netwrix

GDPR Requirements

and Netwrix Auditor Mapping

About the GDPR

The General Data Protection Regulation (GDPR) is a legal act of the European Parliament and the Council that was adopted in April 2016 and came into force on May 25, 2018. The GDPR, formally known as Regulation (EU) 2016/679, 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 replaces Directive 95/46/EC, which had been inconsistently interpreted by the various European Union member states since it was enacted in 1995.

The GDPR does far more than harmonize data protection law across the EU, however; it also has extraterritorial application. All organizations — even those not based in the EU — that offer goods or services to, or monitor the behavior of, European Union residents and therefore process any of their personal data are subject to GDPR compliance.

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

- **Extended rights of data subjects** — These rights include the right of access, the right to data portability and the right to data erasure.
- **72-hour data breach notification** — If an organization suffers a personal data breach, it must notify the supervisory authority within 72 hours of becoming aware of it.
- **Privacy by design** — During both the planning and implementation phases of any new product or service, organizations must ensure that GDPR data protection principles and appropriate safeguards are addressed.
- **Accountability** — Organizations 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 the provisions of the GDPR articles to Control Processes

The following table lists some of the key data protection 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. Principles

GDPR Provision (Extracts. For the full text, refer to the original publication.)	Control Process
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').	**Identification and Authentication** **Access Control** **Configuration Management** **System and Information Integrity** (To address this broad provision, an organization needs to implement a wide set of security procedures and organizational improvements from several different control families; no particular control process alone can ensure compliance with this requirement.)
Article 5. §2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').	**Audit and Accountability**

GDPR Chapter III. Rights of the data subject

GDPR Provision (Extracts. For the full text, refer to the original publication.)	Control Process
Article 15. §1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: **(b)** the categories of personal data concerned;	**System and Information Integrity** • Information Management and Retention

Article 16. The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	**System and Information Integrity** • Information Management and Retention
Article 17. §1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay...	**System and Information Integrity** • Information Management and Retention
Article 20. §1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided...	**System and Information Integrity** • Information Management and Retention

GDPR Chapter IV. Controller and processor

GDPR Provision (Extracts. For the full text, refer to the original publication.)	Control Process
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.	**Audit and Accountability**

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.

Identification and Authentication

Access Control

Incident Response

Risk Assessment

- Risk Assessment
- Security Categorization

System and Information Integrity

(To address this broad provision, an organization needs to implement a wide set of security procedures and organizational improvements from several different control families; no particular control process alone can ensure compliance with this requirement.)

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.

Access Control

- Access Enforcement
- Least Privilege

Incident Response

- Incident Detection

Risk Assessment

- Risk Assessment
- Security Categorization

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;
> **(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.

Identification and Authentication

Access Control

Configuration Management

Incident Response

Risk Assessment

- Risk Assessment
- Security Categorization

System and Information Integrity

(To address this broad provision, an organization needs to implement a wide set of security procedures and organizational improvements from several different control families; no particular control process alone can ensure compliance with this requirement.)

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.	**Risk Assessment** • Risk Assessment • Security Categorization
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 so by Union or Member State law.	**Access Control** • Account Usage Monitoring **Configuration Management** • Access Restrictions for Changes **Incident Response** • Incident Detection • Incident Analysis **System and Information Integrity** • Information System Monitoring
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...	**Incident Response** • Incident Detection
Article 33. §3. The notification referred to in paragraph 1 shall at least: **(a)** describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;	**Incident Response** • Incident Detection • Incident Analysis
Article 34. §1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	**Incident Response** • Incident Detection • Incident Analysis

Control Processes

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.

Identification and Authentication

The objective of the identification and authentication controls is to ensure that all users and devices accessing information systems are uniquely identifiable and their authenticity is verified before the system grants access. Identification and authentication are crucial for ensuring accountability of individual activity in the organizational information systems.

User Identification

Audit the identification and authentication processes for users who access your information systems.

