ISO 27001 COMPLIANCE WITH OBSERVEIT

OVERVIEW

ISO/IEC 27001 is a framework of policies and procedures that include all legal, physical and technical controls involved in an organization's information risk management processes. ISO 27001 provides a checklist of controls that should be considered in order to help organizations keep both their information assets and those of their customers secure.

ObserveIT is well positioned to address the majority of the operations security requirements specified under ISO 27001, specifically around logging and monitoring. However, ObserveIT can also help address the majority of the other controls specified within ISO 27001, such as organization of information security, asset management, access control, communications security, and information security incident management.

The document below provides a high-level view of the main controls addressed by ObserveIT aimed at the security and compliance manager. Appendix A provides a detailed list of the reference control objective and controls list (taken from Annex A of ISO 27001) and how ObserveIT can help implement them.

CONTROL OBJECTIVES

Organizations need to define and apply an information security risk treatment process taking account of the risk assessment results and determine all controls that are necessary to implement the security risk treatment options. ISO 27001 provides a list of such controls that need to be reviewed. The major controls addressed by ObserveIT involve logging and monitoring, privacy and access control, and Information security incident management.

LOGGING AND MONITORING

Logging and monitoring is an essential part of the operations security requirements. The main control objective of logging and monitoring is to record events and generate evidence. It requires that event logs of user activities, exceptions, faults and information security events will be produced, kept and regularly reviewed. Furthermore, logging facilities and log information will be protected against tampering and unauthorized access. ObserveIT records all user activity on desktops, in applications, and on servers. The recorded sessions and logs are stored and encrypted in the database with access controls on who can view the data and the recordings.

The standard also requires that all administrative actions and configuration are logged and that the logs are protected and regularly reviewed. All administrative activity within the ObserveIT server is collected and securely stored for this purpose.

At the same time, the ISO standard point outs that it is important to minimize the impact of audit activities on operational systems and business processes. Unlike proxy-based products that require changes to network configuration, and force administrators to go through a proxy, ObserveIT records activities in the background of the servers and has no impact on how administrators interact with the systems.

ACCESS CONTROLS

The ISO standard explicitly requires that access to information be limited, and that users shall only be provided with access to the network and services that they have been specifically authorized to use. ObserveIT supports this requirement by providing a jump server architecture option that allows you to restrict access to network devices to only go through a monitored server that records all activities. Access is limited through integration with a service desk that requires an active service ticket from the users in order to log in.

The standard also requires the review of user access rights at regular intervals. ObserveIT keeps a detailed record of all user activities and can augment identity governance and entitlement certification processes with information about what users actually performed. This is important because it provides managers with information that helps them make an informed decision on whether users need to have the access that they've been granted.

PRIVACY

Privacy and protection of personally identifiable information is a key requirement in ISO 27001 and is also gaining traction with many legislation initiatives. ISO 27001 requires that the privacy and protection of personally identifiable information will be ensured as required in relevant legislation and regulation. ObserveIT strictly protects personal information of its monitored subjects.

- Users that are being recorded can get a notification that they are being recorded so that they can limit the usage of personal applications.
- Personal applications can be scoped out of monitoring.
- Restricting the recording to activity logs only: This provides visibility into what users are doing (including search, alert and report) without taking screenshots. For example, it enables an ObserveIT administrator to know that a user accessed his bank account, but without details about the account.
- Session reviews can be restricted to specific roles and users.
- Four-eye enforcement can be applied to supervise the process of sessions being opened and viewed.
- Key logging can be configured so that passwords are not recorded. Information is also hashed and cannot be decrypted.

INFORMATION SECURITY INCIDENT MANAGEMENT

The Information security incident management section of ISO 27001 requires a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. The organization is required to define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence. ObserveIT's recorded sessions and user activity logs are stored securely and provide un-repudiated, forensic evidence on exactly what happened during an incident. Customers have used ObserveIT for legal and forensics purposes.

OTHER SECURITY CONTROLS

ObserveIT can address many additional control objectives specified in ISO 27001:

- **Change management** - ObserveIT is integrated into service management tools, such as Remedy and Service Now, to require an approved ticket before providing access to systems.
- **Separation of development, testing and operational environments** - ObserveIT monitors developers and support access to production environments allowing transparent access with proper governance.
- **Segregation of duties** - ObserveIT can alert on violations of segregation of duties policies. For example, when a SalesForce.com administrator approves a quote.
- **Asset management** - ObserveIT provides a detailed activity log of assets used by users including desktops, servers, and applications being accessed. The information can be collected through reports and can augment information received from Identity management or asset management systems by providing the actual use of these assets by the users.
- **Communications Security** - ObserveIT records all activity on the systems, including granular recording of SFTP communications and commands on servers, as well as messaging application communication on desktops.
- **Outsourced development Control** - ObserveIT is used broadly to monitor outsourced developers and contractors.

