NIST SP 800-53 Controls
and Netwrix Auditor Mapping
About FISMA / NIST

The Federal Information Security Management Act of 2002 (commonly abbreviated to FISMA) is another name for Title III of the U.S. E-Government Act (public law 107-347). FISMA defines a framework for ensuring the effectiveness of security controls over information and information systems that support federal operations. FISMA compliance is mandatory for federal agencies, their contractors and other organizations working on behalf of federal agencies.

To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53.

Organizations have flexibility in applying security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to tailor the relevant security controls so that it more closely aligns with their mission and business requirements and environments of operation.

The Federal Information Security Modernization Act of 2014, which is also known by the abbreviation FISMA, is the name of the U.S. public law 113–283. Enacted in 2014, this new legislation updates and modernizes the original FISMA law to address current security concerns. It puts special emphasis on continuous compliance, monitoring and mitigation, periodic risk assessment and evaluation of controls.
Mapping of the NIST SP 800-53 Controls to Control Processes

The following table lists some of the key NIST SP 800-53 Controls and explains how Netwrix Auditor 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 Auditor can possibly support are included. This mapping should be used as a reference guide to help you implement policies and procedures tailored to your organization's unique situation and needs.

**Family: Access Control**

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Control Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-2 Account Management</td>
<td>Access Control</td>
</tr>
</tbody>
</table>

The organization:

- (a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
- (b) Assigns account managers for information system accounts;
- (c) Establishes conditions for group and role membership;
- (d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- (e) Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
- (f) Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- (g) Monitors the use of information system accounts;
- (h) Notifies account managers:
  1. When accounts are no longer required;
  2. When users are terminated or transferred; and

- **Access Control**
  - Role and Group Assignment
  - Personnel Status Changes
3. When individual information system usage or need-to-know changes;

   (i) Authorizes access to the information system based on:
       1. A valid access authorization;
       2. Intended system usage; and
       3. Other attributes as required by the organization or associated missions/business functions;

   (j) Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

   (k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

**AC-2 Account Management (Control Enhancements)**

<table>
<thead>
<tr>
<th>(1) Automated system account management</th>
<th>Access Control</th>
</tr>
</thead>
</table>
| The organization employs automated mechanisms to support the management of information system accounts. | • Account Management Audit  
• Account Usage Monitoring |

<table>
<thead>
<tr>
<th>(3) Disable inactive accounts</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>The information system automatically disables inactive accounts after [Assignment: organization-defined time period].</td>
<td>• Inactive Accounts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(9) Restrictions on use of shared / group accounts</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].</td>
<td>• Account Usage Monitoring</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(11) Usage conditions</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].</td>
<td>• Account Usage Monitoring</td>
</tr>
</tbody>
</table>
(12) **Account monitoring / Atypical usage**

The organization:

(a) Monitors information system accounts for [Assignment: organization-defined atypical usage]; and

(b) Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].

(13) **Disable accounts for high-risk individuals**

The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk.

**Access Control**

- Account Usage Monitoring

---

**AC-3 Access Enforcement**

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

**Access Control**

- Access Enforcement

---

**AC-6 Least Privilege**

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

**Access Control**

- Role and Group Assignment
- Least Privilege

---

**AC-7 Unsuccessful Logon Attempts**

The information system:

(a) Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

(b) Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

**Identification and Authentication**

- Authenticator Management
### AC-17 Remote Access

The organization:

(a) Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

(b) Authorizes remote access to the information system prior to allowing such connections.

### AC-18 Wireless Access

The organization:

(a) Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

(b) Authorizes wireless access to the information system prior to allowing such connections.

