netwrix

ISO/IEC 27001 Controls

and Netwrix Auditor Mapping

About ISO/IEC 27001

ISO 27001 is an international standard that provides requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS). The design and implementation of an organization's ISMS is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization.

Organizations implementing ISO/IEC 27001 can be formally audited and certified compliant with the standard.

The ISO 27002 standard, known as ISO17799 before 2007, is a code of practice for information security, originally based on BS7799 standard first published in 1999 by BSI. The current version of the standard was released in 2013.

ISO/IEC 27002:2013 has 14 security control sections collectively containing a total of 35 main security categories and 114 controls.

...

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 ISO controls

Based on mapping provided by NIST SP800-53 rev4 **(TABLE H-1: MAPPING NIST SP 800-53 TO ISO/IEC 27001)**

6 Organization of information security		
Control	**How to Comply?**	**Processes and Report Categories**
6.1.2 Segregation of duties	Monitor activities and verify that only the authorized individuals can use information systems	Access Control System Access Account Management Account States
6.1.5 Information security in project management	Refer to the audit trail of configuration states and changes provided by Netwrix Auditor to support configuration management plan development and implementation. Utilize Netwrix Auditor for purposes of auditing external service provider information systems activities and configurations for compliance with organization-defined metrics, procedures and baselines.	Configuration Management Policy States Policy Changes Configuration States Configuration Changes Integrity Monitoring System Integrity
6.2.2 Teleworking	Netwrix Auditor is designed to assist with establishment of organization-defined access control procedures. Audit all remote access policies and sessions.	Access Control System Access Policy States Policy Changes

7 Human resource security		
7.2.3 Disciplinary process	Analyze audit trail provided by Netwrix Auditor in order to identify individual and the reason for the sanctions.	Audit Trail User Activity

7.3.1 Termination or change of employment responsibilities	Through reviewing audit trail validate revocation of authenticators/credentials associated with the individual, Audit modifications of access authorizations. Validate information system accounts management for compliance with organization-defined procedures and conditions.	Account Management Account States Account Changes

9 Access control		
9.2.1 User registration and de-registration	While relying on AD mechanisms for identification and authentication purposes utilize auditing capabilities provided by Netwrix Auditor to validate conformance with organization-defined policies and procedures.	Account Management Account States Account Changes Policy Changes Policy States
9.2.2 User access provisioning	Audit authorization and access procedures for discrepancies, Validate that only users and processes necessary for accomplishing assigned tasks in accordance with organizational missions and business functions are present in information systems ,	Account Management Account States Account Changes Access Control System Access Data Access Group Membership States Group Membership Changes
9.2.3 Management of privileged access rights	Validate information system accounts management for compliance with organization-defined procedures and conditions,	Privileged Users Management Group Membership Changes Security Changes Policy Changes Account Changes User Activity
9.2.4 Management of secret authentication information of users	While relying on AD mechanisms for identification and authentication purposes utilize auditing capabilities provided by Netwrix Auditor to validate conformance with organization-defined policies and procedures.	Account Management Credentials Management

9.2.5 Review of user access rights And 9.2.6 Removal or adjustment of access rights	Validate information system accounts management for compliance with organization-defined procedures and conditions	Access Control Account Management Privileged Users Management
9.3.1 Use of secret authentication information	While relying on AD mechanisms for identification and authentication purposes utilize auditing capabilities provided by Netwrix Auditor to validate conformance with organization-defined policies and procedures.	Account Management Credentials Management
9.4.1 Information access restriction	Netwrix Auditor is designed to assist with establishment of organization-defined access control procedures, Audit authorization and access procedures for discrepancies, Validate that only users and processes necessary for accomplishing assigned tasks in accordance with organizational missions and business functions are present in information systems, Validate that only public content is accessible without identification or authentication.	Data Governance Access Control
9.4.2 Secure log-on procedures And 9.4.3 Password management system	Audit failed logon activities. Utilize User Activity Video Recording custom notification feature. Audit logon activities, including state-in-time reports of last logons. Review audit logs to validate systems accessed only in accordance with organization-defined policies. While relying on AD mechanisms for identification and authentication purposes utilize auditing capabilities provided by Netwrix Auditor to validate conformance with organization-defined policies and procedures.	Access Control Account Management Configuration Management Credentials Management

12 Operations security		
12.1.2 Change management	Analyze configuration states and changes to validate conformity with organization-defined baselines, Review configuration changes in accordance with defined frequencies, authorization policies and other organization-defined metrics, Verify that audit trail provided by Netwrix Auditor confirms that changes made to the information systems did not affect correctness of the security functions, Review audit trail to validate that established access restrictions are effective in preventing unauthorized changes to the information systems, Refer to the audit trail of configuration states and changes provided by Netwrix Auditor to support configuration management plan development and implementation,	Audit Trail Configuration Management
12.1.3 Capacity management	Netwrix Auditor supports required functionality with built-in AuditArchive™ feature, Built-in functionality of Netwrix Auditor would notify of audit processing failures, Monitor for user restrictions violations and irregularities in systems functions.	Audit Trail