SUMMARY

ObserveIT provides a broad coverage of the controls defined in ISO 27001. While mostly aligned to logging, monitoring, and incident management, ObserveIT can be used to address many additional controls. Please refer to Appendix A for the full and comprehensive list of controls and how ObserveIT can address them.

APPENDIX 1 - REFERENCE CONTROL OBJECTIVE AND CONTROLS

Annex A of ISO 27001 contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to annex A in order to ensure that no necessary controls are overlooked. Control objectives are implicitly included in the controls chosen.

The *ObserveIT Implementation* Fields describes how ObserveIT can help address the implementation of these controls. The compliance of this standard requires a complete set of security tools and procedures. In the table below we only bring the segments that are relevant for ObserveIT.

A.6 Organization of information security		
A.6.1 Internal Organization		
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.2 Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of an organization's assets.	*ObserveIT Implementation* ObserveIT can alert on violations of segregation of duties policies. For example, when a SalesForce.com administrator approves a quote. By using ticketing integration with Service Now, Remedy etc. Access to servers can be restricted only to users that have the TicketID. With this integration, organizations can also implement access control and provide access only to permitted users.
A.6.2 Mobile device and teleworking		
Objective: To ensure the security of teleworking and use of mobile devices.		
A.6.2.2 Teleworking	*Control* A policy and supporting security measures shall be implemented to protect information accessed, processed or sored at teleworking sites.	*ObserveIT Implementation* ObserveIT monitors and records teleworking workstations to oversee the access of customer and personal information by teleworking employees.

A.7 Human resource security		
A.7.2 During employment		
Objective: To ensure that employees and contractors are aware of and fulfill their information security responsibilities.		
A.7.2.2 Information security awareness, education and training	*Control* All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	*ObserveIT Implementation* ObserveIT can notify employees of the security policy relating to the workstation they are logging in to and require acknowledgement of receiving the policy prior to allowing access to the machine. Live messages can be sent directly to the end user machine notifying them to stop any out of policy activities. The message can block, as well as prevent the user from taking further actions.
A.7.2.3 Disciplinary process	*Control* There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	*ObserveIT Implementation* ObserveIT can provide alerts when the policy is violated and provides the forensics evidence needed in case of a security information breach that results in a disciplinary action against an employee or contractor.
A.8 Asset Management		
A.8.1 Responsibility for assets		
Objective: To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1 Inventory of assets	*Control* Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	*ObserveIT Implementation* ObserveIT provides a detailed activity log of assets used by users including desktops, servers, and applications being accessed. The information can be collected through reports and can augment information received from identity management or asset management systems by providing the actual use of these assets by the users.
A.8.1.3 Acceptable use of	*Control* Rules for the acceptable use of information and of assets associated with	*ObserveIT Implementation* ObserveIT can help enforce the acceptable use of information and assets. ObserveIT

assets	information and information processing facilities shall be identified, documented and implemented.	obtains a detailed record of the use of the information and assets by users, and can alert on violations.
A.9 Access Control		
A.9.1 Business requirements of access control		
Objective: To limit access to information and information processing facilities.		
A.9.1.2 Access to networks and network services	*Control* Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	*ObserveIT Implementation* Ticketing system integration, Secondary Authentication, and blocking messages enhance the access controls on the network. Also, ObserveIT implementation as a jump server allows you to restrict access to network devices to only go through the jump server. All access would be recorded and through integration with a service desk application you can limit access based on an active approved service ticket.
A.9.2 User access management		
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.		
A.9.2.5 Review of user access rights	*Control* Asset owners shall review users' access rights at regular intervals.	*ObserveIT Implementation* ObserveIT keeps a detailed record of all user activities and can augment the entitlement certification process with information about what users actually performed, not only what they can theoretically performed based on their access rights. Alerts can be triggered in real time when entitlements are being changed in applications. This is important because it provides managers with information that helps them make an informed decision on whether users need to have the access being reviewed.
A.9.4 System and application access control		
Objective: To prevent unauthorized access to systems and applications.		
A.9.4.4	*Control*	*ObserveIT Implementation*

Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	ObserveIT is built to monitor all privileged user access. More specifically, it can monitor the use of privileged applications such as SUID programs on Unix and Linux. Alerts can be set to notify of suspicious program activities such as changing configurations or data access in real-time.
A.12 Operations security		
A.12.1 Operational procedures and responsibilities		
Objective: To ensure correct and secure operations of information processing facilities.		
A.12.1.2 Change management	*Control* Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	*ObserveIT Implementation* ObserveIT is integrated into service management tools such as Remedy, and Service Now to require an approved ticket before providing access to systems. The ObserveIT application itself fully audits all administrative changes, health events, and attempts to tamper with the agent.
A.12.1.4 Separation of development, testing and operational environments	*Control* Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	*ObserveIT Implementation* ObserveIT Ticketing integration can enforce separation of access only to permitted users. Users that are not permitted to login to a machine will not be able to access and work on the servers.
A.12.4 Logging and monitoring		
Objective: To record events and generate evidence.		
A.12.4.1 Event logging	*Control* Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	*ObserveIT Implementation* ObserveIT records all user activity on the desktops, in applications, and on servers.
A.12.4.2 Protection of log information	*Control* Logging facilities and log information shall be protected against tampering and unauthorized access	*ObserveIT Implementation* Recorded video sessions are stored encrypted in the database with access controls on who can view the data and the

