netwrix

SOX Controls

and Netwrix Auditor Mapping

About SOX

All public companies in the U.S. are subject to Sarbanes Oxley (SOX) compliance without exceptions. SOX compliance requirements also apply to overseas operations of U.S. public companies and international companies listed on U.S. exchanges.

SOX requires all listed companies to adopt Internal Controls over Financial Reporting (ICFR) and establish internal auditing of the adopted ICFR. The Sarbanes-Oxley Act does not provide any specific recommendations for implementation of internal controls; instead, it requires organization to adopt a “recognized control framework”.

...

Please note that the efforts and procedures required to establish compliance in each section may vary in different organizations depending on their systems configuration, internal procedures, nature of business, and other factors.

Implementation of the described controls will not guarantee organizational compliance. Not all the controls that Netwrix can possibly support are included. This mapping should be used as a reference guide for implementation of an organization tailored policies and procedures.

Mapping of Processes and Report Categories to SOX Controls

Based on interpretations of COSO & Cobit 4.1 recommendations

AI3: Acquire and Maintain Technology Infrastructure (COSO: Control Activities)		
Control	**How to Comply?**	**Processes and Report Categories**
AI3.2 Infrastructure Resource Protection and Availability	Provide continuous change and configuration auditing and evaluation during configuration, integration and maintenance of hardware and software infrastructure to protect resources and ensure availability and integrity.	Integrity Monitoring System Integrity Data Integrity Policy Changes Configuration Management Configuration Changes Configuration States Access Control System Access User Activity
AI3.4 Feasibility Test Environment	Document all configurations and changes made in test environments for later replication in production environments.	Configuration Management Configuration Changes Configuration States
AI3.3 Infrastructure Maintenance	Monitor and report on changes in infrastructure systems to make sure they are controlled in line with the organization's change management procedures.	Configuration Management Configuration Changes Configuration States Privileged Users Management User Activity

AI6: Manage Changes (COSO: Control Activities, Risk Assessment, Monitoring)		
AI6.1 Change Standards and Procedures And AI6.3: Emergency Changes	Make sure no change goes undocumented. Even if your organization already has specialized management tools for making changes there is a chance that these tools can be bypassed in emergency situations and required changes would be made directly into the system. The Netwrix platform captures all changes at the system level, no matter what management tool is used.	Configuration Management Configuration Changes Configuration States All Changes Audit Trail All Changes

AI6.4: Change Status Tracking and Reporting	Netwrix Auditor provides means to automatically document and report on all changes in system components, ensuring that approved changes are implemented as planned, and, most importantly, no unauthorized changes take place.	Configuration Management All Changes
AI6.5: Change Closure and Documentation	Whenever changes are applied, the associated system and user documentation and procedures must be updated accordingly. The Netwrix platform makes it easy to review all changes and make sure that all related aspects are reflected in the documentation.	Audit Trail All Changes

AI7: Install and Accredit Solutions and Changes (COSO: Control Activities, Information and Communication, Monitoring)		
AI7.4: System and Data Conversion	Establishing and subsequently recreating baselines for operations, internal control procedures, and security practices is greatly simplified by having complete audit trail of all configurations and changes across the entire IT infrastructure available.	Configuration Management Configuration States Permission States Policy States Audit Trail All Changes
AI7.7: Final Acceptance Test	The outcome of the testing process can be easily evaluated through review of changes in infrastructure components by business process owners and IT stakeholders.	Audit Trail All Changes
AI7.8: Promotion to Production	Full record of changes implemented in production environments can be reviewed to ensure it is in line with the implementation plan. Audit trails can be compared with those generated in the test environments to make sure everything went as planned.	Configuration Management Configuration States Permission States Policy States Audit Trail Configuration Changes Configuration States All Changes

AI7.9: Post-implementation Review	Simplify burden of post-implementation review by audit of trails collected by Netwrix platform optionally utilizing Review Status reporting mechanism of Netwrix Auditor.	Audit Trail All Changes Configuration Management All Changes

DS3: Manage Performance and Capacity (COSO: Control Activities, Monitoring)		
DS3.4 IT Resources Availability And DS3.5: Monitoring and Reporting	Netwrix Auditor enables visibility that helps to monitor and quickly assess critical changes. Variety of reports and configuration snapshots can be used to effectively assess and mitigate performance and availability of resources.	Access Control System Access Data Governance Data Access Permission Changes Permission States Audit Trail User Activity

DS4: Ensure Continuous Service (COSO: Control Activities, Information and Communication, Control Environment)		
DS4.3: Critical IT Resources	In addition to auditing of changes within critical IT infrastructure for detection and mitigation of malicious changes. Netwrix Auditor provides quick object-level and attribute-level recovery capabilities for Active Directory.	Integrity Monitoring System Integrity Data Integrity Policy Changes Access Control System Access Data Access

DS5: Ensure Systems Security (COSO: Control Activities, Information and Communication, Monitoring)		
DS5.3: Identity Management	Complete auditing of user accounts and associated activities to identify violations. Compare audit trail with HR records. Audit of disabled accounts, automated de-provisioning of inactive users, audit all operations with user accounts.	Account Management Account Changes Account States Credentials Management Password Changes Password Policy Changes

