Audit & Logging Plan

Table of Contents

[Background 3](#_Toc16774170)

[Purpose 3](#_Toc16774171)

[Definitions 3](#_Toc16774172)

[Centralised Monitoring Tool 4](#_Toc16774173)

[Security Information and Event Monitoring Tool 4](#_Toc16774174)

[[Business Name] IT Systems 4](#_Toc16774175)

[Events To Be Logged 4](#_Toc16774176)

[Minimum Logging Requirements 4](#_Toc16774177)

[Event Details 5](#_Toc16774178)

[Event Log Protection and Retention 6](#_Toc16774179)

[Protecting Event Logs 6](#_Toc16774180)

[Retention of Event Logs 6](#_Toc16774181)

[Event Log Auditing 6](#_Toc16774182)

[Information Security Strategy 6](#_Toc16774183)

[Scope of Audits 6](#_Toc16774184)

[Audit Schedule 7](#_Toc16774185)

[Reporting Requirements 7](#_Toc16774186)

# Background

**[Describe The Background Of Why An Audit & Logging Plan Has Come About.]**

This document is the audit and logging plan for **[Business Name]**. This document describes how audit and event logs are captured and managed.

The audit and logging plan outlines all implemented security mechanisms that are utilised in the operation of **[Business Name]** IT environment. This document is intended to be referenced in concert with the **[Business Name]** Security Risk Management Plan (SRMP) that documents the security threats and associated risks within the **[Business Name]** IT environment.

# Purpose

**[Describe What The Intent Of This Document Will Be.]**

This document identifies which logs are required to be collected from within the **[Business Name]** IT environment and outlines requirements for the management and auditing of these logs.

The audit and logging plan aims to increase the security posture of the **[Business Name]** IT environment by ensuring the accountability of all user actions and improving the chances that malicious behaviour will be detected.

# Definitions

**[Define Any Terms That Are Used Throughout This Document.]**

|  |  |
| --- | --- |
| Terms | Definition |
| Information Resources | **Information Resources**: **[Business Name]** Information and related resources, such as equipment, devices, software, and other information technology. |
| Information System Owner | **Information System Owner**: The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of **[Business Name]** and is organisationally responsible for the loss, limited by the bounds of the Information System, associated with a realised information security risk scenario. |
|  |  |
|  |  |
|  |  |
|  |  |

# Centralised Monitoring Tool

## Security Information and Event Monitoring Tool

**[Business Name]** has implemented a centralised logging facility to enable consolidation of event logs from multiple sources, for the purpose of monitoring and analysis. This functionality is provided via a Security Information and Event Monitoring (SIEM) tool.

The SIEM Tool enables event logs from individual systems to be captured and monitored centrally. A dashboard will provide an overview of notable events and supports investigation of unusual activity.

Event logs should be saved to the SIEM tool as soon as possible after each event occurs.

## [Business Name] IT Systems

System-specific event logs are captured and stored by individual systems. Data captured by the **[Business Name]** SIEM tool will be expanded progressively, to include event logs for each of these systems. If this is not possible, a hybrid model should be used, with monitoring of logs at the system level for those systems which have not yet been integrated with the SIEM tool.

The IT team will work to ensure all existing systems are progressively configured to save event logs to the secure centralised logging facility.

All new systems must capture system event logs in line with requirements outlined in this document. Prior to being commissioned into production state, all new systems must be configured to submit event logs to the SIEM tool.

Each system that submits logs to the SIEM tool will use the network time protocol to ensure a consistent and accurate time source is used across systems to assist with the correlation of events.

# Events To Be Logged

## Minimum Logging Requirements

Where technically possible, the following events must be logged for all software components, as a minimum:

• All privileged operations

• Successful and failed elevation of privileges

• Security related system alerts and failures

• User and group additions, deletions and modification to permissions

• Unauthorised access attempts to critical systems and files

• Logons

• Failed logon attempts

• Logoffs

In addition, the events listed below should be logged where technically possible, as they can be useful for reviewing, auditing or investigating software components of systems:

|  |  |
| --- | --- |
| Software Component | Events to Log |
| Database | * Access to particularly sensitive information
* Addition of new users, especially privileged users
* Any query containing comments
* Any query containing multiple embedded queries
* Any query or database alerts or failures
* Attempts to elevate privileges
* Attempted access that is successful or unsuccessful
* Changes to the database structure
* Changes to user roles or database permissions
* Database administrator actions
* Database logons and logoffs
* Modifications to data
* Use of executable commands e.g. xp\_cmdshell
 |
| Operating System | * Access to sensitive data and processes
* Application crashes including any error messages
* Attempts to use special privileges
* Changes to accounts
* Changes to security policy
* Changes to system configuration data
* DNS and HTTP requests
* Failed attempts to access data and system resources
* Service failures and restarts
* Successful and failed attempts to logon and logoff
* System startup and shutdown
* Transfer of data to external media
* User or group management
* Use of special privileges
 |
| Web Application | * Attempted access that is denied
* Search queries initiated by users
* User access to a web application
* Web application crashes including any error messages
 |

## Event Details

For each event logged, sufficient detail needs to be recorded in order for the logs to be useful when reviewed. Consequently, the logging facility must record the following details, where applicable:

• Date and time of the event

• Relevant users or process

• Event description

• Success or failure of the event

• Event source e.g. application name

• ICT equipment location/identification

# Event Log Protection and Retention

## Protecting Event Logs

To help ensure the integrity and availability of captured event logs, the event logs must be protected from modification and unauthorised access; and whole or partial loss within the defined retention period. Therefore, event log data must be archived in a manner that maintains its integrity.

