8.1 of the CIS Controls.

Figure 4. Software Categorization



Data

What is Data?

Data is a collection of facts that can be examined, considered, and used for decision-making. Although data may be physical, the CIS Controls primarily provide protection for digital data that may be stored, transferred, and processed by enterprise assets.

Are there Subsets of Data?

Yes. There are three subsets of Data: Sensitive Data, Log Data, and Physical Data.

Sensitive Data is physical or digital data stored, processed, or managed by the enterprise that must 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 is 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 is 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

What are Users?

Users are 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.

Are there Subsets of Users?

Yes. There are five subsets of **Users** including **Workforce, Service Providers, User Accounts, Administrator Accounts,** and **Service Accounts.**

Workforce includes 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 are entities that offer platforms, software, and services to other enterprises. Examples include IT consultants, managed service provider (MSPs), 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 is 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 this document, user accounts refer to "standard" user accounts with limited privileges and are used for general tasks.

Administrator Accounts are 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 accounts, domain administrator accounts, and network or security appliance administrator accounts.

Service Accounts are 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

What is a Network?

A **network** is a group of interconnected devices that exchange data. Enterprises may operate one or more networks that are managed together or independently.

Are there Subsets of Network?

Yes. There are two subsets of the **Network Asset Class: Network Infrastructure** and **Network Architecture.**

Network Infrastructure refers to all of the resources of a network that make network or internet connectivity, management, business operations, and communication possible. 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

What is Documentation?

Documentation includes 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 and processes that users follow or describe network architecture.

Are there subsets of Documentation?

Yes. There are four subsets of Documentation: **Plan, Policy, Process,** and **Procedure.**

A **plan** implements policies and may include groups of policies, processes, and procedures.

A **policy** is an official governance statement that outlines specific objectives of an information security program. A policy will either dictate actions that must be taken or specify which actions are prohibited.

A **process** is 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.

A **procedure** is an ordered set of steps that must be followed to accomplish a specific task. It provides the approved way of performing an action in a specific technological and organizational environment.

Resources

For more information on CIS Controls v8.1, visit our website at https://www.cisecurity.org/controls. Additionally, find out how to join one of our Communities on CIS WorkBench.

- CIS Hardware and Software Asset Tracking Spreadsheet
- CIS Controls Policy Templates
- CIS Critical Security Controls v8.1
- CIS Critical Security Controls Community

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CIS Center for Internet Security®

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
CenterforIntSec
@CISecurity
TheCISecurity
cisecurity