DS5.4: User Account Management	Audit all changes to user accounts, elevation of privileges, regular and privileged users' activities.	Account Management Account Changes Account States Policy Changes Policy States
DS5.5: Security Testing, Surveillance and Monitoring	Fully featured auditing, reporting and alerting of all user activities including access to sensitive data, across the entire IT infrastructure, recording of who changed what, when, and where, monitoring for detection or prevention of violations. All interactive user activity on the critical systems can be recorded, indexed, archived and made readily available for review.	Integrity Monitoring System Integrity Data Integrity Audit Trail User Activity

DS9: Manage the Configuration (COSO: Control Activities)		
DS9.1 Configuration Repository and Baseline And DS9.2 Identification and Maintenance of Configuration Items And DS9.3 Configuration Integrity Review	Utilize Netwrix Auditor AuditArchive™ - single repository that stores all configurations states and changes, providing reference, rollback feature and reporting capabilities for management and review of system configurations.	Configuration Management All Changes Configuration States Permission States Policy States Configuration Changes

DS10: Manage Problems (COSO: Control Activities, Information and Communication, Monitoring)		
DS10.2: Problem Tracking and Resolution	Refer to the audit trail provided by Netwrix Auditor to analyze and track problems and investigate and determine root cause.	Audit Trail

DS13: Manage Operations (COSO: Control Activities, Information and Communication)		
DS13.3: IT Infrastructure Monitoring	Rely on Netwrix Auditor to collect chronological data on all changes and configuration states across the entire IT infrastructure. This allows reconstruction, review, and analysis of the IT systems operations.	Audit Trail

Control Processes and Report Categories

Control Processes Facilitated by Netwrix Auditor

From the compliance perspective, IT operations can be viewed and managed as a collection of control processes. Such processes allow focusing organizational efforts on a specific area of IT, enforcing certain policies, and establishing particular set of compliance controls. While control processes can be seen as separate entities for the purposes of implementation and management simplicity, in fact all these processes are deeply interconnected and often intrinsic to many regulations and best practices frameworks.

Access Control
Account Management
Credentials Management
Privileged Users Management
Integrity Monitoring
Configuration Management
Data Governance
Audit Trail

Netwrix Auditor Report Categories

For better efficiency and more focused approach to the audit data processing, Netwrix Auditor reports are classified into the following categories:

Account Changes
Account States
All Changes
All States
Configuration Changes
Configuration States
Data Access
Data Changes
Data Integrity
Data States
Group Membership Changes
Group Membership States
Password Changes
Password Policy Changes
Permission Changes
Permission States
Policy Changes
Policy States
Security Changes
System Integrity
System Access
User Activity

Access Control

Process for establishing selective restrictions of access to information systems and data.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	Recently Enabled Accounts	Active Directory	Primary
Account Changes	User Account Status Changes	Active Directory	Secondary
Account States	Accounts with Most Logon Activity	Active Directory	Primary
Account States	Temporary User Accounts	Active Directory	Primary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
Account States	User Accounts	Active Directory	Secondary
Account States	User Accounts - Expired	Active Directory	Secondary
Account States	User Accounts - Locked	Active Directory	Secondary
All Changes	All Active Directory Changes by Group	Active Directory	Secondary
All Changes	All Events by Source	Event Log	Primary
All Changes	Local Users and Groups Changes	Windows Server	Primary
Configuration Changes	Organizational Unit Changes	Active Directory	Secondary
Configuration Changes	User Account Locks and Unlocks	Event Log	Primary
Configuration Changes	Address List Changes	Exchange	Secondary
Configuration Changes	Interactive Logon Setting Changes	Group Policy	Primary
Configuration States	Organizational Units	Active Directory	Secondary
Data Access	All Exchange Server Non-Owner Mailbox Access Events	Exchange	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events by User	Exchange	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Access to Archive Data	File Servers	Primary
Data Access	Data Access Surges	File Servers	Primary
Data Access	Excessive Access Permissions	File Servers	Primary
Data Access	Successful File Reads	File Servers	Secondary
Data Access	Data Access	Oracle Database	Primary
Data Access	SharePoint Read Access	SharePoint	Primary
Data Access	Data Access	SharePoint Online	Primary
Data Changes	SharePoint Content Changes by User	SharePoint	Secondary
Data Changes	All SQL Server Data Changes	SQL Server	Secondary
Data Integrity	Exchange Online Public Folder Changes	Exchange Online	Primary
Data Integrity	Failed Change Attempts	File Servers	Primary
Data Integrity	Failed Read Attempts	File Servers	Primary
Data Integrity	Share Changes	File Servers	Secondary
Group Membership Changes	Distribution Group Changes	Active Directory	Primary

