NIST CSF Controls

and Netwrix Functionality Mapping

www.netwrix.com | Toll-free: 888-638-9749

About NIST Cybersecurity Framework

NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The Framework is voluntary. It gives businesses an outline of best practices to help them decide where to focus their time and money for cybersecurity protection.

The NIST Cybersecurity Framework can be applied in a business in these five areas: Identify, Protect, Detect, Respond, and Recover. This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations or it can be focused on the delivery of critical services within an organization. Different types of entities – including sector coordinating structures, associations, and organizations – can use the Framework for different purposes.

The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program.

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.

Mapping of the NIST CSF Controls to Control Processes

The following table lists some of the key NIST CSF Controls and explains how Netwrix can help your organization implement those controls. Please note that the efforts and procedures required to establish compliance in each section may vary depending on an organization's systems configuration, internal procedures, nature of business and other factors. Implementation of the controls described below will not guarantee organizational 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.

Function: Identify (ID)

Control Description	Control Process
Asset Management (ID.AM)	
ID.AM-4: External information systems are catalogued	**Access Control** • Use of External Information Systems
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**Risk Assessment** • Security Categorization
Risk Assessment (ID.RA)	
ID.RA-1: Asset vulnerabilities are identified and documented	**Risk Assessment** • Risk Assessment **System and Information Integrity** • Information System Monitoring
ID.RA-3: Threats, both internal and external, are identified and documented	**Risk Assessment** • Risk Assessment
ID.RA-4: Potential business impacts and likelihoods are identified	**Risk Assessment** • Risk Assessment • Security Categorization
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**Risk Assessment** • Risk Assessment • Security Categorization

Function: Protect (PR)

Control Description	Control Process
Access Control (PR.AC)	
PR.AC-1: Identities and credentials are managed for authorized devices and users	**Access Control** - Role and Group Assignment - Personnel Status Changes **Identification and Authentication** - Authenticator Management - User Identification - Device Identification - Identifier Management - Inactive Accounts
PR.AC-3: Remote access is managed	**Access Control** - Remote Access - Use of External Information Systems
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**Access Control** - Remote Access - Personnel Status Changes - Access Enforcement - Role and Group Assignment - Least Privilege
Data Security (PR.DS)	
PR.DS-4: Adequate capacity to ensure availability is maintained	**Audit and Accountability** - Audit Record Generation
PR.DS-5: Protections against data leaks are implemented	**Access Control** - Role and Group Assignment - Least Privilege **System and Information Integrity** - Information System Monitoring

Information Protection Processes and Procedures (PR.IP)	
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	**Configuration Management** - Configuration Change Control - Baseline Configuration - Access Restrictions for Changes
PR.IP-3: Configuration change control processes are in place	**Configuration Management** - Configuration Change Control
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	**System and Information Integrity** - Information System Monitoring
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**Incident Response** - Incident Detection
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**Access Control** - Personnel Status Changes
PR.IP-12: A vulnerability management plan is developed and implemented	**Risk Assessment** - Risk Assessment
Protective Technology (PR.PT)	
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**Audit and Accountability**
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**Access Control** - Access Enforcement
PR.PT-4: Communications and control networks are protected	**Access Control** - Remote Access - Wireless Access

Function: Detect

Control Description	Control Process
Anomalies and Events (DE.AE)	
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	**Configuration Management** - Baseline Configuration **System and Information Integrity** - Information System Monitoring
DE.AE-2: Detected events are analyzed to understand attack targets and methods	**Audit and Accountability** - Audit Trail Review **Incident Response** - Incident Detection - Incident Mitigation **System and Information Integrity** - Information System Monitoring
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	**Audit and Accountability** - Audit Trail Review **Incident Response** - Incident Detection - Incident Analysis - Incident Mitigation **System and Information Integrity** - Information System Monitoring
DE.AE-4: Impact of events is determined	**Incident Response** - Incident Detection - Incident Mitigation **Risk Assessment** - Risk Assessment **System and Information Integrity** - Information System Monitoring

DE.AE-5: Incident alert thresholds are established	**Incident Response** - Incident Detection - Incident Analysis - Incident Mitigation
Security Continuous Monitoring (DE.CM)	
DE.CM-1: The network is monitored to detect potential cybersecurity events	**Access Control** - Role and Group Assignment - Personnel Status Changes **Audit and Accountability** - Audit Record Generation **Configuration Management** - Configuration Change Control **System and Information Integrity** - Information System Monitoring
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**Access Control** - Role and Group Assignment - Personnel Status Changes **Audit and Accountability** - Audit Record Generation **Configuration Management** - User-Installed Software
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**System and Information Integrity** - Information System Monitoring
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**Audit and Accountability** - Audit Record Generation **Configuration Management** - Configuration Change Control **System and Information Integrity** - Information System Monitoring

