Audit Log Management Policy Template

**CIS Critical Security Controls**

**November 2022**

# Contents

[Contents 2](#_Toc117435056)

[Acknowledgments 3](#_Toc117435057)

[Introduction 4](#_Toc117435058)

[Purpose 4](#_Toc117435059)

[Types of Audit Logs 4](#_Toc117435060)

[Scope 4](#_Toc117435061)

[Audit Log Asset Lifecycle 6](#_Toc117435062)

[Audit Log Management Policy Template 8](#_Toc117435063)

[Purpose 8](#_Toc117435064)

[Responsibility 8](#_Toc117435065)

[Exceptions 8](#_Toc117435066)

[Policy 8](#_Toc117435067)

[Revision History 10](#_Toc117435068)

[Appendix A: Acronyms and Abbreviations 11](#_Toc117435069)

[Appendix B: Glossary 12](#_Toc117435070)

[Appendix C: Implementation Groups 14](#_Toc117435071)

[Appendix D: CIS Safeguards Mapping 15](#_Toc117435072)

[Appendix E: References and Resources 16](#_Toc117435073)

# Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

**Editors:**

Joshua M Franklin, CIS

**Contributors:**

Tony Krzyzewski, SAM for Compliance Ltd
Staffan Huslid, Truesec
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)
Bryan Chou, CISSP, GSEC, GCED, GCIH
Bryan Ferguson
Gavin Willbond, SSS - IT Security Specialists
Ken Muir
Keala Asato
Jon Matthies
Robin Regnier, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License. (The link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.)

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization, and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to <http://www.cisecurity.org/controls/> when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS®).

# Introduction

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 analyze them. Attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target enterprise knowing.

## Purpose

The CIS Critical Security Controls® (CIS Controls®) recommend multiple information security policies that an enterprise should have in place. This includes an audit log management policy. This policy is meant as a “jumping off point” for organizations needing to draft their own policies to govern a log management strategy. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decision points and areas that must be tailored to your enterprise. In CIS Controls v8, Control 8 states:

**Control 8 – Audit Log Management**

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

To support this Safeguard, it is important for an enterprise to develop a log management process. At a minimum, this process should include procedures for enabling the appropriate logs on enterprise assets, collecting these logs for future analysis, and ensuring sufficient space to store the logs is available within the enterprise This document supports the development of those processes in accordance with the CIS Controls.

## Types of Audit Logs

Many types of audit logs exist. Here are a few examples.

* Operating system log files
* Antivirus, antimalware, or host-based intrusion detection logs
* Application logs
* Firewall logs
* Webserver logs
* Physical access control logs
* Access control logs for sensitive data

## Scope

This policy template is meant to supplement the CIS Controls v8. The policy statements included within this document can be used by all CIS Implementation Groups (IGs), but are specifically geared towards Safeguards in Implementation Group 1 (IG1). In [Appendix D](#_Appendix_D:_CIS), Safeguards unique to IG1 are specifically highlighted for ease of use. For more information on the CIS Implementation Groups, see [Appendix C](#_Appendix_C:_Implementation). Additionally, a glossary in [Appendix B](#_Appendix_B:_Definitions) is provided for guidance on terminology used throughout the document. Future versions of this template may expand the scope to both Implementation Group 2 (IG2) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1, and are welcome to do so. Depending on an enterprise’s sector or mission, other policy statements may also need to be added or removed. This is encouraged as this policy needs to be molded and fit to the enterprise’s needs.

# Audit Log Asset Lifecycle

This *Audit Log Management Policy* is divided into multiple sections based on usage patterns of assets within an enterprise. These sections are shown below in Figure 1 are the high-level “steps” of the audit log management process, followed by a detailed description of what each step entails.



Figure 1. Audit Log Management Lifecycle

* **Generation** – Configuring assets to create audit logs.
* **Transmission** – Moving audit logs from local asset storage to a centralized datastore for collection and analysis.
* **Storage** – Securely storing and retaining audit logs for when analysis must be performed.
* **Analysis** – Analyzing logs to identify anomalous events and errors/issues with enterprise assets.
* **Disposal** – Removing or archiving audit logs from enterprise assets.

**Generation**

Logs are generated *by default* on some platforms and are not on others. Some applications and operating systems have verbose log settings that provide much more information to the user than what is typically provided. Enterprises will need to make a decision on specific log settings so that properly log generation settings are properly enabled on all enterprise assets. This includes contractor assets and third-party service providers. The exact content of what to log will differ for each enterprise. Microsoft provides a [set of recommendations for Windows platforms](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations). The [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/) will also include logging recommendations for many platforms.