The SIEM tool, has been implemented to capture logs for the purpose of centralised monitoring. The SIEM tool should be designed to store logs for archival purposes.

## Retention of Event Logs

To ensure compliance with National Archives of Australia (NAA) Administrative Functions Disposal Authority, event logs must be retained for a minimum of 7 years after action is completed. However, as event logs can assist in reviews, audits and investigations, event logs should ideally be retained for the life of the system and potentially longer.

Domain Name System (DNS) and proxy logs should be retained for at least 18 months.

# Event Log Auditing

Conducting event log audits helps to detect and attribute violations of information security policy, including cyber security incidents, breaches and intrusions. For this reason, event auditing is an integral part of the maintenance of systems.

## Information Security Strategy

The [Business Name] Information Security Strategy sets out the high-level management direction and support for the establishment, implementation, maintenance and oversight of IT security.

Event log monitoring and auditing are required to identify violations of [Business Name] security policies, such as improper use of privileged access, or attempts to circumvent security controls.

Where event log auditing identifies a potential cyber security incident, breach or intrusion, a security incident must be raised and managed in accordance with the [Business Name] Security Incident Response Plan.

## Scope of Audits

The SIEM tool can be configured to highlight notable events, based on agreed correlation rules. In addition, the SIEM tool can be configured to identify whether specified logs are being captured. These automated monitoring and auditing measures assist with identification of unusual or suspicious activity.

The IT Security uses the SIEM tool on a daily basis to review and investigate event log data, using dashboards as a starting point.

In addition, the IT Security team undertakes manual audits of event logs. These manual audits involve reviewing a sample of event logs, line by line, to look for suspicious activity or indications that a breach or intrusion has occurred or has been attempted.

## Audit Schedule

In addition to routine monitoring of data within the SIEM tool, manual event log audits will be conducted on a monthly basis, with at least one system audit per month.

Manual audits of event logs both provide an opportunity to identify unusual activity, and enable the organisation to:

* Validate that system event logs are being appropriately captured in line with the event log requirements outlined in this document; and
* Use the event log sample, together with the latest risk assessment, to verify whether the SIEM correlation rules are appropriate and sufficiently adequate to ensure that suspicious activity will be identified as a notable event by the SIEM tool.

# Reporting Requirements

Audits will be undertaken by the IT Security team. Results of event log audits will be reported to the Security Manager, who will brief the Chief Information Security Officer (CISO).

Reports are due to the CISO on the **[Insert Day]** day of each calendar month. Where the **[Insert Day]** day of the month falls on a non-business day, the report will be due on the following business day. Each report will outline key findings from the previous month’s audit, together with recommended actions and progress to date by the relevant action officer(s).

* As a minimum, the report will outline:
* Name of system audited
* Date(s) of audit
* Name of person who undertook the audit
* Details of audit log sample size
* Description of approach taken/audit methodology
* Key Findings
* Action Log & progress to date

# Logging Specifics

Technical details of logging requirements vary depending on the type of operating system and the function or purpose of the server or host.

The following sections outline logging requirements for a selection of operating systems and server types.

## Windows Server - Generic

Any Windows machine that is required to report into the SIEM tool must have the ability to forward events to the SIEM tool, which is configured to pass log data to