12.4.1 Event logging	Validate that the organization-defined auditable events properly collected, updated and reviewed to ensure that the current set is still necessary and sufficient. Netwrix Auditor collects and consolidates fully detailed information on events across information systems. All collected by Netwrix Auditor events contain necessary time stamps. AuditArchive™ allows flexible configuration of audit data retention policies, Netwrix Auditor enables configurable audit trail generation, User Activity Video Recording feature provides session auditing, regardless of existing logging capabilities.	Audit Trail
12.4.2 Protection of log information	Netwrix Auditor enables required functionality with built-in AuditArchive™ feature, Built-in functionality of Netwrix Auditor would notify of audit processing failures, Two-tiered AuditArchive™ provides technical protection of audit information. Monitor systems for illegal access and suspicious activities, audit privileged users.	Audit Trail
12.4.3 Administrator and operator logs And 12.7.1 Information systems audit controls	Validate that the organization-defined auditable events properly collected, updated and reviewed to ensure that the current set is still necessary and sufficient. Monitor systems for illegal access and suspicious activities, audit privileged users. Netwrix Auditor enables configurable audit trail generation.	Audit Trail Privileged Users Management User Activity

13 Communications security		
13.1.1 Network controls	Audit authorization and access procedures for discrepancies. Audit all remote access policies and sessions. Monitor for user restrictions violations and irregularities in systems functions.	Access Control System Access Data Access
13.1.3 Segregation in networks	Audit privileged users, access control and systems management activities.	Access Control System Access Privileged Users Management Configuration Changes Policy Changes
13.2.1 Information transfer policies and procedures	Netwrix Auditor is designed to assist with establishment of organization-defined access control procedures. Audit authorization and access procedures for discrepancies. Audit all remote access policies and sessions.	Access Control System Access Data Integrity Data Governance Data Access Data Changes
13.2.3 Electronic messaging	Audit trail collected by Netwrix Auditor can provide necessary evidence to associate changes in information systems with a particular individual.	Audit Trail

14 System acquisition, development and maintenance		
14.2.2 System change control procedures	Refer to the audit trail of configuration states and changes provided by Netwrix Auditor to support configuration management plan development and implementation.	Configuration Management Integrity Monitoring Access Control Audit Trail
14.2.3 Technical review of applications after operating platform changes	Review configuration changes in accordance with defined frequencies, authorization policies and other organization-defined metrics. Refer to the audit trail of configuration states and changes provided by Netwrix Auditor to support configuration management plan development and implementation	Configuration Management Access Control Integrity Monitoring Audit Trail

14.2.6 Secure development environment	Analyze configuration states and changes to validate conformity with organization-defined baselines. Verify that audit trail provided by Netwrix Auditor confirms that changes made to the information systems did not affect correctness of the security functions.	Configuration Management Access Control
14.2.9 System acceptance testing	Utilize audit trail of activities and configuration information to perform security assessments and prepare necessary reports. Review configuration changes in accordance with defined frequencies, authorization policies and other organization-defined metrics. Verify that audit trail provided by Netwrix Auditor confirms that changes made to the information systems did not affect correctness of the security functions. Refer to the audit trail of configuration states and changes provided by Netwrix Auditor to support configuration management plan development and implementation, Utilize Netwrix Auditor for purposes of auditing external service provider information systems activities and configurations for compliance with organization-defined metrics, procedures and baselines.	Configuration Management Access Control Audit Trail Integrity Monitoring

15 Supplier relationships		
15.2.1 Monitoring and review of supplier services	Utilize Netwrix Auditor for purposes of auditing external service provider information systems activities and configurations for compliance with organization-defined metrics, procedures and baselines	Audit Trail User Activity

16 Information security incident management		
16.1.2 Reporting information security events	Netwrix Auditor facilitates organization-defined procedures for audit record review and analysis. Utilize built-in scheduled reporting and real-time alerting.	Audit Trail Integrity Monitoring Access Control
16.1.4 Assessment of and decision on information security events and 16.1.5 Response to information security incidents	Monitor systems operations and utilize built-in reporting to perform root cause analysis of incidents.	Audit Trail Configuration Management
16.1.7 Collection of evidence	Built-in capabilities of Netwrix Auditor include audit data archiving and report generation. All collected by Netwrix Auditor events contain necessary time stamps. Two-tiered AuditArchive™ provides technical protection of audit information. AuditArchive™ allows flexible configuration of audit data retention policies. Monitor systems operations and utilize built-in reporting to perform root cause analysis of incidents.	Audit Trail

17 Information security aspects of business continuity management		
17.1.2 Implementing information security continuity	Audit access and activities on the alternative site to validate compliance with organization-defined metrics.	Configuration Management Integrity Monitoring
17.1.3 Verify, review and evaluate information security continuity	Reviewing audit trail of testing activities simplifies analysis of the contingency plans effectiveness.	

18 Compliance		
18.1.3 Protection of records	Audit authorization and access procedures for discrepancies Two-tiered AuditArchive™ provides technical protection of audit information. AuditArchive™ allows flexible configuration of audit data retention policies. Audit all operations with data for compliance with policies and procedures.	Audit Trail Access Control System Access Data Access Data Governance Data Integrity Data States Data Changes
18.1.4 Privacy and protection of personally identifiable information	Audit all operations with data for compliance with policies and procedures.	Access Control System Access Data Access User Activity Data Governance Data Integrity
18.2.2 Compliance with security policies and standards	Utilize audit trail of activities and configuration information to perform security assessments and prepare necessary reports. Netwrix Auditor performs continuous monitoring of activities and configuration changes across the entire IT infrastructure in accordance with organization-defined set of parameters.	Audit Trail
18.2.3 Technical compliance review	Netwrix Auditor performs continuous monitoring of activities and configuration changes across the entire IT infrastructure in accordance with organization-defined set of parameters	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