Group Membership Changes	Security Group Membership Changes	Active Directory	Primary
Group Membership Changes	Administrative Group Membership Changes	Active Directory	Secondary
Group Membership Changes	Exchange Online Group Changes	Exchange Online	Primary
Group Membership Changes	Group Membership by User	File Servers	Primary
Group Membership States	Effective Group Membership	Active Directory	Primary
Group Membership States	Group Members	Active Directory	Primary
Group Membership States	Administrative Group Members	Active Directory	Secondary
Group Membership States	User Accounts - Group Membership	Active Directory	Secondary
Password Changes	Password Resets by Administrator	Active Directory	Secondary
Password Changes	User Password Changes	Active Directory	Secondary
Password Policy Changes	Password Policy Changes	Group Policy	Secondary
Permission Changes	Exchange Online Mail User Changes	Exchange Online	Primary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	Permissions Changes	File Servers	Primary
Permission Changes	SharePoint Permissions Changes by User	SharePoint	Primary
Permission States	Account Permissions	File Servers	Primary
Permission States	Object Permissions by Object	File Servers	Primary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
Policy Changes	User Rights Assignment Policy Changes	Group Policy	Primary
Policy Changes	Account Policy Changes	Group Policy	Secondary
Policy Changes	User Configuration Changes	Group Policy	Secondary
Policy States	Account Policies	Group Policy	Secondary
Security Changes	All Security Events by User	Event Log	Secondary
Security Changes	Renaming of Administrator and Guest Accounts Through Group Policy	Group Policy	Secondary
System Access	Activity Outside Business Hours	Active Directory	Primary
System Access	All Logon Activity	Active Directory	Primary
System Access	Failed Logons	Active Directory	Primary
System Access	Interactive Logons	Active Directory	Primary
System Access	Logons by Multiple Users from Single Endpoint	Active Directory	Primary
System Access	Logons by Single User from Multiple Endpoints	Active Directory	Primary
System Access	Successful Logons	Active Directory	Primary
System Access	User Accounts - Last Logon Time	Active Directory	Primary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
System Access	Azure AD Logon Activity	Azure AD	Primary
System Access	Failed Logon Attempts	Event Log	Primary
System Access	Logoffs by User	Event Log	Primary
System Access	Remote Desktop Sessions	Event Log	Primary
System Access	Successful Logons by User	Event Log	Primary
System Access	Wireless Network Policy Changes	Group Policy	Primary
System Access	All Oracle Database Logons	Oracle Database	Primary

System Access	All SQL Server Logons	SQL Server	Primary
User Activity	All Exchange Server Changes by User	Exchange	Secondary
User Activity	File Server Changes by User	File Servers	Primary
User Activity	All File Server Activity by User	File Servers	Secondary
User Activity	All SQL Server Activity by User	SQL Server	Primary
User Activity	All User Activity by User	User Activity	Primary
User Activity	All Windows Server Changes by User	Windows Server	Secondary

Account Management

Process for issuing, removing, maintaining and configuring information systems' accounts and related privileges.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	Computer Account Changes	Active Directory	Primary
Account Changes	Contact Object Changes	Active Directory	Primary
Account Changes	Recently Enabled Accounts	Active Directory	Primary
Account Changes	User Account Changes	Active Directory	Primary
Account Changes	User Account Status Changes	Active Directory	Primary
Account Changes	User Account Management in Azure AD	Azure AD	Primary
Account Changes	User Accounts Created and Deleted Directly in Azure AD	Azure AD	Primary
Account Changes	User-Initiated Password Changes in Azure AD	Azure AD	Primary
Account Changes	Account Management	Oracle Database	Primary
Account States	Accounts with Most Logon Activity	Active Directory	Primary
Account States	Organizational Unit Accounts	Active Directory	Primary
Account States	Service Principal Names of Computer Accounts	Active Directory	Primary
Account States	User Accounts	Active Directory	Primary
Account States	User Accounts - Expired	Active Directory	Primary
Account States	User Accounts - Locked	Active Directory	Primary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
Configuration Changes	User Account Locks and Unlocks	Event Log	Secondary
Configuration States	Computer Accounts	Active Directory	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events	Exchange	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events by User	Exchange	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Excessive Access Permissions	File Servers	Primary
Data States	Potential Data Owners by Folder	File Servers	Primary

Data States	Top Owners by Total File Size	File Servers	Secondary
Group Membership Changes	Group Membership Changes in Azure AD	Azure AD	Primary
Group Membership Changes	Exchange Online Group Changes	Exchange Online	Primary
Group Membership Changes	Group Membership by User	File Servers	Primary
Group Membership States	Temporary Users in Privileged Groups	Active Directory	Primary
Group Membership States	User Accounts - Group Membership	Active Directory	Primary
Group Membership States	Users Not in Any Distribution Group	Active Directory	Primary
Group Membership States	Effective Group Membership	Active Directory	Secondary
Group Membership States	Group Members	Active Directory	Secondary
Permission Changes	Privilege Management	Oracle Database	Primary
Permission States	Account Permissions	File Servers	Primary
Policy Changes	Account Policy Changes	Group Policy	Primary
Policy Changes	User Configuration Changes	Group Policy	Primary
Policy States	Account Policies	Group Policy	Primary
System Access	Failed Logons	Active Directory	Primary
System Access	Successful Logons	Active Directory	Primary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
User Activity	User Activity Summary	File Servers	Primary