How to Implement Control	Applicable Netwrix Features
Cross-reference HR data with Active Directory user accounts in order to: • Ensure that each user with a business need to access your information systems has a unique account. • Identify personal accounts that cannot be traced to a particular individual.	Active Directory State-in-Time reports • User Accounts
Review audit trails to check whether the use of shared accounts complies with your policies.	User Behavior and Blind Spot Analysis reports • Logons by Single User from Multiple Endpoints Interactive Search • Who = *shared account*

Correlate employee absence data (typically from HR) with the access audit trail to spot suspicious activity.	Active Directory – Logon Activity reports • All Logon Activity Interactive Search • Action = *Interactive Logon*

Device Identification

Audit the identification and authentication processes for devices used to access your information systems.

How to Implement Control	Applicable Netwrix Features
Crosscheck the IT inventory against the list of computer accounts in Active Directory.	Active Directory — State-in-Time reports • Computer Accounts
Review all computer domain joins and all account creations, modifications and deletions to spot any unauthorized changes to computer accounts.	Active Directory Changes reports • Computer Account Changes Interactive Search • Object Type = *Computer*
Audit dynamic address allocation to devices by monitoring the DHCP server for: • DHCP scopes • Lease parameters and assignments	Interactive Search • Object Type = *DHCP Scope*
Audit remote network connections to identify unauthorized remote devices.	Netwrix Auditor Add-on for RADIUS Server Active Directory - Logon Activity reports

Identifier Management

Audit provisioning, modification and de-provisioning of users and groups.

How to Implement Control	Applicable Netwrix Features
Review the creation, modification and deletion of users and groups to spot: • Unauthorized changes • Identifiers that do not comply with your naming standards and policies (e.g., no public, generic or reused identifiers)	Active Directory Changes reports • User Account Changes Active Directory Changes reports • Security Group Changes Interactive Search • Object Type = *Group* | *User*
Configure alerts to notify designated personnel about unauthorized account changes.	Custom alerts for user account modifications

Authenticator Management

Review changes to password policy requirements, and audit user and admin activity for policy compliance.

How to Implement Control	Applicable Netwrix Features
Audit changes to account policy settings to spot inappropriate or unauthorized modifications. Settings to check include: • Account lockout threshold, duration and status reset • Max/min password age • Enforce password history • Enforce strong passwords • Irreversible password encryption	Active Directory – Group Policy Changes reports • Account Policy Changes • Password Policy Changes • GPO Link Changes Active Directory Group Policy State-in-Time reports • Account Policies
Alert designated personnel about Group Policy changes related to account passwords.	Predefined Alerts • Password Tampered
Audit administrative password resets to spot unauthorized or suspicious changes.	Active Directory Changes reports • Password Resets by Administrator
Correlate new user account creation with account password resets to ensure that users change their initial password on first logon.	Active Directory Changes reports • User Account Changes (added) • User Password Changes Interactive Search • Details Contains 'Password Reset'
Ensure that accounts with credentials reported lost or compromised are promptly reset or disabled according to policy.	Active Directory Changes reports • User Account Status Changes • Password Resets by Administrator

Access Control

The goal of access control measures is to ensure that information system accounts are properly managed and that access is granted based on the principle of least privilege. Netwrix Auditor supports access control by enabling full visibility into account provisioning and deprovisioning, permissions management, and user activity.

Account Management Audit

Audit the creation, modification, enabling, disabling and removal of user accounts.

How to Implement Control	Applicable Netwrix Features
Review changes to user accounts on key information systems to spot deviations from your account management policies and procedures.	Active Directory Changes reports • User Account Changes • User Account Status Changes • Recently Enabled Accounts • Temporary User Accounts Azure AD reports • User Account Management in Azure AD Oracle Database reports • Account Management Windows Server Changes reports • Local Users and Groups Changes
Alert designated security personnel whenever a sensitive account is changed.	Predefined alerts • Account Enabled • Account Disabled • Account Deleted • Security Changes on Windows Server

Account Usage Monitoring

Monitor user activity for abnormal or suspicious events.

