ISO 27001 Monitoring and Audit Logging Compliance with ObserveIT

observe it
people audit

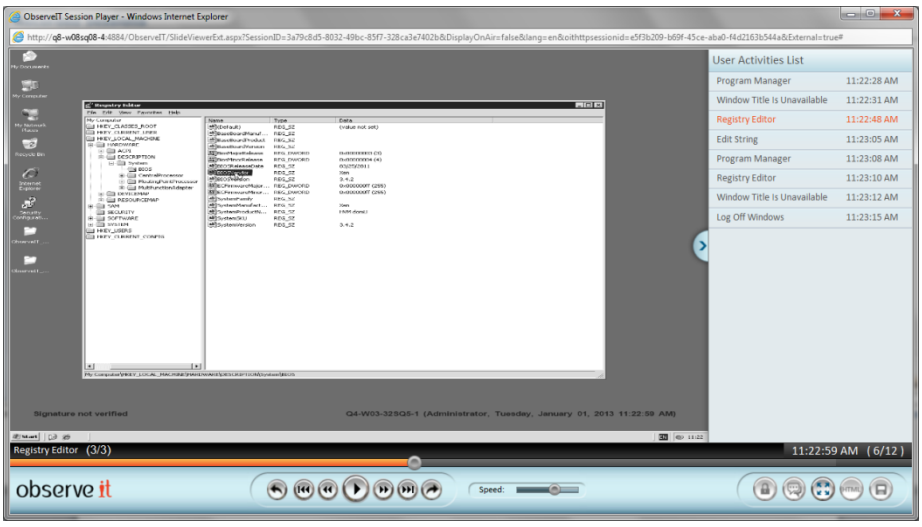
Purpose of this Document

ISO 27001 specifies a wide range of information security governance controls. This document presents a high-level look at how ObserveIT's server session recording solution addresses **Monitoring and Audit Logging** controls. The purpose of this area of the specification is described as: "On-going system monitoring and logging for audit should allow timely detection of and response to unauthorized information processing activities."

What is Session Recording and Logging?

ObserveIT's session recording and logging system generates video recordings of every server session – along with detailed user activity audit logs – providing unparalleled insight into what is being done on company servers. Whereas standard logs collect data on server and network activity, session recordings and logs focus on the *user activity* within the operating system and *every* application (commercial, bespoke, legacy and cloud). This granular, user-focused monitoring capability offers a detailed and invaluable tool with which to understand what administrators and remote vendors are doing on managed servers.

Beyond simply recording videos of user sessions, ObserveIT's session recording systems also generate an easy-to-read summary journal of every application and window accessed by users while logged into company servers. Furthermore, detailed activity data is captured by the system, allowing deep keyword search for any particular action. Searches can locate the names of applications run, windows opened, system commands executed, check boxes clicked, text typed/modified, screen output and nearly every other on-screen event.



Integration with other systems – including log analysis, security information and event monitoring (SIEM), access control and IT ticketing systems – further leverages the value of the session recordings and text logs by making them readily available when and where they are needed.

Learn more about ObserveIT at **www.observeit.com**.

Audit Logging

ISO 27001 requirement: *Audit logs that record user and system activities, exceptions, and information security events should be produced, and kept for an agreed-upon time period, to assist in future investigations and access control monitoring. This could include recording all key events.*

ISO 27001 requirement: *System administrator and system operator activities should be appropriately logged, as part of the general audit trail process.*

ObserveIT's solution:

- ObserveIT generates both visual and textual activity logs of *all* actions performed by *all* users on *all* servers in *all* applications and system areas, with no gaps.
- Auditors can view video recordings of every privileged account login, search for particular sessions using activity-related keywords (e.g., programs run, windows opened, URLs visited, system commands executed, text typed, system settings changed) and review textual activity logs by user or by server.

Monitoring

ISO 27001 requirement: *Procedures for monitoring use of information processing facilities should be established and the results of monitoring activities regularly reviewed. This could include event tracking and recording as specified in the Audit logging policy, and monitoring and review of this data*

ObserveIT's solution:

- Custom alerts can be defined in ObserveIT to immediately notify administrators or IT security staff when the conditions of the alert are met. ObserveIT is unique in that these alerts can be defined using any combination of granular *user activity* criteria, including keyboard input, on-screen text, and entry to particular applications, windows or Web URLs.
- ObserveIT activity logs can be integrated into log management, SIEM and NMS systems for activity monitoring, analytics and alerts in those systems.

Balancing Audit with Operational Requirements

ISO 27001 requirement: *Audit controls should be implemented to allow collection of appropriate audit data on operational systems, while minimizing the risk of disruption to business processes.*

ObserveIT's solution:

- ObserveIT's tiny CPU and RAM footprints ensure that there is no disruption of server performance due to the session recording. When installed on gateways, no software need be installed on actual production servers.
- Session recording can be implemented silently such that users are completely unaware that the auditing system is operating. Alternatively, ObserveIT can display a message to any user logging in to a managed server indicating that recording is occurring and requiring the user's acknowledgment. Despite the extra step, this may be necessary to adhere to local disclosure laws. In any case, when a user knows he is being recorded, he is less likely to engage in frivolous or malicious activity.

Protection of Log Information

ISO 27001 requirement: *Logging facilities and log information should be appropriately protected against tampering and unauthorized access. This could include privacy protection measures for logged data that may be sensitive or confidential; and security protections of a technical, physical and administrative nature to ensure integrity and availability of audit logs.*

ObserveIT's solution:

- ObserveIT can store all session video using industry-standard encryption to prevent someone with direct access to the database from extracting the recorded session data.

- Access to video replay from within the ObserveIT console can be protected with a dual-password (4-eyes) configuration such that even an ObserveIT administrator cannot access recorded videos without an additional password. This secondary password is typically held by legal counsel or employee union representative.
- If the data integrity of ObserveIT's database storage is compromised (for example, if a DBA succeeds in deleting an incriminating screenshot from within the database), ObserveIT provides administrators with a warning about the tampering.

Retention of Log Information

ISO 27001 requirement*: A formal policy should specify the minimum retention periods for log data, consistent with legal-regulatory-certificatory requirements, business needs, and available storage/processing capacities.*

ObserveIT's solution:

- ObserveIT provides both manual and automatic scheduled data archiving according to any preset schedule mandated by the organization.
- Even after the video recordings are archived, textual session data for those recordings will still be found in reports and keyword searches. To replay a particular archived session, then only that individual session need be restored from the archive..