16.6. Event Monitoring, Logging and Auditing

Objective

16.6.1. Information security related events are logged, monitored and audited for accountability, incident management, forensic and system monitoring purposes.

Context

Scope

16.6.2. This section covers information on the automatic logging of information relating to network activities. Information regarding manual logging of system management activities can be found in Section 16.3 - Privileged User Access. See also Chapter7 - Information Security Incidents.

16.6.3. A security event is a change to normal or expected behaviour of a network, network component, system, device or user. Event logging helps improve the security posture of a system by increasing the accountability of all user actions, thereby improving the chances that malicious behaviour will be detected.

16.6.4. It is important that sufficient details are recorded in order for the logs to be useful when reviewed or when an investigation is in progress. Retention periods are also important to ensure sufficient log history is available. Conducting audits of event logs is an integral part of the security and maintenance of systems, since they will help detect and attribute any violations of information security policy, including cyber security incidents, breaches and intrusions.

References

16.6.5. Additional information relating to event logging is contained in:

Title	Publisher	Source
ISO/IEC 27001	ISO/IEC/ Standards NZ	Standards New Zealand
Standard Time for a New Zealand Network	Measurement Standards Laboratory	MSL NTP Server | Measurement Standards Laboratory

Rationale & Controls

Maintaining system management logs

16.6.6.R.01. **Rationale**

Having comprehensive information on the operations of a system can assist system administration, support information security and assist incident investigation and management. In some cases forensic investigations will rely on the integrity, continuity and coverage of system logs.

16.6.6.R.02. **Rationale**

It will be impractical and costly to store all system logs indefinitely. An agency retention policy may consider:

- Legislative and regulatory requirements;
- Ensure adequate retention for operational support and efficiency;
- Minimise costs and storage requirements; and
- An adequate historical archive is maintained.

Care should be taken to ensure that these considerations are properly balanced.
Some practices dictate retention periods, for example good DNSSEC practice requires log information is stored in log servers for 4 months, then archived and retained for at least 2 years.

16.6.6.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:1997]

Agencies MUST maintain system management logs for the life of a system.

16.6.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1998]

Agencies SHOULD determine a policy for the retention of system management logs.

Content of system management logs

16.6.7.R.01. **Rationale**

Comprehensive system management logs will assist in logging key management activities conducted on systems.

16.6.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2001]

A system management log SHOULD record the following minimum information:

- all system start-up and shutdown;
- all system changes;
- user changes;
- service, application, component or system failures;
- maintenance activities;
- backup and archival activities;
- system recovery activities; and
- special or out of hours activities.

Logging requirements

16.6.8.R.01. **Rationale**

Event logging and monitoring can help raise the security posture of a system by increasing the accountability for all system user actions.

16.6.8.R.02. **Rationale**

Event logging and monitoring can increase the chances that malicious behaviour will be detected by logging the actions of a malicious party.

16.6.8.R.03. **Rationale**

Well configured event logging allows for easier and more effective auditing and forensic examination if an information security incident occurs.

16.6.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2006]

Agencies MUST develop and document logging requirements covering:

- the logging facility, including:
  - log server availability requirements; and
  - the reliable delivery of log information to the log server;
- the list of events associated with a system or software component to be logged; and
- event log protection and archival requirements.

Events to be logged

16.6.9.R.01. **Rationale**

The events to be logged are key elements in the monitoring of the security posture of systems and contributing to reviews, audits, investigations and incident management.

16.6.9.C.01. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:2009]

Agencies MUST log, at minimum, the following events for all software components:

- any login activity or attempts;
- date and time;
- all privileged operations;
- failed attempts to elevate privileges;
- security related system alerts and failures;
- software upgrades and/or software patching;
- system recovery activities;
- system user and group additions, deletions and modification to permissions; and
- unauthorised or failed access attempts to systems and files identified as critical to the organisation.

Additional events to be logged

16.6.10.R.01.

Rationale

The additional events to be logged can be useful for reviewing, auditing or investigating software components of systems.

16.6.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2012]

Agencies SHOULD log the events listed in the table below for specific software components.

Software component	Events to log
Database	System user access to the database.
	Attempted access that is denied.
	Changes to system user roles or database rights.
	Addition of new system users, especially privileged users.
	Modifications to the data.
	Modifications to the format or structure of the database.
Network/operating system	Successful and failed attempts to logon and logoff.
	Changes to system administrator and system user accounts.
	Failed attempts to access data and system resources.
	Attempts to use special privileges.
	Use of special privileges.
	System user or group management.
	Changes to the security policy.
	Service failures and restarts.
	System startup and shutdown.
	Changes to system configuration data.
	Access to sensitive data and processes.
	Data import/export operations.
Web application	System user access to the Web application.
	Attempted access that is denied.
	System user access to the Web documents.
	Search engine queries initiated by system users.

