YOUR LOGO HERE

netwrix

GDPR Controls

and Netwrix Auditor Mapping

About GDPR

The General Data Protection Regulation (GDPR) is a legal act of the European Parliament and the Council (Regulation (EU) 2016/679) that was adopted in April 2016 and comes into force on May 25, 2018. The GDPR primarily seeks to provide unified and clear rules on stronger data protection that are fit for the digital age, give individuals more control of their personal information processed by companies and ease law enforcement. The GDPR will repeal the current legal act (Directive 95/46/EC) enacted in 1995, which has been inconsistently interpreted by the various European Union member states.

In addition to harmonizing data protection law across the EU, the new regulation will also affect non-European companies that offer goods or services to, or monitor the behavior of, European Union residents, and therefore process any of their personal data. This refers to the extraterritorial application of the law. In other words, organizations of all types from across all industries that are established outside the European Union but that conduct business within it will be subject to GDPR compliance starting May 25, 2018.

The extended jurisdiction of the GDPR is arguably the biggest change to the 1995 Directive. The other important principles laid down in the GDPR are the following:

- **Extended rights of data subjects** — These, among others, include the right of access, the right to data portability and the right to data erasure.
- **72-hour data breach notification** — In the case of a personal data breach, an organization must notify the supervisory authority not later than 72 hours after having become aware of it.
- **Privacy by design** — Organizations must ensure that, both in the planning phase of processing activities and in the implementation phase of any new product or service, GDPR data protection principles and appropriate safeguards are addressed and implemented.
- **Accountability** — An organization must ensure and demonstrate compliance with the data protection principles of the GDPR.

Fines for non-compliance with the GDPR depend on the infraction. In the case of a personal data breach (defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed), the fine is up to 4% of the company's annual worldwide turnover or €20 million, whichever is higher. For other infringements of GDPR provisions, the fine is up to 2% of annual worldwide turnover or €10 million, whichever is higher.

Mapping of processes and report categories to the provisions of the GDPR articles

The following table lists some of the key provisions of the GDPR and explains how Netwrix Auditor can help your organization achieve compliance with those provisions. Please note that the efforts and procedures required to comply with GDPR requirements may vary depending on an organization's systems configuration, internal procedures, nature of business and other factors. Implementation of the procedures described below will not guarantee GDPR compliance, and not all the controls that Netwrix Auditor can possibly support are included. This mapping should be used as a reference guide to help you implement policies and procedures tailored to your organization's unique situation and needs.

GDPR Chapter II		
Provisions	**How to Achieve?**	**Processes and Report Categories**
Article 5. §1. Personal data shall be: **(f)** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	Use report subscriptions to set an appropriate schedule for reviewing reports that show all user accounts with the current or historical state of permissions granted on files and folders; current and past group membership; object permissions granted to user accounts; excessive access permissions; permission inheritance breaks; and changes to user rights assignments. Use the collected audit trail to review user access to sensitive content and data in SharePoint, Exchange, Exchange Online, Windows-based file servers, network-attached storage devices, databases and other IT systems. Use reports to see all data manipulations that occurred on a specified SQL Server, including changes to keys, indexes, server roles, logins and database content. Review changes to user privileges, roles, tables, views and triggers, as well as successful and failed attempts to modify or access your structured data in Oracle Database. Enable timely detection of any user actions that violate your data protection policies by subscribing to the following reports: Files and Folders Deleted, Data Deletions, Files and Folders Moved, Files and Folders Renamed, and Files Copied.	**[Report Categories]** Account Management Account States Group Membership States Group Membership Changes Access Control Data Access Data Governance Data Changes Integrity Monitoring Data Integrity Configuration Changes Policy Changes
Article 5. §2. The controller shall be responsible for, and be able to demonstrate compliance with,	Demonstrate the effectiveness of your data protection controls using a complete audit trail that is consolidated and reliably preserved by Netwrix Auditor in a two-tiered (file-based + SQL database)	**[Process]** Centralized collection, consolidation and archiving of a complete

paragraph 1 ('accountability').	AuditArchive™ storage system. Easily access the archived audit data anytime it is required for security assessments, investigations and compliance processes. Gain meaningful intelligence about user actions and demonstrate the effectiveness of your controls using predefined reports and dashboards. Create custom reports or easily pinpoint specific data with Interactive Search.	audit trail are enabled by the AuditArchive™ feature of Netwrix Auditor. **[Report Categories]** Audit Trail

GDPR Chapter IV		
Provisions	**How to Comply?**	**Processes and Report Categories**
Article 24. §1. ...the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.	Review the required Netwrix Auditor reports to gain relevant knowledge of the context around system configuration changes and system and data access that posed threats to personal data; use reports to get valuable details about existing controls in order to validate those controls and establish user accountability.	**[Report Categories]** Audit Trail
Article 25. §1. ...the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures... ...which are designed to implement data-protection principles... ...and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	Identify and evaluate the effectiveness of your controls for protecting personal data using the complete audit trail provided by Netwrix Auditor and its extensive reporting capabilities. Subscribe to the required reports and periodically review summaries of IT changes and access events across critical IT systems and applications with who, what, when and where details for each change or data access event. Periodically review reports that provide easy-to-read information about critical events in your event logs and Syslog. Periodically review reports that provide details on all installations and removals of software applications and hardware devices; review report showing creation of potentially harmful files. Use the Interactive Search feature to search through consolidated audit trails and quickly find the exact information you need. Interactive Search enables you to create easy-to-read custom reports	**[Report Categories]** Configuration Management System Integrity Security Changes Integrity Monitoring System Access Data Integrity Access Control All Changes Data Access Privileged Users Management Configuration Changes **[Process]** Search contextual data and investigate data breaches using the