Once logs are enabled on the appropriate assets, these assets need to be checked from time to time to ensure that the correct log settings are still enabled, or configuration drift has not occurred. As technology changes, log generation settings will need to be updated. When systems and software versions are updated, log settings may revert back to default settings or new settings chosen by the developer that are not in line with enterprise standards. Finally, enterprises should ensure that sufficient local storage is available for devices and applications to generate and store logs on before they are sent elsewhere for analysis and storage This is especially important on embedded devices or other devices without much local storage. If sufficient storage is not present, undesirable events may occur such as loss of logs, unexpected application functionality, or even device failure in rare cases.

**Transmission**

Most devices will not have sufficient storage to keep large volumes of logs for extended periods of time. This means that logs will need to be offloaded to another, often dedicated log storage system. This process should be done in a secure manner with established protocols and proper forms of mutual authentication to ensure that logs are not viewed or modified by unauthorized parties. Proper security controls should be used whenever logs are moved from one system to another, whether it is for long-term storage, analysis, or responding to legal requests.

**Storage**

Log retention may be accomplished by transferring logs to an external archival asset for storage in real-time or sent in batches on a pre-specified schedule. In some enterprises, there may be a single log storage datastore for the entire network, or logs may be stored in many areas throughout the network. Regardless, security protections need to be applied to logs as they are stored. This includes proper encryption and forms of integrity protection like cryptographic hashes.

**Analysis**

Manual log analysis does not necessarily scale with even a small enterprise. There are often simply too many unique assets generating a large number of logfiles, and a seasoned team of incident response responders would struggle to keep up. This is regardless of how logs are used, such as within investigations after the fact once a data breach occurs. Things are different for automated log analysis. There may be a single system performing analysis of all logs in an enterprise such as a Security Information and Event Management (SIEM), or analysis may take place on a per-application basis. The goal of automated log analysis is multifold; event correlation to decide if a breach occurred, proactively identify vulnerabilities before a breach occurs, identify faults, errors, or other issues in enterprise assets that need to be fixed. Reporting anomalies of all types to the appropriate person or group within the enterprise.

**Disposal**

Logs may need to be archived indefinitely or for a specific period of time dictated by local/governmental laws. Industry norms may also dictate storage timeframe. This is important to do on devices without large amounts available storage for log files since the local log storage location may fill up and logs may no longer be stored, or old ones may be overwritten. CIS recommends that audit logs are retained for a minimum period of 90 days before disposal.

**Alert**

When log analysis is being performed, at times there will be an issue or event that merits further. This is the case with both manual and automated log analysis. There should be a process in place for who is alerted to specific types of events in the network. Thresholds for SIEMs reporting alerts can be very tricky to get right, with large amounts of false positives. Regardless, it is important for a knowledgeable professional to review all alerts from systems and engineers performing log analysis to see if the incident response plans need to be activated.

# Audit Log Management Policy Template

## Purpose

Audit log management includes generating, storing, analyzing logs files in order to identify and respond to suspicious or anomalous events occurring within the enterprise. prioritizing, and remediating vulnerabilities in enterprise systems and software. The *Audit Log Management Policy* provides the processes and procedures for ensuring logs are created and properly analyzed. This policy applies to all departments and all assets connected to the enterprise network.

## Responsibility

The Information Technology (IT) business unit is responsible for all log management functions. Specifically, administrators are responsible for configuring the correct devices to generate, store, and transmit logs. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them, such as applying updates in a regular manner or restarting their systems. All enterprise assets are required to comply with the enterprise audit logging procedures.

## Exceptions

Exceptions to this policy are likely to occur. Requests for exception must be made in writing and must contain:

* The reason for the request,
* Risk to the enterprise of not following the written policy,
* Specific mitigations that will not be implemented,
* Technical and other difficulties, and
* Date of review.

## Policy

**Generation**

1. An enterprise-wide strategy must be developed to establish and maintain an audit log process.
2. This strategy must be documented.
3. Documentation must be updated annually, or when significant changes have occurred.
4. The contents of logs must be specified within the Secure Configuration Policy.
5. Audit logging must be enabled on all enterprise assets, as is practical.
6. Audit logs must not be disabled on enterprise assets.

**Transmission**

1. Procedures must be developed to move logs from enterprise assets to an audit log datastore.
2. This may be done manually or via electronic means.
3. Access controls must be used to prevent audit logs from being modified in an unauthorized manner.

**Storage**

1. Procedures must be developed to collect audit logs from enterprise assets.
2. Sufficient storage space must be allocated for audit logs for the period of time required for analysis and retention.
3. Sufficient space must be allocated to store audit logs on all enterprise assets.
4. Sufficient space must be allocated to store audit logs on any centralized audit log datastore.
5. Retention timeframes for audit logs should be in accordance with the enterprise data management process.

