HIPAA CONTROLS

POWERED BY AUDITOR MAPPING

WHITE PAPER

TetherView

TetherView

HIPAA CONTROLS

POWERED BY AUDITOR MAPPING

The Health Insurance Portability and Accountability Act (HIPAA) is a set of standards created by Congress that aim to safeguard protected health information (PHI) by regulating healthcare providers. HIPAA has been in effect since 1996.

It was not effectively enforced before the act called HITECH (The Health Information Technology for Economic and Clinical Health Act) was enacted in 2009. HITECH among other requirements added HIPAA Breach Notification Rule that requires full disclosure of any leaked PHI directly to the patients and government authorities.

Further strengthening PHI protection and issuing more precise and even more strident requirements is the Omnibus Final Rule enacted in 2013, it provides various clarifications and final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by HITECH.

Complying with the HIPAA regulations requires all healthcare organizations to setup processes and controls that ensure security and integrity of PHI. The ability to demonstrate that PHI is secured through reliable access control and monitoring is key to ensure a successful HIPAA audit.

Majority of the requirements related to the information systems is contained within the HIPAA Security Rule.

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

TetherView

MAPPING OF PROCESSES AND REPORT CATEGORIES TO HIPAA CONTROLS

§164.308 Administrative safeguards. (HIPAA Security Rule)		
Control	**How to Comply?**	**Processes and Report Categories**
§164.308 (a)(1)(i) Security management process.	In accordance with implemented policies, review activities in information systems to detect and investigate security violations.	• Audit Trail • All Changes • Configuration Management • Policy States • Configuration States
§164.308 (a)(1)(ii)(A) Risk analysis.	Utilize audit trail recorded by Auditor, while performing assessment of risks to confidentiality, integrity, and availability of PHI.	• Access Control • All Changes • Integrity Monitoring • System Integrity • Data Integrity
§164.308 (a)(1)(ii)(B) Risk management.	Validate that the implemented security measures are sufficient and appropriate relying on organization defined procedures and audit trail produced by Auditor.	• Data Governance • Data Integrity • User Activity • Configuration Management • Configuration Changes • Configuration States
§164.308 (a)(1)(ii)(C) Sanction policy.	To support this requirement please refer to the user activities trail for violations of security policies.	• Access Control • User Activity • Account Management • Account States
§164.308 (a)(1)(ii)(D) Information system activity review.	Utilize built-in capabilities for alerts and on-demand reports to regularly audit activities in organization-defined information systems.	• Audit Trail • All Changes • User Activity
§164.308 (a)(3)(ii)(C) Termination procedures.	Use inactive users tracking and audit users' states and activities in coordination with HR department to ensure proper actions were taken to protect access to PHI upon termination.	• Account Management • Account States • Account Changes

Control	How to Comply?	Processes and Report Categories
§164.308 (a)(4)(i) Information access management.	Validate that audit trail provided by Auditor confirms that implemented access management is functioning properly.	• Access Control • System Access • Data Access • Privileged Users Management • Group Membership Changes • Policy Changes • Permission Changes
§164.308 (a)(4)(ii) (A) Isolating health care clearing house functions	Audit all access and data modifications to ensure no unauthorized access is taking place.	• Access Control • System Access • Data Governance • Data Integrity
§164.308 (a)(4)(ii)(C) Access establishment and modification.	Track all changes to access rights, relevant groups membership and compare with authorization procedures for discrepancies.	• Access Control • Account Changes • Account States • Policy Changes Policy States • Group Membership Changes • Group Membership States
§164.308 (a)(5)(ii)(A) Security reminders. Periodic security updates.	Prove that appropriate updates were performed by analyzing audit trail of changes to the information systems.	• Integrity Monitoring • Configuration Changes • System Integrity Configuration • Management System Integrity
§164.308 (a)(5)(ii)(B) Protection from malicious software.	Audit SW and registry changes on sensitive WS machines to confirm that implemented measures for malware protection are in place.	• Integrity Monitoring • Configuration Changes • System Integrity • Privileged Users Management • Configuration Changes
§164.308 (a)(5)(ii)(C) Log-in monitoring.	Refer to the audit logs of Netwrix Auditor to review successful logons for traces of unauthorized access.	• Access Control • System Access
§164.308 (a)(5)(ii)(D) Password management.	Audit all password activities across information systems to confirm compliance with policies and procedures.	• Credentials Management • Password Changes • Password Policy Changes

Control	How to Comply?	Processes and Report Categories
§164.308 (a)(6)(i) Security incident procedures.	Netwrix Auditor helps with this control implementation by providing complete audit trail of all activities and allows effective root cause analysis. In addition built-in AD recovery feature can be used.	• Audit Trail • All Changes • User Activity
§164.308 (a)(6)(ii) Response and reporting.	To support with this control implementation Auditor provides complete audit trail of activities leading to the incident and helps with root cause analysis afterwards.	• Audit Trail
§164.308 (a)(7)(ii)(B) Disaster recovery plan.	Investigate complete audit trail of changes including before/after values for immediate data recovery. Quick rollback of unauthorized and accidental changes to Active Directory objects, including restore of deleted objects.	• Audit Trail • All Changes • User Activity • Configuration Management • Configuration States • Permission States
§164.312 Administrative safeguards. (HIPAA Security Rule)		
§164.312(a)(1) Standard: Access control.	Relying on built-in Active Directory mechanisms greatly simplified by Auditor that provides greater visibility into all activities and configurations and helps to confirm that access control is established in accordance with organization-defined policies and procedures.	• Access Control
§164.312 (a) (2) (i) Unique user identification.	Audit user access and activities across all information systems and validate that no simultaneous activities by the same user are happening, nor multiple access instances are found.	• Account Management • Account Changes • Account States • Access Control • System Access • Data Access
§164.312 (a)(2)(iii) Automatic logoff.	Analyze 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.	• Access Control • Policy States • Configuration Changes • Policy Changes • System Access