	with just a few clicks, simplifying investigation of security incidents or data breaches and helping you quickly understand why and how those events happened.	Interactive Search feature of Netwrix Auditor.
Article 25. §2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	Periodically review all attempts to access critical resources or settings, including both successful and failed attempts. Subscribe to daily or weekly reports showing changes to user permissions and group membership to control privilege delegation. Compare lists of enabled user accounts with current or historical state of permissions to validate that your access controls are working properly. Review excessive permissions, failed activity trends, and newly created files that might contain sensitive data. Define a schedule to review reports that deliver details about successful and failed system logon attempts; validate that there are no multiple access instances. Monitor changes to Group Policy Objects that could affect password policy, and audit all password activities across all information systems to confirm compliance with policies and procedures. Periodically review reports that show enabled, disabled, expired and locked user accounts. Review reports on user account last logon time, and coordinate with your HR department all user statuses. Use Netwrix Auditor to set up automatic deactivation of user accounts after a certain period of inactivity. Enable user activity video recording to audit user actions.	**[Report Categories]** Access Control System Access Data Access Password Policy Changes Account Management Account States Group Membership States Group Membership Changes Integrity Monitoring User Activity Data Integrity Credentials Management **[Process]** Monitor your IT environment for inactive users with the Inactive Users feature of Netwrix Auditor.
Article 32. §1. ...the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including...: **(b)** the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;	Use overview dashboards to see what is happening in your IT infrastructure on a high level, including how often changes are made, which systems are most affected, and whether there are unusual spikes in the number of modifications and file and folder access attempts. Review the required predefined reports to get a broad understanding of the context in which security incidents occurred; audit reports provide meaningful details about user activities to help you quickly find the root cause of a problem and establish user accountability. Use Netwrix Auditor to quickly revert unauthorized	**[Report Categories]** Audit Trail All Changes Access Control Password Policy Changes Policy Changes Configuration Changes System Access Configuration Management System Integrity

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; **(d)** a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	or accidental Active Directory changes to a previous state and restore deleted objects when needed, without any domain controller downtime or having to restore from backup.	Policy Changes Configuration Changes **[Process]** Establish and maintain continuous control over IT infrastructure changes, configurations and data access with Netwrix Auditor using all report categories. **[Process]** Restore a working/safe configuration of Active Directory with the Active Directory Object Restore feature of Netwrix Auditor.
Article 32. §2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.	Review Netwrix Auditor reports to track all changes and all data access in a particular IT system to assess risks to the confidentiality, integrity and availability of personal data. Enable timely detection of any user actions that violate your data protection policies by subscribing to the following reports: Files and Folders Deleted, Data Deletions, Files and Folders Moved, Files and Folders Renamed, and Files Copied.	**[Report Categories]** Audit Trail All Changes Access Control Data Access Group Membership Changes Permission Changes Privileged Users Management Data Integrity Data Governance Data Changes Integrity Monitoring Data Integrity
Article 32. §4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do	Subscribe to the Activity Outside Business Hours report to stay aware of any employees who are active on the network at the time when they are not supposed to perform any actions. Periodically review the Access to Archive Data report to detect a suspiciously high number of file reads in your archive storage, which might indicate malicious activity. Periodically verify the appropriateness of user access rights by reviewing each user's assigned	**[Report Categories]** Access Control System Access Data Access User Activity Account Management Data Access Permission States

so by Union or Member State law.	permissions to files and folders against HR employee listings and employee job descriptions using the Account Permissions report. Review the Excessive Access Permissions report to verify that no excessive access rights are assigned to employees beyond those needed for their primary job responsibilities. Use the video recording capability of Netwrix Auditor to capture the screen activity of privileged users in critical IT systems and applications (in particular, those that do not log events); use the video recording notification feature to notify users that their activity can be monitored and recorded, which fosters appropriate use of systems and data.	
Article 33. §1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority…	Use preconfigured alerts to respond quickly to threat patterns that violate corporate security policies and indicate possible cyber security incidents, including a personal data breach. The notifications, which you can easily customize, are sent to the specified emails as the events occur, enabling you to rapidly react to a possible data breach and notify authorities promptly. Use report subscriptions to automate delivery of critical audit reports to a set of email addresses or a designated network folder daily or on any other schedule. Each report can be delivered to multiple recipients at the same time without the need to configure each subscription separately.	**[Process]** Establish an effective early warning system with the alerting feature of Netwrix Auditor. **[Process]** Enable continuous monitoring of critical IT systems and ongoing review of critical reports with the report subscription feature of Netwrix Auditor.

Control Processes and Report Categories

Control Processes Facilitated by Netwrix Auditor

From a compliance perspective, IT operations can be viewed and managed as a collection of control processes. Such processes enable 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 are 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 a 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

The tables below detail the predefined reports in each category.

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
Data Integrity	Files and Folders Moved	File Servers	Secondary

Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	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	Exchange Online	Primary

	Events by User		
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
Data Integrity	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	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	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	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	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	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	Files and Folders Moved	File Servers	Secondary
Data Integrity	Files and Folders Renamed	File Servers	Secondary
Data Integrity	Files Copied	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	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