Credentials Management

Process for management of credential information such as user names and passwords.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	User-Initiated Password Changes in Azure AD	Azure AD	Primary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
Password Changes	Password Resets by Administrator	Active Directory	Primary
Password Changes	User Password Changes	Active Directory	Primary
Password Policy Changes	Password Policy Changes	Group Policy	Primary

Privileged Users Management

Process for management of privileged accounts, including their provisioning and life cycle management, authentication, authorization, credentials management, auditing, and access control.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	User Account Changes	Active Directory	Secondary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
All Changes	All System Events by User	Event Log	Secondary
All Changes	Exchange Database Changes	Exchange	Secondary
All Changes	New Exchange Servers	Exchange	Secondary
All Changes	All Exchange Server Changes by Date	Exchange Online	Primary
All Changes	All Oracle Database Administrative Activity	Oracle Database	Primary

All Changes	All User Activity	User Activity	Secondary
All Changes	All VMware Changes by User	VMware	Secondary
All Changes	Local Users and Groups Changes	Windows Server	Secondary
Configuration Changes	Active Directory Schema Container Changes	Active Directory	Secondary
Configuration Changes	Mailbox Changes	Exchange	Secondary
Configuration Changes	Exchange Online Management Role Changes	Exchange Online	Primary
Configuration Changes	Interactive Logon Setting Changes	Group Policy	Secondary
Configuration Changes	DNS Configuration Changes	Windows Server	Secondary
Configuration Changes	DNS Resource Record Changes	Windows Server	Secondary
Configuration Changes	General Computer Settings Changes	Windows Server	Secondary
Configuration Changes	Programs Added and Removed	Windows Server	Secondary
Configuration Changes	Windows Registry Changes	Windows Server	Secondary
Data Integrity	Files and Folders Deleted	File Servers	Secondary
Group Membership Changes	Administrative Group Membership Changes	Active Directory	Primary
Group Membership Changes	Security Group Membership Changes	Active Directory	Secondary
Group Membership Changes	Exchange Online Group Changes	Exchange Online	Primary
Group Membership States	Administrative Group Members	Active Directory	Primary
Group Membership States	Temporary Users in Privileged Groups	Active Directory	Primary
Permission Changes	Mailbox Delegation and Permissions Changes	Exchange	Secondary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	Privilege Management	Oracle Database	Primary
Permission Changes	VMware Virtual Machine Permissions Changes	VMware	Secondary
Permission States	Group Policy Object Delegation	Group Policy	Secondary
Policy Changes	Email Address Policy Changes	Exchange	Secondary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
Policy Changes	Administrative Template Changes	Group Policy	Primary
Policy Changes	Restricted Groups Policy Changes	Group Policy	Primary
Policy Changes	Public Key Policy Changes	Group Policy	Secondary
Policy Changes	User Rights Assignment Policy Changes	Group Policy	Secondary
Security Changes	Security Group Changes	Active Directory	Secondary
Security Changes	Renaming of Administrator and Guest Accounts Through Group Policy	Group Policy	Primary
Security Changes	Security Settings Changes	Group Policy	Secondary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
System Access	Failed Logon Attempts	Event Log	Secondary
System Access	Logoffs by User	Event Log	Secondary
System Access	Remote Desktop Sessions	Event Log	Secondary
System Access	Successful Logons by User	Event Log	Secondary
User Activity	All Active Directory Changes by User	Active Directory	Secondary
User Activity	All Changes by User	All Audited Systems	Secondary
User Activity	All Events by User	Event Log	Secondary

User Activity	All Exchange Server Changes by Group	Exchange	Secondary
User Activity	File Server Changes by User	File Servers	Secondary
User Activity	All Group Policy Changes by Group	Group Policy	Secondary
User Activity	All SharePoint Changes by User	SharePoint	Secondary
User Activity	All SQL Server Activity by User	SQL Server	Secondary
User Activity	All User Activity by User	User Activity	Secondary

Integrity Monitoring

Process for performing validation of data and configurations integrity by comparing between the current state and the known, good baseline.

Report Category	Netwrix Auditor Report	Audited System	Priority
Account States	Accounts with Most Logon Activity	Active Directory	Primary
Account States	User Accounts - Passwords Never Expire	Active Directory	Primary
All Changes	All Active Directory Changes by Date	Active Directory	Primary
All Changes	All Active Directory Changes by Object Type	Active Directory	Secondary
All Changes	All Changes by Server	All Audited Systems	Secondary
All Changes	All Exchange Server Changes by Server	Exchange	Secondary
All Changes	All Exchange Server Changes by Date	Exchange Online	Primary
All Changes	All SharePoint Changes by Site Collection	SharePoint	Secondary
All Changes	All SQL Server Activity by Server	SQL Server	Secondary
All Changes	All VMware Changes by Server	VMware	Secondary
All Changes	All Windows Server Changes by Date	Windows Server	Primary
All Changes	All Windows Server Changes by Server	Windows Server	Secondary
Configuration Changes	Active Directory Schema Container Changes	Active Directory	Primary
Configuration Changes	All Exchange Server Changes by Object Type	Exchange	Secondary
Configuration Changes	VMware Cluster Changes	VMware	Secondary
Configuration Changes	VMware Snapshot Changes	VMware	Secondary
Configuration Changes	Programs Added and Removed	Windows Server	Primary
Configuration Changes	Service Changes	Windows Server	Primary
Configuration Changes	Windows Registry Changes	Windows Server	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Excessive Access Permissions	File Servers	Primary
Data Access	SharePoint Read Access	SharePoint	Primary
Data Changes	File Server Changes by Action	File Servers	Secondary
Data Changes	Folder Changes	File Servers	Secondary
Data Integrity	Potentially Harmful Files - Activity	File Servers	Primary
Data Integrity	Potentially Harmful Files on File Shares	File Servers	Primary
Data Integrity	All File Server Activity by Action Type	File Servers	Secondary