		recordings.
A.12.4.3 Administrator and operator logs	*Control* System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	*ObserveIT Implementation* All administrative activity within the ObserveIT server is collected and securely stored.
A.12.4.4 Clock synchronization	*Control* The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	*ObserveIT Implementation* The ObserveIT system synchronizes clocks across of its server and agents and also protects against session replay attacks that may be attempted.
A.12.7 Information systems audit considerations		
Objective: To minimize the impact of audit activities on operational systems.		
A.12.7.1 Information systems audit controls	*Control* Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.	*ObserveIT Implementation* Unlike proxy based products that require changes to network configuration routing the networking via the proxy, and forcing administrators to go through a proxy, ObserveIT records activities on the servers in the backgrounds and has minimal impact on operational activities.
A.13 Communications security		
A.13.2 Information transfer		
Objective: To maintain the security of information transferred within an organization and with any external entity.		
A.13.2.1 Information transfer policies and procedures	*Control* Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	*ObserveIT Implementation* ObserveIT records all activity on the systems, including granular recording of SFTP communications and commands. This allows for effective enforcement of the information transfer policies and procedures. *ObserveIT Compliance* Sessions can be exported from ObserveIT and shared with 3rd party. Those sessions

		are protected by password. All internal communication within the product is encrypted with SSL.
A.13.2.3 Electronic messaging	*Control* Information involved in electronic messaging shall be appropriately protected.	*ObserveIT Implementation* ObserveIT installed on desktops will capture, and record messenger communication. This allows for effective enforcement of the information transfer policies and procedures. *ObserveIT Compliance* Sessions can be exported from ObserveIT and shared with a 3rd party. Those sessions are protected by password.
A.14 System acquisition, development and maintenance		
A.14.2 Security in development and support processes		
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.		
A.14.2.7 Outsourced development	*Control* The organization shall supervise and monitor the activity of out- sourced system development.	*ObserveIT Implementation* ObserveIT is used broadly to monitor outsource developer and contractors.
A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.7 Collection of evidence	*Control* The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	*ObserveIT Implementation* ObserveIT's recorded sessions and logs are stored securely and provide un repudiated, forensic evidence on exactly what happened during an incident. Secondary authentication ensures the accountability of the activity even when shared accounts are being used.
A.17 Information security aspects of business continuity management		
A.17.1 Information security continuity		

<table>
<tr><td colspan="3">Objective: Information security continuity shall be embedded in the organization's business continuity management systems.</td></tr>
<tr><td colspan="3">ObserveIT Compliance

ObserveIT is built to support a for disaster recovery architecture with a secondary site consciously collecting the recorded information so that in case of a catastrophic event, the recorded activities and logs are secure.</td></tr>
<tr><td colspan="3">A.17.2 Redundancies</td></tr>
<tr><td colspan="3">Objective: To ensure availability of information processing facilities..</td></tr>
<tr><td colspan="3">ObserveIT Compliance

ObserveIT is built to support a high availability architecture that ensures uptime in case of application or hardware failure and ensures that recorded sessions and logs are not lost.</td></tr>
<tr><td colspan="3">A.18 Compliance</td></tr>
<tr><td colspan="3">A.18.1 Compliance with legal and contractual requirements</td></tr>
<tr><td colspan="3">Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.</td></tr>
<tr><td>A.18.1.3

Protection of records</td><td>Control

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.</td><td>ObserveIT Implementation

ObserveIT recorded video sessions are stored encrypted and protected from un-authorized access. There is a strict auditing monitor who has access to the session information.

Only permitted users that have access to the ObserveIT Web Console can view sessions and search in the user activity database</td></tr>
<tr><td>A.18.1.4

Privacy and protection of personally identifiable information</td><td>Control

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.</td><td>ObserveIT Implementation

ObserveIT strictly protects personal information of its monitored subjects.

▪ Users that are being recorded can get a notification that they are being recorded so that they can limit the usage of personal applications.

▪ Personal applications can be scoped out of monitoring.

▪ Restricting the recording to activity logs only: This provides visibility into</td></tr>
</table>

		what users are doing (including search, alert and report) without taking screenshots. It allows for example to know that a user accessed his bank account, but without details about the account. ▪ Sessions review can be restricted to specific roles and users. ▪ 4-eye enforcement can be applied to supervise the process of sessions being opened and viewed. ▪ Key logging can be configured so that passwords will not be recorded. Information is also hashed and cannot be decrypted.