Detection Processes (DE.DP)	
DE.DP-2: Detection activities comply with all applicable requirements	**System and Information Integrity** • Information System Monitoring
DE.DP-4: Event detection information is communicated to appropriate parties	**Audit and Accountability** • Audit Trail Review **System and Information Integrity** • Information System Monitoring
DE.DP-5: Detection processes are continuously improved	**System and Information Integrity** • Information System Monitoring

Function: Respond

Control Description	Control Process
Response Planning (RS.RP)	
RS.RP-1: Response plan is executed during or after an event	**Incident Response** • Incident Detection • Incident Mitigation
Communications (RS.CO)	
RS.CO-2: Events are reported consistent with established criteria	**Audit and Accountability** • Audit Trail Review
RS.CO-3: Information is shared consistent with response plans	**Incident Response** • Incident Detection • Incident Mitigation **System and Information Integrity** • Information System Monitoring

Analysis (RS.AN)	
RS.AN-1: Notifications from detection systems are investigated	**Audit and Accountability** • Audit Trail Review **Incident Response** • Incident Detection • Incident Analysis • Incident Mitigation **System and Information Integrity** • Information System Monitoring
RS.AN-2: The impact of the incident is understood	**Incident Response** • Incident Detection • Incident Mitigation
RS.AN-3: Forensics are performed	**Audit and Accountability** • Report Generation and Audit Reduction **Incident Response** • Incident Detection • Incident Mitigation
RS.AN-4: Incidents are categorized consistent with response plans	**Incident Response** • Incident Detection • Incident Analysis • Incident Mitigation
Mitigation (RS.MI)	
RS.MI-1: Incidents are contained	**Incident Response** • Incident Detection • Incident Mitigation
RS.MI-2: Incidents are mitigated	**Incident Response** • Incident Detection • Incident Mitigation

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**Risk Assessment** • Risk Assessment
Improvements (RS.IM)	
RS.IM-1: Response plans incorporate lessons learned	**Incident Response** • Incident Detection • Incident Mitigation
RS.IM-2: Response strategies are updated	**Incident Response** • Incident Detection • Incident Mitigation

Function: Recover

Control Description	Control Process
Recovery Planning (RC.RP)	
RC.RP-1: Recovery plan is executed during or after an event	**Incident Response** • Incident Detection • Incident Mitigation
Improvements (RC.IM)	
RC.IM-1: Recovery plans incorporate lessons learned	**Incident Response** • Incident Detection • Incident Mitigation
RC.IM-2: Recovery strategies are updated	**Incident Response** • Incident Detection • Incident Mitigation
Communications (RC.CO)	
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	**Incident Response** • Incident Detection • Incident Mitigation

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
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 Active Directory Federation Services reports WMware – Logon Activity reports • All ESXi and vCenter 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 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 Active Directory Federation Services • Active Directory Federation Services Overview • Logons through AD FS 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 WMware – Logon Activity reports • All ESXi and vCenter Logon Activity
Review user access to sensitive and regulated data to detect access policy violations.	Data classification reports for file servers • Sensitive Files and Folders Permissions Details • Most Accessible Sensitive Files and Folders Data classification reports for SharePoint • Sensitive Data Object Permissions • Most Exposed Sensitive Data Objects Data classification reports for SharePoint Online • Sensitive Data Object Permissions • Most Exposed Sensitive Data Objects
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*
Monitor privileged accounts usage to spot abnormal or suspicious events.	Netwrix Auditor Add-on for CyberArk Privileged Access Security

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*) • SQL Server-Level Roles 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 classification reports for file servers • Sensitive File and Folder Permissions Details Data classification reports for SharePoint • Sensitive Data Object Permissions Data classification reports for SharePoint Online • Sensitive Data Object Permissions

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 SharePoint Online State-in-Time reports • SharePoint Online Object Permissions

	• SharePoint Online Broken Permissions Inheritance • SharePoint Online Objects with Broken Inheritance • SharePoint Online Site Collections External Sharing Exchange Online State-in-Time reports • Mailbox Non-Owner Permissions Details • Mailboxes Accessible by Non-Owners • User Permissions on Delegated Mailboxes SQL Server State-in-Time reports • Object Permissions in SQL Server • SQL Server-Level Roles • SQL Server Means Granted VMware State-in-Time reports • Detailed Account Privileges in vCenter • Object Permissions in v Center Data classification reports for file servers • Sensitive Files and Folders by Owner • Sensitive File and Folder Permissions Details Data classification reports for SharePoint • Sensitive Data Object Permissions Data classification reports for SharePoint Online • Sensitive Data Object Permissions
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
- SharePoint Online State-in-Time reports
  - Account Permissions in SharePoint Online
  - SharePoint Online Object Permissions
  - SharePoint Online Site Collections Accessible by User Account
- Exchange Online State-in-Time reports
  - Mailbox Non-Owner Permissions Details
  - Mailboxes Accessible by Non-Owners
  - User Permissions on Delegated Mailboxes
- SQL Server State-in-Time reports
  - Object Permissions in SQL Server
  - Account Permissions in SQL Server
  - SQL Server-Level Roles
  - SQL Server Means Granted
- VMware State-in-Time reports
  - Detailed Account Privileges in vCenter
  - Object Permissions in v Center
  - Account Permissions in vCenter