Data Integrity	All File Server Activity by Server	File Servers	Secondary
Data Integrity	Failed Change Attempts	File Servers	Secondary
Data Integrity	Failed Delete Attempts	File Servers	Secondary
Data Integrity	File Server Changes by Server	File Servers	Secondary
Data Integrity	Creation of Files with Sensitive Data	File Servers, SharePoint	Primary
Data Integrity	File Names Containing Sensitive Data	File Servers, SharePoint	Primary
Data States	Potential Data Owners by Folder	File Servers	Primary
Data States	Files and Folders by Owner	File Servers	Secondary
Data States	Largest Files	File Servers	Secondary
Policy Changes	Registry Policy Changes	Group Policy	Primary
Policy Changes	Software Restriction Policy Changes	Group Policy	Primary
Security Changes	Object Security Changes	Active Directory	Secondary
Security Changes	Operations Master Role Changes	Active Directory	Secondary
System Access	All Logon Activity	Active Directory	Primary
System Access	Failed Logons	Active Directory	Primary
System Access	Interactive Logons	Active Directory	Primary
System Access	Successful Logons	Active Directory	Primary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
System Access	Wireless Network Policy Changes	Group Policy	Secondary
System Integrity	Service Pack Installations	Active Directory	Primary
System Integrity	Event Details	Event Log	Primary
System Integrity	Message Details	Event Log	Primary
System Integrity	Service Events	Event Log	Secondary
System Integrity	Service Starts and Stops	Event Log	Secondary
System Integrity	Software Settings Changes	Group Policy	Primary
System Integrity	System Services Policy Changes	Group Policy	Primary
System Integrity	Windows Settings Changes	Group Policy	Primary
System Integrity	Failed Activity	Oracle Database	Primary
System Integrity	Trigger Management	Oracle Database	Primary
System Integrity	VMware Power State Changes	VMware	Secondary
System Integrity	All Activity with Review Status	Windows Server	Primary
System Integrity	Audit Log Clearing	Windows Server	Primary
System Integrity	Hardware Changes	Windows Server	Primary
System Integrity	System Shutdowns and Reboots	Windows Server	Primary
User Activity	All File Server Activity by Date	File Servers	Primary
User Activity	User Activity Summary	File Servers	Primary
User Activity	SharePoint Activity Summary	SharePoint	Primary
User Activity	All SQL Server Activity by Date	SQL Server	Primary
User Activity	All User Activity by Server	User Activity	Secondary

Data Governance

Process for management of the availability, usability, integrity, and security of the data employed in an organization.

Report Category	Netwrix Auditor Report	Audited System	Priority
All Changes	File Server Changes	File Servers	Primary
All Changes	All File Server Activity	File Servers	Secondary
All Changes	All SharePoint Changes by Date	SharePoint	Primary
Configuration Changes	Mailbox Storage Quota Changes	Exchange	Secondary
Configuration Changes	SharePoint Configuration Changes	SharePoint	Secondary
Data Access	All Exchange Server Non-Owner Mailbox Access Events	Exchange	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events by User	Exchange	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Access to Archive Data	File Servers	Primary
Data Access	Data Access Surges	File Servers	Primary
Data Access	Excessive Access Permissions	File Servers	Primary
Data Access	Successful File Reads	File Servers	Primary
Data Access	Data Access	Oracle Database	Primary
Data Access	SharePoint Read Access	SharePoint	Primary
Data Access	Data Access	SharePoint Online	Primary
Data Changes	All Data Activity	All Audited Systems	Primary
Data Changes	File Server Changes by Action	File Servers	Primary
Data Changes	Files and Folders Created	File Servers	Primary
Data Changes	Folder Changes	File Servers	Primary
Data Changes	Data Deletions	Oracle Database	Primary
Data Changes	SharePoint Content Changes by User	SharePoint	Primary
Data Changes	Content Management	SharePoint Online	Primary
Data Changes	All SQL Server Data Changes	SQL Server	Primary
Data Integrity	Exchange Online Public Folder Changes	Exchange Online	Primary
Data Integrity	All File Server Activity by Action Type	File Servers	Primary
Data Integrity	All File Server Activity by Server	File Servers	Primary
Data Integrity	Failed Delete Attempts	File Servers	Primary
Data Integrity	File Server Changes by Server	File Servers	Primary
Data Integrity	Files and Folders Deleted	File Servers	Primary
Data Integrity	Potentially Harmful Files - Activity	File Servers	Primary
Data Integrity	Potentially Harmful Files on File Shares	File Servers	Primary
Data Integrity	Share Changes	File Servers	Primary
Data Integrity	Failed Read Attempts	File Servers	Secondary

