netwrix

PCI Requirements
and Netwrix Auditor Mapping

About PCI DSS v3.2

Anyone who accepts credit, debit or prepaid cards over the internet, telephone, or terminals as payment; stores card data, or processes card transactions is responsible to be PCI compliant. Failure to comply with PCI may result in fines, loss of reputation, and inability to accept major credit cards.

Appropriate policies and procedures, technical measures, administrative efforts, and physical security should supplement each other in the organization in order to ensure continuous compliance with PCI Requirements.

...

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 PCI Controls

Requirement 3: Protect stored cardholder data		
Control	**How to Comply?**	**Processes and Report Categories**
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes	Monitor all designated locations for data creation and deletions to confirm that retention and disposal policies are effective.	Data Governance Data Changes
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.		

Requirement 5: Use and regularly update anti-virus software or programs		
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Configure Group policies appropriately as to not allow not authorized users to disable or change antivirus software. Audit all changes to sensitive systems to ensure that antivirus mechanisms have not been tempered with.	Privileged Users Management Configuration Changes

Requirement 6: Develop and maintain secure systems and applications		
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Audit user account states and changes to verify that no test/development user accounts are present in the production systems.	Account Management Account Changes Account States
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	Support this requirement by referring to the complete audit trail provided by Netwrix Auditor to verify that all changes are authorized in accordance with organization-defined policies and procedures. Review Status mechanism can be utilized.	Audit Trail All Changes

6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls. **6.4.2** Separation of duties between development/test and production environments	Audit all access rights changes, activities of users with development/test user access rights, across all information systems to ensure no unauthorized access to production environments is possible.	Access Control Group Membership Changes Group Membership States All Changes All States
6.4.4 Removal of test data and accounts from system components before the system becomes active/goes into production.	Validate that all test user accounts are removed and created temporary data is deleted in accordance with the requirements.	Account Management Account Changes Account States
6.4.5.2 Documented change approval by authorized parties.	Utilize the audit trail provided by Netwrix Auditor to supply reference of activities. In addition, Review Status mechanism can be utilized.	Audit Trail All Changes

Requirement 7: Restrict access to cardholder data by business need to know		
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Audit access to information systems in order to confirm that no access by unauthorized personnel is taking place.	Access Control System Access Data Access Account Management Account Changes Account States
7.1.3 Assign access based on individual personnel's job classification and function.	Combine audit trail provided by Netwrix Auditor and HR department records to validate that assigned access is necessary and appropriate.	Account Management Account Changes Privileged Users Management Account Changes
7.1.4 Require documented approval by authorized parties specifying required privileges.	Compare Netwrix Auditor records of assignments of privileges and changes with internal authorization documents for each case of the privileges assignment.	Account Management Account Changes Account States
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Audit user access rights, files folders and their permissions across the entire IT infrastructure for early detection of unauthorized changes to security settings (e.g. granting of new permissions, elevation of privileges, etc.)	Access Control Policy Changes Policy States System Access User Activity Integrity Monitoring System Integrity

Requirement 8: Assign a unique ID to each person with computer access		
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: **8.2** In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components	Complement administrative efforts of various departments of organization and built-in capabilities of Active Directory for identity management with enhanced visibility, complete audit trail of states and changes and other features provided by Netwrix Auditor.	Account Management Configuration States Accounts States Account Changes Policy Changes Policy States Privileged Users Management User Activity Access Control System Access
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	Complete auditing of user accounts and logons to analyze violations and prevent usage of the same ID by multiple persons (e.g. from different computers) Compare audit trail with HR records.	Access Control System Access Data Access Account Management Accounts States Audit Trail User Activity
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Audit user creations, deletions, password resets, and modifications to all account policies and attributes across all information systems.	Account Management Account Changes Credentials Management Password Changes Password Policy Changes
8.1.3 Immediately revoke access for any terminated users.	Manage user accounts in coordination with HR department. Auditing of disabled accounts, automated de-provisioning of inactive user accounts.	Account Management Account Changes Account States
8.1.4 Remove/disable inactive user accounts within 90 days.	Utilize Netwrix Auditor built-in automated disabling and removal with full reporting.	Account Management Account Changes Account States
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access.	Audit user access and all operations with accounts in order to establish and maintain control of system components that allow remote access.	Access Control System Access Account Management Account Changes Account States
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	Analyze Netwrix Auditor audit logs of to confirm that AD account lockout policy (Account Lockout Threshold) is configured and functioning properly.	Access Control System Access Policy Changes Policy States Security Changes