§164.312 (b) Standard: Audit controls.	Built-in capabilities of Netwrix auditor ensure that complete audit trail of monitored systems is collected and securely retained for future reference.	• Audit Trail
§164.312 (c)(1) Integrity.	Monitor all access to and modifications of PHI across all information systems to discover and fix violations.	• Integrity Monitoring
§164.312 (d) Person or entity authentication.	Audit all logon activities for traces of illegal access.	• Access Control • System Access • User Activity • All Changes
§164.312 (e)(2)(i) Integrity controls.	Monitor all changes to the PHI to ensure that no unauthorized changes are taking place.	• Integrity Monitoring • Data Integrity All Changes

§164.316 Administrative safeguards. (HIPAA Security Rule)		
§164.316 (b)(1) (ii) Documentation.	Auditor provides configurations states and complete audit trail of access and changes, including who, when, where, what with before and after values, consolidated from across various information systems.	• Audit Trail
§164.316 (b)(2)(i) Time limit.	Configurable two-tiered AuditArchive™ enables cost effective audit storage, holding data for up to 10 years or more.	• Audit Trail
§164.316 (b)(2)(ii) Availability.	AuditArchive™ provides easily available access to the audit data of all audited systems for any time period.	• Audit Trail

§164.528 Accounting of disclosures of protected health information. (HIPAA Privacy Rule)		
§164.528 (a) Right to an accounting of disclosures of protected health information	Holding audit records for as long as necessary can help with reconstruction of activities and access attempts to protected health information upon request.	• Audit Trail • Integrity Monitoring • Data Integrity • All Changes

TetherView

CONTROL PROCESSES AND REPORT CATEGORIES

Control Processes

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

Auditor Report Categories

For better efficiency and more focused approach to the audit data processing, 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

TetherView

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

Report Category	Netwrix Auditor Report	Audited System	Priority
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

Report Category	Netwrix Auditor Report	Audited System	Priority
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	Successful Logons by User	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

TetherView

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 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
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 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 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 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	All User Activity	User Activity	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

Report Category	Netwrix Auditor Report	Audited System	Priority
Group Membership States	Administrative Group Members	Active Directory	Primary
Group Membership States	Temporary Users in Privileged Groups	Active Directory	Primary
Permission States	Group Policy Object Delegation	Group Policy	Secondary
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	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

TetherView

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 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	Programs Added and Removed	Windows Server	Primary
Configuration Changes	Service Changes	Windows Server	Primary
Configuration Changes	Windows Registry Changes	Windows Server	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

Report Category	Netwrix Auditor Report	Audited System	Priority
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	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	All User Activity by Server	User Activity	Secondary

TetherView

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
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 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 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	Primary
Data Integrity	File Names Containing Sensitive Data	File Servers	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

Report Category	Netwrix Auditor Report	Audited System	Priority
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 States	Account Permissions	File Servers	Primary
Permission States	Object Permissions by Object	File Servers	Secondary
User Activity	All File Server Activity by User	File Servers	Primary
User Activity	User Activity Summary	File Servers	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	GPO Link Changes	Group Policy	Primary
All Changes	All Group Policy Changes with Review Status	Group Policy	Secondary
All Changes	All Windows Server Changes with Review Status	Windows Server	Secondary
Configuration Changes	Active Directory Configuration Container Changes	Active Directory	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

Report Category	Netwrix Auditor Report	Audited System	Priority
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 States	Account Permissions	File Servers	Primary
Permission States	Group Policy Object Delegation	Group Policy	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	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

TetherView

Audit Trail

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

Report Category	Netwrix Auditor Report	Audited System	Priority
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 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 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 User Activity	User Activity	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

Report Category	Netwrix Auditor Report	Audited System	Priority
Configuration Changes	IIS Application Pool Changes	Event Log	Primary
Configuration Changes	IIS Website Changes	Event Log	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	Access to Archive Data	File Servers	Primary
Data Access	Data Access Surges	File Servers	Primary
Data Changes	Files and Folders Created	File Servers	Secondary
Data Integrity	Potentially Harmful Files - Activity	File Servers	Primary
Data Integrity	Creation of Files with Sensitive Data	File Servers	Primary
Data Integrity	File Names Containing Sensitive Data	File Servers	Primary
Data States	Folder Summary Report	File Servers	Secondary
Permission States	Object Permissions by Object	File Servers	Secondary
Policy Changes	All Group Policy Changes	Group Policy	Primary
Policy Changes	Audit Policy Changes	Group Policy	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

Report Category	Netwrix Auditor Report	Audited System	Priority
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 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 File Server Activity by Date	File Servers	Primary
User Activity	All User Activity by Server	User Activity	Primary
User Activity	All Windows Server Changes by User	Windows Server	Primary