Data Integrity	Creation of Files with Sensitive Data	File Servers, SharePoint	Primary
Data Integrity	File Names Containing Sensitive Data	File Servers, SharePoint	Primary
Data States	Duplicate Files	File Servers	Primary
Data States	Empty Folders	File Servers	Primary
Data States	Files and Folders by Owner	File Servers	Primary
Data States	Folder Summary Report	File Servers	Primary
Data States	Largest Files	File Servers	Primary
Data States	Most Used File Types	File Servers	Primary
Data States	Potential Data Owners by Folder	File Servers	Primary
Data States	Stale Data by Folder	File Servers	Primary
Data States	Stale Files	File Servers	Primary
Data States	Top Owners by Total File Size	File Servers	Primary
Permission Changes	Exchange Online Mail User Changes	Exchange Online	Primary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	Permissions Changes	File Servers	Secondary
Permission Changes	SharePoint Permissions Changes by User	SharePoint	Secondary
Permission States	Account Permissions	File Servers	Primary
Permission States	Object Permissions by Object	File Servers	Secondary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
User Activity	All File Server Activity by User	File Servers	Primary
User Activity	User Activity Summary	File Servers	Primary
User Activity	All SharePoint Activity	SharePoint	Primary
User Activity	SharePoint Activity Summary	SharePoint	Primary
User Activity	All SQL Server Activity by Date	SQL Server	Primary

Configuration Management

Process for interrelated processes and management techniques for evaluating, coordinating, and controlling changes to and configurations states of the information systems

Report Category	Netwrix Auditor Report	Audited System	Priority
Account States	Organizational Unit Accounts	Active Directory	Secondary
Account States	Service Principal Names of Computer Accounts	Active Directory	Secondary
All Changes	All Active Directory Changes with Review Status	Active Directory	Secondary
All Changes	Exchange Database Changes	Exchange	Primary
All Changes	New Exchange Servers	Exchange	Primary
All Changes	All Exchange Server Changes	Exchange	Secondary
All Changes	All Exchange Server Changes with Review Status	Exchange	Secondary
All Changes	GPO Link Changes	Group Policy	Primary
All Changes	All Group Policy Changes with Review Status	Group Policy	Secondary
All Changes	All SharePoint Changes by Site Collection	SharePoint	Primary
All Changes	SharePoint Changes with Review Status	SharePoint	Primary

All Changes	All SQL Server Activity by Object Type	SQL Server	Secondary
All Changes	All VMware Changes by Object Type	VMware	Secondary
All Changes	All Windows Server Changes with Review Status	Windows Server	Secondary
All States	Groups	Active Directory	Secondary
All States	Group Policy Objects by Policy Name	Group Policy	Primary
Configuration Changes	Active Directory Configuration Container Changes	Active Directory	Primary
Configuration Changes	IIS Application Pool Changes	Event Log	Primary
Configuration Changes	IIS Application Pool Changes	Event Log	Primary
Configuration Changes	IIS Website Changes	Event Log	Primary
Configuration Changes	IIS Website Changes	Event Log	Primary
Configuration Changes	Address List Changes	Exchange	Primary
Configuration Changes	Mailbox Changes	Exchange	Primary
Configuration Changes	Mailbox Storage Quota Changes	Exchange	Primary
Configuration Changes	Exchange Online Management Role Changes	Exchange Online	Primary
Configuration Changes	SharePoint Configuration Changes	SharePoint	Primary
Configuration Changes	VMware Cluster Changes	VMware	Primary
Configuration Changes	VMware Datacenter Changes	VMware	Primary
Configuration Changes	VMware Datastore Changes	VMware	Primary
Configuration Changes	VMware Host System Changes	VMware	Primary
Configuration Changes	VMware Resource Pool Changes	VMware	Primary
Configuration Changes	VMware Snapshot Changes	VMware	Primary
Configuration Changes	VMware Virtual Machine Changes	VMware	Primary
Configuration Changes	DNS Configuration Changes	Windows Server	Primary
Configuration Changes	DNS Resource Record Changes	Windows Server	Primary
Configuration Changes	File Share Changes	Windows Server	Primary
Configuration Changes	General Computer Settings Changes	Windows Server	Primary
Configuration Changes	Printer Changes	Windows Server	Primary
Configuration Changes	Scheduled Task Changes	Windows Server	Primary
Configuration Changes	System Time Changes	Windows Server	Primary
Configuration States	Domain Controllers	Active Directory	Primary
Configuration States	Organizational Units	Active Directory	Primary
Configuration States	Service Principal Names of Domain Controllers	Active Directory	Primary
Configuration States	Computer Accounts	Active Directory	Secondary
Configuration States	Empty Group Policy Objects	Group Policy	Primary
Configuration States	Group Policy Object Link Status	Group Policy	Primary
Configuration States	Group Policy Objects by Setting Name	Group Policy	Primary
Configuration States	Identical Settings in Different GPOs	Group Policy	Primary
Group Membership States	Users Not in Any Distribution Group	Active Directory	Secondary
Permission Changes	Mailbox Delegation and Permissions Changes	Exchange	Primary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary

Permission Changes	VMware Virtual Machine Permissions Changes	VMware	Primary
Permission States	Account Permissions	File Servers	Primary
Permission States	Group Policy Object Delegation	Group Policy	Primary
Policy Changes	Email Address Policy Changes	Exchange	Primary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
Policy Changes	Public Key Policy Changes	Group Policy	Primary
Policy Changes	Registry Policy Changes	Group Policy	Secondary
Policy Changes	Restricted Groups Policy Changes	Group Policy	Secondary
Policy Changes	Software Restriction Policy Changes	Group Policy	Secondary
Policy Changes	Audit Policy and Setting Changes	Oracle Database	Primary
Policy Changes	Local Audit Policy Changes	Windows Server	Primary
Policy States	Group Policy Object Status	Group Policy	Primary
Security Changes	Security Settings Changes	Group Policy	Primary
System Integrity	Service Events	Event Log	Primary
System Integrity	Service Starts and Stops	Event Log	Primary
System Integrity	All Events by Computer	Event Log	Secondary
System Integrity	Software Settings Changes	Group Policy	Secondary
System Integrity	System Services Policy Changes	Group Policy	Secondary
System Integrity	VMware Power State Changes	VMware	Primary

Audit Trail

Process for collection, consolidation, retention and processing of the audit data

Report Category	Netwrix Auditor Report	Audited System	Priority
Account Changes	User Account Management in Azure AD	Azure AD	Primary
Account Changes	User Accounts Created and Deleted Directly in Azure AD	Azure AD	Primary
Account Changes	User-Initiated Password Changes in Azure AD	Azure AD	Primary
Account Changes	Account Management	Oracle Database	Primary
All Changes	All Active Directory Changes	Active Directory	Primary
All Changes	All Active Directory Changes by Date	Active Directory	Primary
All Changes	All Active Directory Changes by Domain Controller	Active Directory	Primary
All Changes	All Active Directory Changes by Group	Active Directory	Primary
All Changes	All Active Directory Changes by Object Type	Active Directory	Primary
All Changes	All Active Directory Changes with Review Status	Active Directory	Primary
All Changes	Activity by Audited System	All Audited Systems	Primary
All Changes	All Changes by Audited System	All Audited Systems	Primary
All Changes	All Changes by Date	All Audited Systems	Primary
All Changes	All Changes by Server	All Audited Systems	Primary
All Changes	All Azure AD Activity by Date	Azure AD	Primary
All Changes	All Azure AD Activity by Object Type	Azure AD	Primary

All Changes	All Azure AD Activity by User	Azure AD	Primary
All Changes	All Generic Syslog Events	Event Log	Primary
All Changes	All System Events by User	Event Log	Primary
All Changes	All Events by Source	Event Log	Secondary
All Changes	All Exchange Server Changes	Exchange	Primary
All Changes	All Exchange Server Changes by Server	Exchange	Primary
All Changes	All Exchange Server Changes with Review Status	Exchange	Primary
All Changes	All Exchange Online Changes	Exchange Online	Primary
All Changes	All Exchange Server Changes by Date	Exchange Online	Primary
All Changes	All File Server Activity	File Servers	Primary
All Changes	File Server Changes	File Servers	Secondary
All Changes	All Group Policy Changes with Review Status	Group Policy	Primary
All Changes	All Oracle Database Activity by Object	Oracle Database	Primary
All Changes	All Oracle Database Activity by Session ID	Oracle Database	Primary
All Changes	All Oracle Database Activity by User	Oracle Database	Primary
All Changes	All Oracle Database Administrative Activity	Oracle Database	Primary
All Changes	All SharePoint Changes	SharePoint	Primary
All Changes	All SharePoint Changes by Date	SharePoint	Primary
All Changes	All SharePoint Changes by Object Type	SharePoint	Primary
All Changes	SharePoint Changes with Review Status	SharePoint	Secondary
All Changes	All SharePoint Online Activity by User	SharePoint Online	Primary
All Changes	All SQL Server Activity	SQL Server	Primary
All Changes	All SQL Server Activity by Object Type	SQL Server	Primary
All Changes	All SQL Server Activity by Server	SQL Server	Primary
All Changes	All User Activity	User Activity	Primary
All Changes	All VMware Changes	VMware	Primary
All Changes	All VMware Changes by Date	VMware	Primary
All Changes	All VMware Changes by Object Type	VMware	Primary
All Changes	All VMware Changes by Server	VMware	Primary
All Changes	All VMware Changes by User	VMware	Primary
All Changes	All Windows Server Changes	Windows Server	Primary
All Changes	All Windows Server Changes by Date	Windows Server	Primary
All Changes	All Windows Server Changes by Object Type	Windows Server	Primary
All Changes	All Windows Server Changes by Server	Windows Server	Primary
All Changes	All Windows Server Changes with Review Status	Windows Server	Primary
All States	Groups	Active Directory	Primary
All States	Group Policy Objects by Policy Name	Group Policy	Secondary
Configuration Changes	Active Directory Site Changes	Active Directory	Primary
Configuration Changes	Domain Controller Changes	Active Directory	Primary
Configuration Changes	Organizational Unit Changes	Active Directory	Primary