How to Implement Control	Applicable Netwrix Features
Review user logons and resource access on a regular basis to spot abnormal account use and violations of account use policy.	Activity Summary email notifications User Behavior and Blind Spot Analysis reports • Temporary User Accounts • Recently Enabled Accounts • Access to Archive Data • Data Access Surges • Activity Outside Business Hours • Failed Activity Trend • Logons by Multiple Users from Single Endpoint

	• Logons by Single User from Multiple Endpoints • Non-owner Mailbox Access
Review user access to sensitive and regulated data to detect access policy violations.	Data Discovery and Classification reports • Sensitive Files and Folders Permissions Details • Most Accessible Sensitive Files and Folders
Enable designated security personnel to respond promptly to potential access abuse.	Predefined alerts • Logon to a Specific Machine • Logon Attempt to a Disabled Account • Multiple Failed Logons Interactive Search • Who = *suspicious account*
Review audit trails to spot use of shared accounts that violates your policies.	User Behavior and Blind Spot Analysis reports • Logons by Single User from Multiple Endpoints Interactive Search • Who = *shared account*

Inactive Accounts

Disable unused accounts after a defined period of inactivity.

How to Implement Control	Applicable Netwrix Features
Identify dormant or orphaned user and computer accounts and handle them appropriately according to policy.	Inactive User Tracker tool, which can identify unused accounts and automatically: • Notify the manager • Disable the account • Change the password • Move the account to a specified OU • Remove the account Active Directory State-in-Time reports • User Accounts – Last Logon Time

Role and Group Assignment

Review group and role assignments to ensure that user accounts meet established membership conditions and the principle of least privilege.

How to Implement Control	Applicable Netwrix Features
Ensure that users are added security groups and access roles in accordance with the least privilege principle and only with proper authorization.	Active Directory Changes reports • Security Group Membership Changes Azure AD reports • Group Membership Changes in Azure AD Active Directory State-in-Time reports • Group Members • Effective Group Membership Windows Server State-in-Time reports • Local Users and Groups
Monitor privileged group and role assignments to prevent unauthorized privilege escalation, and regularly review the membership of these groups and roles to validate the need for privileged access.	Active Directory Changes reports • Administrative Group Membership Changes User Behavior and Blind Spot Analysis reports • Temporary Users in Privileged Groups Windows Server Changes reports • Local Users and Groups Changes Active Directory State-in-Time reports • Administrative Group Members Windows Server State-in-Time reports • Members of Local Administrators Group Oracle Database reports • Privilege Management SQL Server reports • All SQL Server Activity by Object Type (Object Type = *Server Role* | *Database Role* |*Application Role*) Predefined alerts • Group Membership Changes

Personnel Status Changes

Ensure proper handling of the accounts and access permissions of temporary, transferred or terminated employees.

How to Implement Control	Applicable Netwrix Features
Review audit trails to confirm that the user accounts of temporary and terminated employees are disabled or removed in all information systems and applications according to your policy.	Active Directory Changes reports • User Account Changes • User Account Status Changes
Review current access permissions of transferred or reassigned employees with particular attention on sensitive and regulated data to ensure they do not exceed their new job requirements.	Active Directory Changes reports • User Account Changes Active Directory State in Time reports • Users and Computers - Effective Group Membership Data Discovery and Classification reports • Sensitive File and Folder Permissions Details

Access Enforcement

Ensure user permissions comply with your access control policies.

How to Implement Control	Applicable Netwrix Features
Review access permissions for sensitive information assets on a regular basis to identify and rectify the following: • Excessive permissions • Permissions assigned directly, rather than through roles and groups • Broken permission inheritance	User Behavior and Blind Spot Analysis • Data Access • Excessive Permissions File Servers State-in-Time reports • Folder and File Permission Details • Folder Permissions SharePoint State-in-Time reports • SharePoint Object Permissions • SharePoint Site Collections with Broken Inheritance • SharePoint Objects with Broken Inheritance Data Discovery and Classification reports • Sensitive Files and Folders by Owner • Sensitive File and Folder Permissions Details

Audit and alert on changes to permissions in order to promptly spot any improper or authorized modifications.	Predefined alerts • File Share Permissions Changed • Object Permissions Changed in Active Directory • Security Changes on Windows Server Activity Summary email notifications

Least Privilege

Maintain user access permissions based on the principle of least privilege.

How to Implement Control	Applicable Netwrix Features
Regularly review access rights granted to users and roles to ensure users have only the permissions they need to do their jobs.	User Behavior and Blind Spot Analysis reports • Excessive Permissions Active Directory Changes reports • Object Security Changes • Security Group Changes Active Directory State-in-Time reports • Account Permissions in Active Directory • Object Permissions in Active Directory • Users and Computers - Effective Group Membership Group Policy Changes reports • User Rights Assignment Policy Changes • Security Settings Changes Exchange Server reports • Mailbox Delegation and Permissions Changes File Servers Activity reports • Permissions Changes File Servers State-in-Time reports • Account Permissions • Excessive Access Permissions • Folder and File Permission Details • Folder Permissions Windows Server Changes reports • File Share Changes SharePoint Activity reports • SharePoint Permission Changes by User SharePoint State-in-Time reports • Account Permissions in SharePoint • SharePoint Site Collections Accessible by User Account

Ensure that privileged accounts are restricted to the specific users and roles who need access to security-related functions on the information systems.	Predefined alerts • User Added to AD Administrative Group • User Added to Windows Server Administrative Group
Ensure that privileged administrative accounts are used exclusively for performing security-related tasks.	Interactive Search • Who = *privileged account* • Use the In Group search filter to look for activity of all members of a privileged group Windows Server User Activity reports • User activity video recording (available even for systems and applications that do not produce logs)

Remote Access

Monitor remote access connections to ensure they conform to organizational secure access policies.

How to Implement Control	Applicable Netwrix Features
Review detailed remote access logon events along with AD logon activity.	Interactive Search • (Object Type = *RADIUS Logon*) Active Directory - Logon Activity reports Netwrix Auditor Add-on for RADIUS Server Network Devices reports • VPN Logon Attempts
Monitor changes to security groups used for remote access authorization.	Active Directory Changes reports • Security Group Membership Changes Interactive Search • Object Type = *Group* AND What CONTAINS *GroupID* Predefined alerts • Group Membership Changes

Wireless Access

Monitor wireless network connections for conformance with your wireless networking policies.

How to Implement Control	Applicable Netwrix Features
Monitor wireless connections to your networks.	Network Devices reports
Monitor your wireless networking policies for unauthorized or inappropriate changes.	Active Directory – Group Policy Changes reports • Wireless Network Policy Changes

Use of External Information Systems

Control the use of external information systems, including cloud-based services.

How to Implement Control	Applicable Netwrix Features
Audit user activity in SharePoint Online, Exchange Online and OneDrive for Business in order to discover and prevent violations of your information handling policies, such as the storing of sensitive data outside of your control boundaries.	Office 365 Overview Dashboards SharePoint Online reports • All SharePoint Online Activity by User • Content Management • Data Access • Sharing and Security Changes User Behavior and Blind Spot Analysis reports • Information Disclosure • Suspicious Files

Audit and Accountability

Audit and accountability measures are intended to maintain a trail of activity in information systems that ensures individuals can be held accountable for their actions. Netwrix Auditor directly implements many of the audit and accountability requirements by capturing a complete audit trail and securely storing it for more than 10 years, enabling easy access to audit information for investigations and compliance reviews, and enabling video recording of user activity in systems that do not produce audit events.

Audit Record Generation

Generate audit records containing information that establishes what type of event occurred, when and where it occurred, the source of the event, the outcome of the event, and the identity of any individuals associated with the event.

How to Implement Control	Applicable Netwrix Features
Collect detailed records (including Who, What, When, Where and Where details) of events in your information systems and applications.	 A complete audit trail from across all IT systems and applications  Data-in API, which enables creation of add-ons for integrating Netwrix Auditor with other systems and applications
Adjust the data collection settings to ensure the audit trail contains all required details.	 Review reports and Interactive Search results and fine-tune monitoring plans as needed

Audit Record Retention

Retain audit records for the time period required by your record retention policy or by compliance regulations.

How to Implement Control	Applicable Netwrix Features
Store your audit data in a way that ensures easy access for incident investigations while meeting long-term retention requirements specified by your policies or regulatory mandates.	 AuditArchive™, a two-tiered storage that provides: • SQL Server audit database for operational reporting (data is stored for 180 days by default) • Separate file-based archive for long-term storage of audit data (data is stored for 10 years by default)

Audit Trail Review

Regularly review audit records for indications of inappropriate or unusual activity and report findings to appropriate personnel, such as your incident response team or InfoSec group.

How to Implement Control	Applicable Netwrix Features
Regularly review a consolidated audit trail across your critical information systems.	Predefined change and activity reports Activity Summary email notifications Interactive Search
Export reports for evidence when reporting inappropriate or unusual activity to responsible security staff.	Export of reports to a variety of formats, including PDF and Microsoft Excel
Configure alerts to automatically trigger incidents in your IT service support management (ITSSM) solution.	Netwrix Auditor Add-On for ServiceNow Incident Management (ticket creation)
Add audit records from other key systems and applications to your system-wide, time-correlated audit trail.	Netwrix Auditor Add-On for Linux Systems Netwrix Auditor Add-On for Privileged User Monitoring on Linux and Unix Systems Netwrix Auditor Add-On for RADIUS Server Data-in API, which enables creation of add-ons for integrating Netwrix Auditor with other systems and applications

Report Generation and Audit Reduction

Provide summary reports to support on-demand audit review, analysis and reporting requirements and incident investigations without altering the original audit logs.

How to Implement Control	Applicable Netwrix Features
Aggregate audit records from multiple information systems.	Enterprise Overview Dashboards, Overview Diagrams, Organization Level reports, predefined change and activity reports Activity Summary email notifications
Generate custom reports on events of interest across all monitored systems.	Reports based on Interactive search results

Protection of Audit Information

Protect audit information and audit tools from unauthorized access, modification and deletion.

How to Implement Control	Applicable Netwrix Features
Protect audit information by storing it in a physically separate repository.	AuditArchive™, a two-tiered storage that provides: • SQL Server audit database for operational reporting • Separate file-based archive for long-term storage of audit data
Restrict access to audit records and tools by assigning security personnel to operational roles using the least privilege principle	Role delegation for audit configuration and review, both on the global level and on the individual monitoring plan level
Monitor changes to your audit configuration settings to spot modification that could reduce the level of audit, either intentionally or by accident.	Group Policy Changes reports • Audit Policy Changes Windows Server Changes reports • Audit Log Clearing report • Local Audit Policy Changes report

Session Audit

Capture user activity for audit purposes.

How to Implement Control	Applicable Netwrix Features
Record user activity in mission-critical systems.	Windows Server User Activity reports • User activity video recording (available even for systems and applications that do not produce logs)

Response to Audit Processing Failures

Monitor for audit processing failures and take corrective actions to restore normal audit capturing process.

How to Implement Control	Applicable Netwrix Features
Monitor the status of audit data collection across managed systems and audit storage capacity on a regular basis	Health Status dashboard Health Summary report
Alert designated personnel about audit failures.	Event Log Manager • System health alerts

Configuration Management

Configuration management is required to ensure that the configuration of information systems complies with internal policies and external regulations, and that all changes are both proper and authorized.

Baseline Configuration

Establish and maintain baseline configurations and inventories of organizational information systems.

How to Implement Control	Applicable Netwrix Features
Review the configuration of your Windows servers and identify deviations from the established baseline.	Windows Server State-in-Time reports • Windows Server Inventory • Windows Server Configuration Details • Members of Local Administrators Group

Configuration Change Control

Audit changes to the configuration of your information systems.

How to Implement Control	Applicable Netwrix Features
Review changes to the server and network infrastructure to ensure that only authorized changes are being implemented in accordance with you change management procedures.	Windows Server Changes reports • All Windows Server Changes Active Directory – Group Policy Changes VMware reports • All VMware change SharePoint reports • SharePoint Configuration Changes Exchange reports • Database Changes • New Exchange Servers Network Devices reports • Configuration Changes on Network Devices • Logons to Network Devices Interactive Search • Source = *Windows Server* • Source = *Policy* • Source = *Netwrix API*
Identify inappropriate or unapproved changes (e.g., installation of non-approved software).	Windows Server Changes reports • All Windows Server Changes with Review Status
Alert designated security personnel to critical change events to enable timely response.	Custom alerts on specific configuration changes

Access Restrictions for Changes

Establish and enforce logical access restrictions associated with changes to the information system.

How to Implement Control	Applicable Netwrix Features
Ensure that information system configuration is limited to authorized users by reviewing privileged security groups and monitoring changes to their membership.	Windows Server State-in-Time reports • Members of Local Administrator Group • Local Users and Groups Windows Server Changes reports • Local Users and Groups Changes Predefined alerts • User Added to Windows Server Administrative Group

User-Installed Software

Control and monitor user-installed software.

How to Implement Control	Applicable Netwrix Features
Exercise security control over programs and applications on your critical Windows Servers by maintaining an inventory of resident software and ensuring that only permitted software is installed.	Windows Server State-in-Time reports • Windows Server Configuration Details • Installed Software

Incident Response

Incident response controls prescribe careful planning of response measures to security incidents on the organizational level, along with proper training of personnel and regular testing of the plan. The plan should cover incident detection, analysis, containment and recovery. Netwrix Auditor capabilities relating to incident response revolve around the detection (including automated response triggering through the ServiceNow integration) and analysis aspects of security incident handling.

Incident Detection

Detect security incidents in a timely manner.

How to Implement Control	Applicable Netwrix Features
Regularly review user activity (system logons, resource access, configuration changes) across information systems to spot abnormal behavior that could lead to a security breach.	Behavior Anomalies Discovery • Top users with behavior anomalies • Detailed trail of user anomalous behavior User Behavior and Blind Spot Analysis reports • Temporary User Accounts • Recently Enabled Accounts • Access to Archive Data • Data Access Surges • Activity Outside Business Hours • Failed Activity Trend • Logons by Multiple Users from Single Endpoint Data Discovery and Classification reports • Activity Related to Sensitive Files and Folders
Configure alerts to automatically notify designated security staff of a potential incident or initiate an automated response script, based on either a triggering event or a defined threshold.	Predefined alerts • User Account Locked Out • User Added to AD Administrative Group • User Added to Windows Server Administrative Group • Unrestricted Access to the File Share Custom alerts based on either a triggering event or a defined threshold Automated Response

Incident Analysis

Investigate anomalous activity and events that are detected.

How to Implement Control	Applicable Netwrix Features
Perform forensic analysis of each potential security incident to understand its full scope and impact on information systems and protected data, and determine appropriate response measures including reporting of the incidents within the organization and to authorities and affected parties.	Interactive Search • Who and Where filters Windows Server User Activity reports • Replay of user activity video recordings Behavior Anomalies Discovery • Detailed trail of user anomalous behavior Data Discovery and Classification reports • Activity Related to Sensitive Files and Folders
Adjust alerts settings or create new alerts based on findings from the security incident analysis.	Custom alerts based on Interactive Search

Incident Mitigation

Respond quickly to a security incident to mitigate its effects.

How to Implement Control	Applicable Netwrix Features
Automate the triggering of incident response procedures upon detection of suspicious activity to ensure timely response and remediation.	Netwrix Auditor Add-On for ServiceNow Incident Management
Ensure instant response to anticipated incidents by scripting.	Automated Response on alerts
Quickly revert unauthorized changes to accounts and configuration.	Predefined change reports • Before and after details Object Restore for Active Directory tool

Risk Assessment

Every organization needs to conduct information system risk assessments to understand the likelihood and magnitude of harm from various threats so they can prioritize them and mitigate risk to an acceptable level. Netwrix Auditor reports on configuration risk factors common in Microsoft-centric IT infrastructures and estimates their impact in your environment. In addition, the data discovery and classification functionality enables data risk assessments based on the sensitivity of the information stored and processed by the organizational information systems.

Risk Assessment

Regularly assess risks to your information systems and act on the findings.

How to Implement Control	Applicable Netwrix Features
Examine the configuration of your information systems using common security best practices and identify risks that may require mitigation in the following areas: • Account management • Data governance • Security permissions	IT Risk Assessment Overview dashboard with drill-down reports • Users and Computers • Data • Permissions
Review the results of data discovery and classification to assess the risks posed by sensitive data not being stored and processed according to the established data security policy.	Data Discovery and Classification reports • Overexposed Files and Folders • Most Accessible Sensitive Files and Folders • Sensitive Files Count by Source • File and Folder Categories by Object DDC Collector console provides simple reporting capabilities that help identify sensitive content stored across file servers, SharePoint sites, SQL databases, cloud storage and content management systems.

Security Categorization

Conduct the security categorization process for the data hosted by the organization.

How to Implement Control	Applicable Netwrix Features
Perform automated discovery of relevant types of sensitive and regulated data in order to prioritize data protection measures.	DDC Collector Console that enables you to adjust predefined data categorization rules or define new rules.

System and Information Integrity

System and information integrity measures aim to protect information systems and the data they store and process from being compromised by outsider attackers and malicious insiders. Netwrix Auditor reports and alerts on user behavior indicative of an attack or unauthorized use of information systems.

Information System Monitoring

Monitor your information systems for indicators of potential attacks and unauthorized activity.

How to Implement Control	Applicable Netwrix Features
Spot and investigate anomalies in user behavior in time to block external attackers who have compromised valid user accounts, as well as trusted insiders who have gone rogue.	Behavior Anomalies Discovery • List of users with the most behavior anomalies • Detailed trail of each user's anomalous actions
Configure alerts to automatically notify designated security staff of a potential attack or unauthorized activity.	Predefined alerts • User Account Locked Out • User Added to AD Administrative Group • User Added to Windows Server Administrative Group • Unrestricted Access to the File Share Custom alerts based on either a triggering event or a defined threshold

Information Management and Retention

Manage and retain sensitive personal information in accordance with applicable laws, regulations and operational requirements.

How to Implement Control	Applicable Netwrix Features
Ensure that personally identifiable and other sensitive information in the organizational data repositories is appropriately secured, including protection against unauthorized disclosure or accidental loss.	Data Discovery and Classification reports • Overexposed Files and Folders • Most Accessible Sensitive Files and Folders • Sensitive File and Folder Permissions Details Data Remediation Workflows enable automatic response actions including sensitive content redaction, documents quarantining, permission lockdown and email notifications. Classification Tagging enables integration with DLP solutions to enforce data protection policies using persistent classification tags.
Monitor for personally identifiable and other sensitive information in the organizational data repositories, which exceeds its legitimate retention time.	Data Discovery and Classification reports • Sensitive Files Count by Source • File and Folder Categories by Object Data Remediation Workflows help to enforce data retention polices based on document classification. Policy actions may include migration or removal of obsolete data, email notification to initiate disposition review, etc.
Establish processes and procedures to support customers wishing to exercise their data subject rights: • Right of access • Right to rectification • Right to erasure (right to be forgotten) • Right to portability	DDC Collector Console enables you to locate personal data instances across file servers, SharePoint sites, SQL databases, cloud storage and content management systems.

Data Sanitization

Perform data sanitization on sensitive information outside of authorized storage boundaries.

How to Implement Control	Applicable Netwrix Features
Implement appropriate de-identification, redaction or similar measures to comply with legal obligations and mitigate the risk of unauthorized data access.	Data Remediation Workflows enable automatic document redaction to mask sensitive information and/or move the file to a designated secure location.

About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

Netwrix Auditor is an agentless data security platform that empowers organizations to accurately identify sensitive, regulated and mission-critical information and apply access controls consistently, regardless of where the information is stored. It enables them to minimize the risk of data breaches and ensure regulatory compliance by proactively reducing the exposure of sensitive data and promptly detecting policy violations and suspicious user behavior.

For more information, visit www.netwrix.com.

If you want to evaluate Netwrix Auditor in your environment, choose one of the deployment options below. To see Netwrix Auditor in action without having to download and install it, visit netwrix.com/browser_demo.

On-Premises Deployment

Download a
Free 20-day trial

netwrix.com/go/freetrial

Virtual Appliance

Download our
virtual machine image

netwrix.com/go/appliance

Cloud Deployment

Deploy Netwrix Auditor
in the cloud

netwrix.com/go/cloud

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

netwrix.com/social