Default location of logs: %programdata%\Microsoft\Windows Server\Logs

The event IDs of interest are shown in the following table. These logs need to be available to the IT Security team if the server’s purpose is one of the following: Domain Controller, IIS, File Server, Database.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event Log**  | **Level**  | **ID**  | **Error Name**  | **Source**  |
| Security  | Informational  | 4740  | Account Lockouts  | Microsoft-Windows- Security-Auditing  |
| Security  | Informational  | 4728, 4732, 4756  | User Added to Privileged Group  | Microsoft-Windows- Security-Auditing  |
| Security  | Informational  | 4735  | Security-Enabled Group Modification  | Microsoft-Windows- Security-Auditing  |
| Security  | Informational  | 4724  | Successful User Account Login  | Microsoft-Windows- Security-Auditing  |
| Security  | Informational  | 4625  | Failed User Account Login  | Microsoft-Windows- Security-Auditing  |
| Security  | Informational  | 4648  | Account Login with Explicit Credentials  | Microsoft-Windows- Security-Auditing  |
| System  | Informational  | 104  | Event Log was Cleared  | Microsoft-Windows- EventLog  |
| System  | Informational  | 102  | Audit Log was Cleared  | Microsoft-Windows- EventLog  |
| System  | Informational  | 4719  | System audit policy was changed  | Microsoft-Windows- EventLog  |
| System  | Error  | 1125  | Internal Error  | Microsoft-Windows- GroupPolicy  |
| System  | Error  | 1127  | Generic Internal Error  | Microsoft-Windows- GroupPolicy  |
| System  | Error  | 1129  | Group Policy Application Failed due to Connectivity  | Microsoft-Windows- GroupPolicy |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event Log**  | **Level**  | **ID**  | **Error Name**  | **Source**  |
| Windows Firewall WithAdvancedSecurity/ Firewall  | Informational  | 2004  | Firewall Rule Add  | Microsoft-Windows- Windows FirewallWith Advanced Security  |
| Windows Firewall WithAdvancedSecurity/ Firewall  | Informational  | 2005  | Firewall Rule Change  | Microsoft-Windows- Windows FirewallWith Advanced Security  |
| Windows Firewall WithAdvancedSecurity/ Firewall  | Informational  | 2006, 2033  | Firewall Rules Deleted  | Microsoft-Windows- Windows FirewallWith Advanced Security  |
| Windows Firewall WithAdvancedSecurity/ Firewall  | Error  | 2009  | Firewall Failed to load Group Policy  | Microsoft-Windows- Windows FirewallWith Advanced Security  |

## Windows Server – IIS Generic

In addition to the items listed above, a number of events must also be logged for Windows Server IIS servers, as outlined below.

Default location of IIS logs: %SystemDrive%\inetpub\logs\LogFiles

Logging format should be set to W3C and the following fields need to be enabled to be logged:

|  |  |  |
| --- | --- | --- |
| Date | Method | Bytes received |
| Time | URI Stem | User Agent |
| Client IP Address | URI Query | Cookie |
| Server name | Protocol Status | Referrer |
| Server IP | Bytes Sent |  |

## Windows SQL Server – Generic

In addition to the items listed above, a number of events must also be logged for Windows servers that are running SQL Server, as outlined below.

Default location of logs: %ProgramFiles%\Microsoft SQL Server\MSSQL.1\MSSQL\LOG (this location may vary, depending on the version of SQL server).

Event IDs of interest for SQL server are shown in the following table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event Log**  | **Level**  | **ID**  | **Error Name**  | **Source**  |
| Application  | Informational  | 24001  | Login Succeeded  | Microsoft-Windows- Application  |
| Application  | Informational  | 24003  | Login Failed  | Microsoft-Windows- Application  |
| Application  | Informational  | 24013  | Account Unlocked  | Microsoft-Windows- Application  |
| Application  | Informational  | 24016/24017  | Add member to server role succeeded/failed  | Microsoft-Windows- Application  |
| Application  | Informational  | 24018/24019  | Remove member from server role succeeded/failed  | Microsoft-Windows- Application |
| Application  | Informational  | 24020/24021  | Add member to database role succeeded/failed  | Microsoft-Windows- Application  |
| Application  | Informational  | 24022/24023  | Remove member from database role succeeded/failed  | Microsoft-Windows- Application  |
| Application  | Informational  | 24054  | Started SQL Server  | Microsoft-Windows- Application  |
| Application  | Informational  | 24057  | Stopped SQL Server  | Microsoft-Windows- Application  |

## Linux Server – Generic

Default location of Linux logs: /var/log

Logs of interest for the IT Security team:

|  |  |
| --- | --- |
| **Event Log**  | **Description**  |
| messages  | Global system messages, including those logged during system startup.  |
| secure  | Information about authentication and authorisation privileges.  |
| auth.log  | System authorisation information, including user logins and authentication mechanisms used.  |
| boot.log  | Information logged during the system boot process.  |
| kern.log  | Information logged by the kernel.  |
| faillog  | User failed login attempts.  |
| cron  | Details about scheduled tasks (cron jobs), logged on commencement of the job.  |
| utmp  | User logins, logouts, system events, system status and system boot time.  |
| wtmp  | Historical utmp data.  |
| btmp  | Information about failed login attempts.  |
| lastlog  | Recent login information for users.  |
| dmesg  | Kernel ring buffer information, relating to hardware display or driver messages for hardware devices that the kernel detects during boot process.  |
| Maillog.log  | Messages from the mail server (if any).  |
| daemon.log  | Tracks background services.  |
| audit.log  | Information regarding user read/write activity.  |
| yum.log or dnf.log  | Information logged when a package is installed or removed using yum or dnf. |

Notes: - Log names may vary between Linux distributions.

- Depending on the Linux installation and purpose, additional logs may be required.

In addition, to the logs outlined above,

* If the Linux server is running a web server, the /var/log/httpd (or) var/log/apache2logs must be forwarded to the SIEM tool.
* If the Linux server is running an SQL database, the /var/log/mysqld.log files must be forwarded to the SIEM tool