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 Netwrix Auditor Add-on for CyberArk Privileged Access Security
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) Netwrix Auditor Add-on for CyberArk Privileged Access Security

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 Exchange Online reports • All Exchange Online Changes by User User Behavior and Blind Spot Analysis reports • Information Disclosure • Suspicious Files
Monitor successful and failed authentication attempts through AD FS to keep authentication to partner resources or cloud applications visible and under control.	Active Directory Federation Services reports

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: • 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
Ensure integrity of auditing process by monitoring changes to audit scope.	Netwrix Auditor Self-Audit

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 Netwrix Auditor Self-Audit

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) Netwrix Auditor Add-on for CyberArk Privileged Access Security

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 changes 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
Monitor all activities associated with the privileged identities to detect unwanted configuration changes.	Netwrix Auditor Add-on for CyberArk Privileged Access Security

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 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 classification reports for files servers • Activity Related to Sensitive Files and Folders Data classification reports for SharePoint • Activity Related to Sensitive Data Objects Data classification reports for SharePoint Online • Activity Related to Sensitive Data Objects
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 classification reports for file servers • Activity Related to Sensitive Files and Folders Data classification reports for SharePoint • Activity Related to Sensitive Data Objects Data classification reports for SharePoint Online • Activity Related to Sensitive Data Objects Netwrix Auditor Add-on for CyberArk Privileged Access Security Netwrix Auditor Add-on for Nutanix AHV
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 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 • Infrastructure
Review the results of data classification to assess the risks posed by sensitive data not being stored and processed according to the established data security policy.	Data classification reports for file servers • Overexposed Files and Folders • Most Accessible Sensitive Files and Folders • Sensitive Files Count by Source • File and Folder Categories by Object Data classification reports for SharePoint • Most Exposed Sensitive Data Objects • Sensitive Data Objects by Site Collection Data classification reports for SharePoint Online • Most Exposed Sensitive Data Objects • Sensitive Data Objects by Site Collection Netwrix Data Classification provides simple reporting capabilities that help identify sensitive content stored across file servers, SharePoint and SharePoint Online sites, Exchange mailboxes, SQL and Oracle databases and cloud storages (Google Drive, Box and Dropbox).

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.	Netwrix Data Classification 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 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 classification reports for file servers • Overexposed Files and Folders • Most Accessible Sensitive Files and Folders • Sensitive File and Folder Permissions Details Data classification reports for SharePoint • Overexposed Sensitive Data Objects • Most Exposed Sensitive Data Objects • Sensitive Data Object Permissions Data classification reports for SharePoint Online • Overexposed Sensitive Data Objects • Most Exposed Sensitive Data Objects • Sensitive Data Object Permissions 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. Netwrix Data Classification integrates with Microsoft Information Protection (MIP) to enrich its security capabilities with accurate labeling of data.
Monitor for personally identifiable and other sensitive information in the organizational data repositories, which exceeds its legitimate retention time.	Data classification reports for file servers • Sensitive Files Count by Source • File and Folder Categories by Object Data classification reports for SharePoint • Sensitive Data Objects by Site Collection Data classification reports for SharePoint Online • Sensitive Data Objects by Site Collection 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	DSAR searches enable you to locate personal data instances across file servers, SharePoint and SharePoint Online sites, SQL and Oracle databases, Exchange mailboxes and cloud storages (Google Drive, Box and Dropbox).

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.

For more information, visit www.netwrix.com.

Next Steps

Free Trial — Set up Netwrix in your own test environment: netwrix.com/freetrial

In-Browser Demo — Take an interactive product demo in your browser: netwrix.com/browser_demo

Live Demo — Take a product tour with a Netwrix expert: netwrix.com/livedemo

Request Quote — Receive pricing information: netwrix.com/buy

CORPORATE HEADQUARTER:	PHONES:
300 Spectrum Center Drive Suite 200 Irvine, CA 92618	1-949-407-51 Toll-free (USA): 888-638-9749
565 Metro Place S, Suite 400 Dublin, OH 43017	1-201-490-8840
5 New Street Square London EC4A 3TW	+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social