Configuration Changes	IIS Application Pool Changes	Event Log	Primary
Configuration Changes	IIS Website Changes	Event Log	Primary
Configuration Changes	All Exchange Server Changes by Object Type	Exchange	Primary
Configuration Changes	Exchange Online Management Role Changes	Exchange Online	Primary
Configuration Changes	File Share Changes	Windows Server	Primary
Configuration Changes	System Time Changes	Windows Server	Primary
Configuration States	Empty Group Policy Objects	Group Policy	Secondary
Configuration States	Group Policy Objects by Setting Name	Group Policy	Secondary
Configuration States	Identical Settings in Different GPOs	Group Policy	Secondary
Data Access	All Exchange Server Non-Owner Mailbox Access Events	Exchange	Primary
Data Access	All Exchange Server Non-Owner Mailbox Access Events by User	Exchange	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events	Exchange Online	Primary
Data Access	All Exchange Online Non-Owner Mailbox Access Events by User	Exchange Online	Primary
Data Access	Access to Archive Data	File Servers	Primary
Data Access	Data Access Surges	File Servers	Primary
Data Access	Data Access	Oracle Database	Primary
Data Access	Data Access	SharePoint Online	Primary
Data Changes	All Data Activity	All Audited Systems	Primary
Data Changes	Files and Folders Created	File Servers	Secondary
Data Changes	Data Deletions	Oracle Database	Primary
Data Integrity	Exchange Online Public Folder Changes	Exchange Online	Primary
Data Integrity	Potentially Harmful Files - Activity	File Servers	Primary
Data Integrity	Creation of Files with Sensitive Data	File Servers, SharePoint	Primary
Data Integrity	File Names Containing Sensitive Data	File Servers, SharePoint	Primary
Data States	Folder Summary Report	File Servers	Secondary
Group Membership Changes	Group Membership Changes in Azure AD	Azure AD	Primary
Group Membership Changes	Exchange Online Group Changes	Exchange Online	Primary
Permission Changes	Exchange Online Mail User Changes	Exchange Online	Primary
Permission Changes	Exchange Online Mailbox Permissions Changes	Exchange Online	Primary
Permission Changes	Privilege Management	Oracle Database	Primary
Permission States	Object Permissions by Object	File Servers	Secondary
Policy Changes	Exchange Online Mailbox Policy Changes	Exchange Online	Primary
Policy Changes	All Group Policy Changes	Group Policy	Primary
Policy Changes	Audit Policy Changes	Group Policy	Primary
Policy Changes	Audit Policy and Setting Changes	Oracle Database	Primary
Policy Changes	Local Audit Policy Changes	Windows Server	Primary
Policy States	Group Policy Object Status	Group Policy	Secondary

Security Changes	Domain Trust Changes	Active Directory	Primary
Security Changes	Object Security Changes	Active Directory	Primary
Security Changes	Operations Master Role Changes	Active Directory	Primary
Security Changes	Security Group Changes	Active Directory	Primary
Security Changes	All Security Events by User	Event Log	Primary
Security Changes	Netwrix Auditor System Health	Event Log	Primary
Security Changes	Sharing and Security Changes	SharePoint Online	Primary
System Access	Activity Outside Business Hours	Active Directory	Primary
System Access	All Logon Activity	Active Directory	Primary
System Access	Failed Logons	Active Directory	Primary
System Access	Interactive Logons	Active Directory	Primary
System Access	Logons by Multiple Users from Single Endpoint	Active Directory	Primary
System Access	Logons by Single User from Multiple Endpoints	Active Directory	Primary
System Access	Successful Logons	Active Directory	Primary
System Access	User Logons and Logoffs on Domain Controllers	Active Directory	Primary
System Access	Azure AD Logon Activity	Azure AD	Primary
System Access	All Oracle Database Logons	Oracle Database	Primary
System Access	All SQL Server Logons	SQL Server	Primary
System Integrity	All Events by Computer	Event Log	Primary
System Integrity	Failed Activity	Oracle Database	Primary
System Integrity	All Activity with Review Status	Windows Server	Primary
System Integrity	Audit Log Clearing	Windows Server	Primary
System Integrity	System Shutdowns and Reboots	Windows Server	Primary
System Integrity	Hardware Changes	Windows Server	Secondary
User Activity	All Active Directory Changes by User	Active Directory	Primary
User Activity	All Changes by User	All Audited Systems	Primary
User Activity	All Events by User	Event Log	Primary
User Activity	All Exchange Server Changes by Group	Exchange	Primary
User Activity	All Exchange Server Changes by User	Exchange	Primary
User Activity	All File Server Activity by Date	File Servers	Primary
User Activity	All SharePoint Activity	SharePoint	Primary
User Activity	All SharePoint Changes by User	SharePoint	Primary
User Activity	All SQL Server Activity by Date	SQL Server	Primary
User Activity	All User Activity by Server	User Activity	Primary
User Activity	All Windows Server Changes by User	Windows Server	Primary