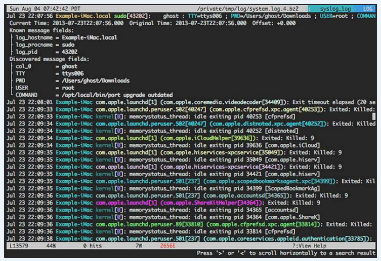
ISO/IEC 27001:2013 Information security management systems
-Logging and monitoring-

Security category – 12.4. Logging and monitoring



Control – 12.4.1. Event logging

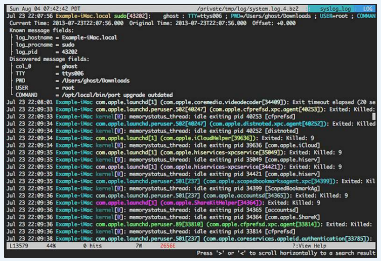
Event logs record user activities, exceptions, faults and security events. The organization should ensure that such logs are produced, kept and regularly reviewed.

Logs are valuable to investigate incidents, events that led to security problems and to determine who is accountable for different activities.

For every information processing facility there should be an event log kept – that is independent and not accessible by the user.

ISO/IEC 27001:2013 Information security management systems
-Logging and monitoring-

Some guidelines for what event logs should refer to:

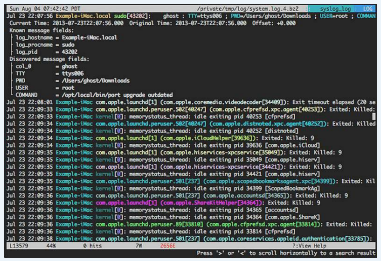


a) user IDs;
b) system activities;
c) dates, times and details of key events, e.g. log-on and log-off;
d) device identity or location if possible;
e) records of successful and rejected system access attempts;
f) changes to system configuration;
g) use of privileges;
h) use of system utilities and applications;
i) files accessed;
j) alarms raised;
k) activation and de-activation of protection systems, such as the anti-virus systems;
l) records of transactions executed by users in applications…

Review of logs should respect the segregation of duty principle.
Logs should be kept for a sufficient period of time so that they can be used if needed for an investigation.

ISO/IEC 27001:2013 Information security management systems
-Logging and monitoring-

Control – 12.4.2. Protection of log information
The organization should protect logging facilities and log information against tampering and unauthorized access.



The information contained in logs is valuable as log as its integrity is preserved.

Controls should aim to protect against unauthorized changes like: editing or deleting the information recorded; modifying the type of information that is being recorded or overwriting logs because storage capacity is exceeded***.***

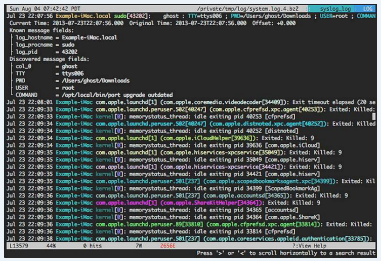
A method to safeguard logs is to copy them in real time to a system outside the control of the system administrator.

ISO/IEC 27001:2013 Information security management systems

-Logging and monitoring-

Control – 12.4.3. Administrator and operator logs

The activities of system administrators and the activities of operators should be logged and the logs should be protected and reviewed regularly.



A user with privileges may be able to manipulate logs so its necessary to employ some protection for such situations.

An intrusion detection system managed outside the control of the administrator is a solution proposed by ISO/IEC 27002 for the control of logs.

ISO/IEC 27001:2013 Information security management systems
-Logging and monitoring-

Control – 12.4.4. Clock synchronization
The clocks of all relevant information processing systems within an organization or security domain should be synchronized to a single reference time source.

An internal reference time should be established, documented and implemented.

Clock synchronization is needed because most logs are time and date stamped.

In most cases – reference time is local time.
For organizations with multiple locations – a reference time should be decided.

All system clocks should be automatically synchronized with a master clock.