8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Analyze Netwrix Auditor audit logs of to confirm that AD account lockout policy (Account lockout duration) is configured and functioning properly.	Configuration Changes User Activity
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Analyze Netwrix Auditor audit logs to confirm that Group policy for time-out settings for disconnected, active, and idle sessions (Idle session limit) is configured and functioning properly.	
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Utilize built-in encryption features of Active Directory and validate proper policy states and functionality by analyzing audit trail provided by Netwrix Auditor.	Access Control Policy Changes Policy States Credentials Management Password Changes Password Policy Changes Configuration Management Policy States Configuration States
8.2.3 Passwords/passphrases require a minimum length of at least seven characters and contain both numeric and alphabetic characters or equivalent parameters are specified. **8.2.4** Change user passwords/passphrases at least once every 90 days. **8.2.5** Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	Audit state and changes of Active Directory password policy settings to ensure compliance with the requirement. Refer to the audit trail of all password changes to validate that policy was enforced properly.	
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	Audit all newly created user accounts, logons and password changes to confirm compliance and/or prevent violation .	

8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	Utilizing automatic password expiration alerting mechanism of Netwrix Auditor may help with this requirement.	Access Control Policy States Configuration Management Policy States Configuration States
8.5 Do not use group, shared, or generic IDs, passwords.	Audit actions done under a shared account (e.g. same user/different workstations) and help to eliminate its usage	Access Control User Activity Account Management Account Changes
8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	Audit access and activities logs across information systems to validate that credentials used for POS remote access cannot be used to access any of the other systems.	

Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1 Implement audit trails to link all access to system components to each individual user.	Utilize Netwrix Auditor's fully featured auditing and reporting of all user activities including access to sensitive files, across the entire IT infrastructure and recording of who changed what, when, and where.	Access Control System Access Data Access User Activity Audit Trail User Activity
10.2 Implement automated audit trails for all system components to reconstruct the following events:	This requirement is supported by built-in functionality of Netwrix auditor.	Audit Trail All Changes All States
10.2.1 All individual user accesses to cardholder data.	Audit all user access to designated locations in information systems, where cardholder data is stored.	Access Control Data Access Data Integrity User Activity
10.2.2 All actions taken by any individual with root or administrative privileges.	Audit all activities of users with administrative privileges across information systems.	Privileged Users Management User Activity

10.2.3 Access to all audit trails	Turn on user activity video recording feature on systems with Netwrix Auditor installations and capture all interactions.	Audit Trail User Activity
10.2.4 Invalid logical access attempts.	Audit failed logon attempts.	Access Control System Access
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	Audit user logons, activities and changes to account policies and modifications to user accounts including elevation of privileges.	Access Control System Access Account Management Account Changes Policy Changes Privileged Users Management Account Changes Group Membership Changes
10.2.6 Initialization, stopping, or pausing of the audit logs	Monitor changes to the auditing policies on critical systems, optionally utilize user activity video recording. Watch for problems with audit collection in daily summary report of Netwrix Auditor.	Audit Trail User Activity Policy Changes
10.2.7 Creation and deletion of system-level objects	Audit all modifications to critical files, database tables, AD objects, registry keys, etc.	Integrity Monitoring System Integrity Security Changes
10.3 Record at least the following audit trail entries for all system components for each event: User identification; Type of event; Date and time; Success or failure indication; Origination of event	This requirement is supported by built-in functionality of Netwrix auditor.	Audit Trail All Changes
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	Full-featured reporting functionality with predefined reports and ability to create custom reports on any type of collected data. Out-of-the box reports scheduled daily and sent via e-mail for review.	Configuration Management All Changes
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Unlimited storage capabilities with efficient storage use to store up to 10 years and more of past audit trails and history of changes to system components and security settings. Full-featured reporting for immediate access to all required data.	Audit Trail

Requirement 11: Regularly test security systems and processes		
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). **11.3** Implement a methodology for penetration testing	Refer to the audit trail generated by Netwrix Auditor to ensure that there're no traces of unauthorized access and no degrading changes to security mechanisms.	Access Control System Access Audit Trail User Activity All Changes
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Audit all changes to sensitive information systems to detect violations.	Integrity Monitoring System Integrity Data Integrity User Activity All Changes

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