16.6.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2013]

Agencies SHOULD log, at minimum, the following events for all software components:

- Any login activity or attempts; all privileged operations;
- failed attempts to elevate privileges;
- security related system alerts and failures;
- all software updates and/or patching;
- system user and group additions, deletions and modification to permissions; and
- unauthorised or failed access attempts to systems and files identified as critical to the organisation.

Event log facility

16.6.11.R.01. **Rationale**

The act of logging events is not enough in itself. For each event logged, sufficient detail needs to be recorded in order for the logs to be useful when reviewed. An authoritative external time source, a local **Time Source Master Clock or server or** Co-ordinated Universal Time (UTC) is essential for the time-stamping of events and later inspection or forensic examination. The NZ Interoperability Framework (e-GIF) recognises the time standard for New Zealand as UTC (MSL), with Network Time Protocol (NTP) v.4 as the delivery method over the Internet.

16.6.11.R.02. **Rationale**

New Zealand standard time is maintained by the Measurement Standards Laboratory of New Zealand (MSL), a part of Industrial Research Limited (IRL). New Zealand standard time is based on UTC, a worldwide open standard used by all modern computer operating systems. UTC (MSL) is kept within 200 nanoseconds of the international atomic time scale maintained by the Bureau International des Poids et Mesures (BIPM) in Paris.

16.6.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2017]

For each event identified as needing to be logged, agencies MUST ensure that the log facility records at least the following details, where applicable:

- date and time of the event;
- relevant system user(s) or processes;
- event description;
- success or failure of the event;
- event source (e.g. application name); and
- IT equipment location/identification.

16.6.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2018]

Agencies SHOULD establish an authoritative time source.

16.6.11.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2019]

Agencies SHOULD synchronise all logging and audit trails with the time source to allow accurate time stamping of events.

Event log protection

16.6.12.R.01. **Rationale**

Effective log protection and storage (possibly involving the use of a dedicated event logging server) will help ensure the integrity and availability of the collected logs when they are audited.

16.6.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2022]

Event logs MUST be protected from:

- modification;
- unauthorised access; and
- whole or partial loss within the defined retention period.

16.6.12.C.02. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:2023]

Agencies MUST configure systems to save event logs to separate secure servers as soon as possible after each event occurs.

16.6.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2024]

Agencies SHOULD ensure that:

- systems are configured to save event logs to a separate secure log server; and
- event log data is archived in a manner that maintains its integrity.

Event log archives

16.6.13.R.01. **Rationale**

It is important that agencies determine the appropriate length of time to retain DNS, proxy, event systems and other operational logs. Logs are an important information source in reviews, audits and investigations ideally these should be retained for the life of the system or longer.

16.6.13.R.02. **Rationale**

The Archives, Culture, and Heritage Reform Act 2000, the Public Records Act 2005 and the Official Information Act 1982 may determine or influence the length of time that logs need to be retained and if they should be archived.

16.6.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2028]

Event logs MUST be archived and retained for an appropriate period as determined by the agency.

16.6.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2029]

Disposal or archiving of DNS, proxy, event, systems and other operational logs MUST be in accordance with the provisions of the relevant legislation.

16.6.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2030]

Agencies SHOULD seek advice and determine if their logs are subject to legislation.

16.6.13.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2031]

Agencies SHOULD retain DNS, proxy and event logs for a minimum of 12 months.

16.6.13.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7557]

Agencies should prioritise their log retention requirements based on the risks surrounding their most sensitive systems.

Event log auditing

16.6.14.R.01. **Rationale**

Conducting audits of event logs is seen as an integral part of the maintenance of systems, as they will assist in the detection and attribution of any violations of agency security policy, including information security incidents, breaches and intrusions.

16.6.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2034]

Agencies MUST develop and document event log audit requirements covering:

- the scope of audits;
- the audit schedule;
- action to be taken when violations are detected;
- reporting requirements; and
- roles and specific responsibilities.

Event log monitoring

16.6.15.R.01. **Rationale**

Event log monitoring is similar to auditing, however monitoring is conducted in near-real time. This provides early detection of any incidents and potential authentication violations and incidents.

Early identification of anomalies can protect the security posture of a system.

16.6.15.R.02. **Rationale**

Monitoring of event logs is essential to understand what system 'normal' look like to be able to detect future authentication violations and anomalies.

16.6.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7560]

Agencies SHOULD have a monitoring solution implemented that enables detection of incidents as they occur so that appropriate responses can be taken in adequate timeframes.

16.6.15.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7561]

Agencies SHOULD have systems available for processing system event logs to identify and correlate events which indicate behavioural anomalies or potential security compromise in the systems, in a near real-time manner.