**Review and Analysis**

1. All high severity events must be acted upon in accordance with the audit log management process.

**Disposal**

1. All audit logs must be stored for a period of time specified by the audit log management process.
2. Archived logs must be available for analysis.
3. Disposal of audit logs should be in accordance with the enterprise data management process.

**Alert**

There are no IG1 safeguards that support this portion of the audit log management process.

Revision History

Each time this document is updated, this table should be updated.
.

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Revision Date | Revision Description | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix A: Acronyms and Abbreviations

|  |  |
| --- | --- |
| CIS | Center for Internet Security |
| CIS Controls | Center for Internet Security Critical Security Controls |
| COTS | Commercial-off-the-shelf |
| IaaS | Infrastructure as a Service (IaaS) |
| IG | Implementation Group |
| IoT | Internet of Things |
| IT | Information Technology |
| SIEM | Security Information and Event Management |

# Appendix B: Glossary

|  |  |
| --- | --- |
| Asset | Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).Source: [Asset(s) - Glossary | CSRC (nist.gov)](https://csrc.nist.gov/glossary/term/asset) |
| Asset inventory  | An asset inventory is a register, repository or comprehensive list of an enterprise’s assets and specific information about those assets.Source: [Asset Inventory | FTA (dot.gov)](https://www.transit.dot.gov/TAM/resources/assetinventory) |
| Asset owner | The department, business unit, or individual responsible for an enterprise asset.Source: CIS |
| Cloud environment | A virtualized environment that 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). |
| Enterprise assets | Assets with the potential to store or process data. For the purpose of this 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.Source: CIS Controls v8  |
| End-user devices | Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones, and tablets as well as desktops and workstations. For the purpose of this document, end-user devices are a subset of enterprise assets.Source: CIS Controls v8 |
| Enterprise asset identifier  | Often a sticker or tag with a unique number or alphanumeric string that can be tracked within an enterprise asset inventory.Source: CIS |
| Mobile end-user devices | Small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile end-user devices are a subset of portable end-user devices, including laptops, which may require external hardware for connectivity. For the purpose of this document, mobile end-user devices are a subset of end-user devices.Source: CIS Controls v8 |
| Network devices | 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. For the purpose of this document, network devices are a subset of enterprise assets.Source: CIS Controls v8 |
| 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. 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. For the purpose of this document, non-computing/IoT devices are a subset of enterprise assets.Source: CIS Controls v8 |
| Physical environment | Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network.Source: CIS Controls v8 |
| Portable end-user devices | Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this document, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets.Source: CIS Controls v8 |
| Remote devices | Any enterprise asset 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.Source: CIS Controls v8 |
| Servers | A device or system that provides 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. Examples include web servers, application servers, mail servers, and file servers.Source: CIS Controls v8 |
| User | Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset.Source: CIS |
| Virtual 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.Source: CIS Controls v8 |

# Appendix C: Implementation Groups

As a part of our most recent version of the CIS Controls, v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

**IG1**

An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards 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**

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 may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information, and they 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**

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 must 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 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at <https://www.cisecurity.org/controls/cis-controls-list/>.

# Appendix D: CIS Safeguards Mapping

**CIS Controls & Safeguards Covered by this Policy**

This policy helps to bolster IG1 Safeguards in CIS Control 8: *Audit Log Management*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table 1 - Safeguards covered by IG1

|  |  |  |  |
| --- | --- | --- | --- |
| CIS Control | Policy Statement | CIS Safeguard | CIS Safeguard Description |
| 3.3 | Transmission 2 | Configure Data Access Control Lists  | Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |
| 3.4 | Storage 3 | Enforce Data Retention | Retain data according to the enterprise’s data management process. Data retention must include both minimum and maximum timelines. |
| 3.6 | Transmission 2 | Encrypt Data on End-User Devices | Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt. |
| 8.1 | Generation 1, 1a, 1b, 1c, 1d Transmission 1, 1aReview & Analysis 1 | Establish and Maintain an Audit Log Management Process | Establish and maintain an audit log management process that defines the enterprise’s logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard |
| 8.2 | Generation 2, 3Storage 1 | Collect Audit Logs | Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets. |
| 8.3  | Storage2, 2a, 2b | Ensure Adequate Audit Log Storage | Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process. |

# Appendix E: References and Resources

Center for Internet Security®

<https://www.cisecurity.org/>

CIS Benchmarks™
https://www.cisecurity.org/cis-benchmarks/

CIS Critical Security Controls®

<https://www.cisecurity.org/controls/>

Microsoft Audit Policy Recommendations
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations