

ISO/IEC 27001 Controls

and Netwrix Functionality Mapping



About ISO/IEC 27001

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

ISO/IEC 27001:2005 was the first edition of the standard. This edition was technically revised in 2013 and replaced by the current version of the standard, ISO/IEC 27001:2013.

ISO/IEC 27001:2013 has 14 security control sections collectively containing a total of 35 main security categories and 114 controls.

This document is for informational purposes only and does not constitute a commitment from Netwrix Corporation of any features or functions. Netwrix hereby disclaims all warranties related to the information in this document, whether express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. This document does not provide you with any legal rights to any intellectual property in any Netwrix product or service. You may copy and use this document only for your internal, reference purposes.

© 2019 Netwrix Corporation. All rights reserved. The Netwrix name, logo, products, service names, slogans and all Netwrix trademarks are the property of Netwrix Corporation.

Mapping of the provisions of the ISO/IEC 27001 information security controls to Control Processes

The following table lists some of the key controls of the ISO/IEC 27001 and explains how Netwrix can help your organization implement those controls and achieve compliance with ISO/IEC 27001. Please note that the efforts and procedures required to comply with ISO/IEC 27001 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 ISO/IEC 27001 compliance, and not all the controls that Netwrix 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.

A.6 Organization of information security

Control Description	Control Process
A.6.2.1 Mobile device policy A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	<u>Access Control</u> <ul style="list-style-type: none"> Remote Access Wireless Access
A.6.2.2 Teleworking A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	<u>Access Control</u> <ul style="list-style-type: none"> Remote Access

A.8 Asset management

Control Description	Control Process
A.8.2.1 Classification of information Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	<u>Risk Assessment</u> <ul style="list-style-type: none"> Security Categorization

A.9 Access control

Control Description	Control Process
A.9.1.2 Access to networks and network services Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	<u>Access Control</u> <ul style="list-style-type: none"> Access Enforcement

A.9.2.1 User registration and de-registration

A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

Identification and Authentication

- [User Identification](#)
- [Identifier Management](#)
- [Authenticator Management](#)

Access Control

- [Account Management Audit](#)
- [Account Usage Monitoring](#)

A.9.2.2 User access provisioning

A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

Access Control

- [Account Management Audit](#)
- [Account Usage Monitoring](#)

A.9.2.3 Management of privileged access rights

The allocation and use of privileged access rights shall be restricted and controlled.

Access Control

- [Role and Group Assignment](#)

Configuration Management

- [Configuration Change Control](#)

A.9.2.4 Management of secret authentication information of users

The allocation of secret authentication information shall be controlled through a formal management process.

Identification and Authentication

- [Authenticator Management](#)

Access Control

- [Account Usage Monitoring](#)

A.9.2.5 Review of user access rights

Asset owners shall review users' access rights at regular intervals.

Access Control

- [Role and Group Assignment](#)
- [Least Privilege](#)

A.9.2.6 Removal or adjustment of access rights

The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Access Control

- [Inactive Accounts](#)
- [Personnel Status Changes](#)

A.9.3.1 Use of secret authentication information

Users shall be required to follow the organization's practices in the use of secret authentication information.

Identification and Authentication

- [Authenticator Management](#)

Access Control

- [Account Usage Monitoring](#)

A.9.4.2 Secure log-on procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

Access Control

- [Account Usage Monitoring](#)

A.9.4.3 Password management system

Password management systems shall be interactive and shall ensure quality passwords.

A.9.4.5 Access control to program source code

Access to program source code shall be restricted.

Identification and Authentication

- [Authenticator Management](#)

Access Control

- [Account Usage Monitoring](#)

Configuration Management

- [Configuration Change Control](#)

A.12 Operations security

Control Description

A.12.1.2 Change management

Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.

A.12.4.1 Event logging

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.4.2 Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorized access.

A.12.4.3 Administrator and operator logs

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

A.12.5.1 Installation of software on operational systems

Procedures shall be implemented to control the installation of software on operational systems.

Control Process

Configuration Management

- [Configuration Change Control](#)

Access Control

- [Account Management Audit](#)

Audit and Accountability

- [Audit Record Generation](#)
- [Audit Record Retention](#)
- [Audit Trail Review](#)
- [Session Audit](#)

Audit and Accountability

- [Protection of Audit Information](#)

Audit and Accountability

- [Audit Record Generation](#)
- [Audit Trail Review](#)
- [Protection of Audit Information](#)
- [Session Audit](#)

Configuration Management

- [Configuration Change Control](#)

A.13 Communications security

Control Description	Control Process
A.13.1.1 Network controls Networks shall be managed and controlled to protect information in systems and applications.	<u>Access Control</u> <ul style="list-style-type: none"> • Remote Access • Wireless Access
A.13.2.1 Information transfer policies and procedures Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	<u>Access Control</u> <ul style="list-style-type: none"> • Remote Access • Wireless Access • Use of External Information Systems

A.14 System acquisition, development and maintenance

Control Description	Control Process
A.14.2.2 System change control procedures Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	<u>Configuration Management</u> <ul style="list-style-type: none"> • Configuration Change Control
A.14.2.4 Restrictions on changes to software packages Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	<u>Configuration Management</u> <ul style="list-style-type: none"> • Configuration Change Control

A.16 Information security incident management

Control Description	Control Process
A.16.1.2 Reporting information security events Information security events shall be reported through appropriate management channels as quickly as possible.	<u>Audit and Accountability</u> <ul style="list-style-type: none"> • Audit Trail Review
A.16.1.4 Assessment of and decision on information security events Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	<u>Audit and Accountability</u> <ul style="list-style-type: none"> • Audit Trail Review <u>Incident Response</u> <ul style="list-style-type: none"> • Incident Detection • Incident Analysis

A.16.1.5 Response to information security incidents

Information security incidents shall be responded to in accordance with the documented procedures.

A.16.1.7 Collection of evidence

The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

Incident Response

- [Incident Analysis](#)
- [Incident Mitigation](#)

Audit and Accountability

- [Audit Record Retention](#)

A.18 Compliance

Control Description

A.18.1.3 Protection of records

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.

A.18.1.4 Privacy and protection of personally identifiable information

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

Control Process

Audit and Accountability

- [Protection of Audit Information](#)

System and Information Integrity

- [Information Management and Retention](#)
- [Data Sanitization](#)

Control Processes

Control Processes Facilitated by Netwrix

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](#)
- [Access Control](#)
- [Audit and Accountability](#)
- [Configuration Management](#)
- [Incident Response](#)
- [Risk Assessment](#)
- [System and Information Integrity](#)

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
<p>Cross-reference HR data with Active Directory user accounts in order to:</p> <ul style="list-style-type: none"> • 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. 	<div>  <div> Active Directory State-in-Time reports <ul style="list-style-type: none"> • User Accounts </div> </div>
<p>Review audit trails to check whether the use of shared accounts complies with your policies.</p>	<div> <div>  <div> User Behavior and Blind Spot Analysis reports <ul style="list-style-type: none"> • Logons by Single User from Multiple Endpoints </div> </div> <div>  <div> Interactive Search <ul style="list-style-type: none"> • Who = <i>shared account</i> </div> </div> </div>

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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Computer Account Changes  Interactive Search <ul style="list-style-type: none"> • Object Type = <i>Computer</i>
Audit dynamic address allocation to devices by monitoring the DHCP server for: <ul style="list-style-type: none"> • DHCP scopes • Lease parameters and assignments 	 Interactive Search <ul style="list-style-type: none"> • Object Type = <i>DHCP Scope</i>
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: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • User Account Changes  Active Directory Changes reports <ul style="list-style-type: none"> • Security Group Changes  Interactive Search <ul style="list-style-type: none"> • Object Type = <i>Group User</i>
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
<p>Audit changes to account policy settings to spot inappropriate or unauthorized modifications. Settings to check include:</p> <ul style="list-style-type: none"> Account lockout threshold, duration and status reset Max/min password age Enforce password history Enforce strong passwords Irreversible password encryption 	<ul style="list-style-type: none">  Active Directory – Group Policy Changes reports <ul style="list-style-type: none"> Account Policy Changes Password Policy Changes GPO Link Changes  Active Directory Group Policy State-in-Time reports <ul style="list-style-type: none"> Account Policies
Alert designated personnel about Group Policy changes related to account passwords.	<ul style="list-style-type: none">  Predefined Alerts <ul style="list-style-type: none"> Password Tampered
Audit administrative password resets to spot unauthorized or suspicious changes.	<ul style="list-style-type: none">  Active Directory Changes reports <ul style="list-style-type: none"> Password Resets by Administrator
Correlate new user account creation with account password resets to ensure that users change their initial password on first logon.	<ul style="list-style-type: none">  Active Directory Changes reports <ul style="list-style-type: none"> User Account Changes (added) User Password Changes  Interactive Search <ul style="list-style-type: none"> Details Contains 'Password Reset'
Ensure that accounts with credentials reported lost or compromised are promptly reset or disabled according to policy.	<ul style="list-style-type: none">  Active Directory Changes reports <ul style="list-style-type: none"> 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 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 <ul style="list-style-type: none"> • User Account Changes • User Account Status Changes • Recently Enabled Accounts • Temporary User Accounts  Azure AD reports <ul style="list-style-type: none"> • User Account Management in Azure AD  Oracle Database reports <ul style="list-style-type: none"> • Account Management  Windows Server Changes reports <ul style="list-style-type: none"> • Local Users and Groups Changes
Alert designated security personnel whenever a sensitive account is changed.	 Predefined alerts <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> Active Directory Changes reports <ul style="list-style-type: none"> Security Group Membership Changes Azure AD reports <ul style="list-style-type: none"> Group Membership Changes in Azure AD Active Directory State-in-Time reports <ul style="list-style-type: none"> Group Members Effective Group Membership Windows Server State-in-Time reports <ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Active Directory Changes reports <ul style="list-style-type: none"> Administrative Group Membership Changes User Behavior and Blind Spot Analysis reports <ul style="list-style-type: none"> Temporary Users in Privileged Groups Windows Server Changes reports <ul style="list-style-type: none"> Local Users and Groups Changes Active Directory State-in-Time reports <ul style="list-style-type: none"> Administrative Group Members Windows Server State-in-Time reports <ul style="list-style-type: none"> Members of Local Administrators Group Oracle Database reports <ul style="list-style-type: none"> Privilege Management SQL Server reports <ul style="list-style-type: none"> All SQL Server Activity by Object Type (Object Type = <i>Server Role</i> <i>Database Role</i> <i>Application Role</i>) Predefined alerts <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • User Account Changes  Active Directory State in Time reports <ul style="list-style-type: none"> • Users and Computers - Effective Group Membership  Data Discovery and Classification reports <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Excessive permissions • Permissions assigned directly, rather than through roles and groups • Broken permission inheritance 	 User Behavior and Blind Spot Analysis <ul style="list-style-type: none"> • Data Access • Excessive Permissions  File Servers State-in-Time reports <ul style="list-style-type: none"> • Folder and File Permission Details • Folder Permissions  SharePoint State-in-Time reports <ul style="list-style-type: none"> • SharePoint Object Permissions • SharePoint Site Collections with Broken Inheritance • SharePoint Objects with Broken Inheritance  Data Discovery and Classification reports <ul style="list-style-type: none"> • 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.	<div> User Behavior and Blind Spot Analysis reports <ul style="list-style-type: none"> • Excessive Permissions </div> <div> Active Directory Changes reports <ul style="list-style-type: none"> • Object Security Changes • Security Group Changes </div> <div> Active Directory State-in-Time reports <ul style="list-style-type: none"> • Account Permissions in Active Directory • Object Permissions in Active Directory • Users and Computers - Effective Group Membership </div> <div> Group Policy Changes reports <ul style="list-style-type: none"> • User Rights Assignment Policy Changes • Security Settings Changes </div> <div> Exchange Server reports <ul style="list-style-type: none"> • Mailbox Delegation and Permissions Changes </div> <div> File Servers Activity reports <ul style="list-style-type: none"> • Permissions Changes </div> <div> File Servers State-in-Time reports <ul style="list-style-type: none"> • Account Permissions • Excessive Access Permissions • Folder and File Permission Details • Folder Permissions </div> <div> Windows Server Changes reports <ul style="list-style-type: none"> • File Share Changes </div> <div> SharePoint Activity reports <ul style="list-style-type: none"> • SharePoint Permission Changes by User </div> <div> SharePoint State-in-Time reports <ul style="list-style-type: none"> • Account Permissions in SharePoint • SharePoint Site Collections Accessible by User Account </div>

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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • All SharePoint Online Activity by User • Content Management • Data Access • Sharing and Security Changes  User Behavior and Blind Spot Analysis reports <ul style="list-style-type: none"> • 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 solutions directly implement 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 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: <ul style="list-style-type: none"> • 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 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: <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • Audit Policy Changes Windows Server Changes reports <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 your change management procedures.	 Windows Server Changes reports <ul style="list-style-type: none"> • All Windows Server Changes  Active Directory – Group Policy Changes  VMware reports <ul style="list-style-type: none"> • All VMware change  SharePoint reports <ul style="list-style-type: none"> • SharePoint Configuration Changes  Exchange reports <ul style="list-style-type: none"> • Database Changes • New Exchange Servers  Network Devices reports <ul style="list-style-type: none"> • Configuration Changes on Network Devices • Logons to Network Devices  Interactive Search <ul style="list-style-type: none"> • Source = <i>Windows Server</i> • Source = <i>Policy</i> • Source = <i>Netwrix API</i>
Identify inappropriate or unapproved changes (e.g., installation of non-approved software).	 Windows Server Changes reports <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> Members of Local Administrator Group Local Users and Groups  Windows Server Changes reports <ul style="list-style-type: none"> Local Users and Groups Changes  Predefined alerts <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 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.	<div> Behavior Anomalies Discovery <ul style="list-style-type: none"> • Top users with behavior anomalies • Detailed trail of user anomalous behavior </div> <div> User Behavior and Blind Spot Analysis reports <ul style="list-style-type: none"> • 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 </div> <div> Data Discovery and Classification reports <ul style="list-style-type: none"> • Activity Related to Sensitive Files and Folders </div>
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.	<div> Predefined alerts <ul style="list-style-type: none"> • User Account Locked Out • User Added to AD Administrative Group • User Added to Windows Server Administrative Group • Unrestricted Access to the File Share </div> <div> Custom alerts based on either a triggering event or a defined threshold </div> <div> Automated Response </div>

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 <ul style="list-style-type: none"> Who and Where filters Windows Server User Activity reports <ul style="list-style-type: none"> Replay of user activity video recordings Behavior Anomalies Discovery <ul style="list-style-type: none"> Detailed trail of user anomalous behavior Data Discovery and Classification reports <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 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
<p>Examine the configuration of your information systems using common security best practices and identify risks that may require mitigation in the following areas:</p> <ul style="list-style-type: none"> Account management Data governance Security permissions 	<p> IT Risk Assessment Overview dashboard with drill-down reports</p> <ul style="list-style-type: none"> Users and Computers Data Permissions Infrastructure
<p>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.</p>	<p> Data Discovery and Classification reports</p> <ul style="list-style-type: none"> Overexposed Files and Folders Most Accessible Sensitive Files and Folders Sensitive Files Count by Source File and Folder Categories by Object <p> Netwrix Data Classification provides simple reporting capabilities that help identify sensitive content stored across file servers, SharePoint sites, SQL databases, cloud storage and content management systems.</p>

Security Categorization

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




How to Implement Control	Applicable Netwrix Features
<p>Perform automated discovery of relevant types of sensitive and regulated data in order to prioritize data protection measures.</p>	<p> Netwrix Data Classification enables you to adjust predefined data categorization rules or define new rules.</p>

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 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.	<div>  Behavior Anomalies Discovery <ul style="list-style-type: none"> List of users with the most behavior anomalies Detailed trail of each user's anomalous actions </div>
Configure alerts to automatically notify designated security staff of a potential attack or unauthorized activity.	<div>  Predefined alerts <ul style="list-style-type: none"> User Account Locked Out User Added to AD Administrative Group User Added to Windows Server Administrative Group Unrestricted Access to the File Share </div> <div>  Custom alerts based on either a triggering event or a defined threshold </div>


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 <ul style="list-style-type: none"> • 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.  Data 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 <ul style="list-style-type: none"> • Sensitive Files Count by Source • File and Folder Categories by Object  Data Remediation Workflows help to enforce data retention policies 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: <ul style="list-style-type: none"> • Right of access • Right to rectification • Right to erasure (right to be forgotten) • Right to portability 	 Netwrix Data Classification 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 provides a 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 in your environment, choose one of the deployment options below. To see Netwrix 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
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