### AC-20 Use of External Information Systems

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

(a) Access the information system from external information systems; and

(b) Process, store, or transmit organization-controlled information using external information system.
## Family: Audit and Accountability

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Control Process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AU-3 Content of Audit Records</strong></td>
<td><strong>Audit and Accountability</strong></td>
</tr>
<tr>
<td>The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.</td>
<td>- Audit Record Generation</td>
</tr>
</tbody>
</table>

**AU-4 Audit Storage Capacity**

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

**Audit and Accountability**

- Audit Record Generation

**AU-5 Response to Audit Processing Failures**

The information system:

(a) Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and

(b) Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

**Audit and Accountability**

- Response to Audit Processing Failures

**AU-6 Audit Review, Analysis, and Reporting**

The organization:

(a) Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and

(b) Reports findings to [Assignment: organization-defined personnel or roles].

**Audit and Accountability**

- Audit Trail Review
AU-7 Audit Reduction and Report Generation

The information system provides an audit reduction and report generation capability that:

(a) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
(b) Does not alter the original content or time ordering of audit records.

Audit and Accountability
- Report Generation and Audit Reduction

AU-8 Time Stamps

The information system:

(a) Uses internal system clocks to generate time stamps for audit records; and
(b) Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

Audit and Accountability
- Audit Record Generation

AU-9 Protection of Audit Information

The information system: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Audit and Accountability
- Protection of Audit Information

AU-11 Audit Record Retention

The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Audit and Accountability
- Audit Record Retention
**AU-12 Audit Generation**

The information system:

(a) Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];

(b) Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and

(c) Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

**AU-14 Session Audit**

The information system provides the capability for authorized users to select a user session to capture/record or view/hear.

**Family: Configuration Management**

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Control Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-2 Baseline Configuration</td>
<td>Configuration Management</td>
</tr>
</tbody>
</table>

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

**CM-3 Configuration Change Control**

The organization:

(a) Determines the types of changes to the information system that are configuration-controlled;

(b) Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;

(c) Documents configuration change decisions associated with the information system;
(d) Implements approved configuration-controlled changes to the information system;
(e) Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];
(f) Audits and reviews activities associated with configuration-controlled changes to the information system; and
(g) Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

CM-5 Access Restrictions for Change

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

CM-6 Configuration Settings

The organization:

(a) Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
(b) Implements the configuration settings;
(c) Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and
(d) Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.
CM-11 User-installed Software

The organization:

(a) Establishes [Assignment: organization-defined policies] governing the installation of software by users;
(b) Enforces software installation policies through [Assignment: organization-defined methods];
(c) Monitors policy compliance at [Assignment: organization-defined frequency].

Family: Identification and Authentication

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Control Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>IA-2 Identification and Authentication (Organizational Users)</td>
<td>Identification and Authentication</td>
</tr>
</tbody>
</table>

The organization:

(a) Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
(b) Reviews and updates the current:
1. Identification and authentication policy [Assignment: organization-defined frequency]; and
2. Identification and authentication procedures [Assignment: organization-defined frequency].
IA-3 Device Identification and Authentication

The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

**Identification and Authentication**
- Device Identification

---

IA-4 Identifier Management

The organization manages information system identifiers by:

(a) Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;
(b) Selecting an identifier that identifies an individual, group, role, or device;
(c) Assigning the identifier to the intended individual, group, role, or device;
(d) Preventing reuse of identifiers for [Assignment: organization-defined time period]; and
(e) Disabling the identifier after [Assignment: organization-defined time period of inactivity].

**Identification and Authentication**
- Identifier Management
- Inactive Accounts

---

IA-5 Authenticator Management

The organization manages information system authenticators by:

(a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
(b) Establishing initial authenticator content for authenticators defined by the organization;
(c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
(d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
(e) Changing default content of authenticators prior to information system installation;
(f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.

**Identification and Authentication**
- Authenticator Management
(g) Changing/refreshing authenticators \[Assignment: organization-defined time period by authenticator type\];

(h) Protecting authenticator content from unauthorized disclosure and modification;

(i) Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

(j) Changing authenticators for group/role accounts when membership to those accounts changes.

Family: Incident Response

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Control Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-4 Incident Handling</td>
<td>Incident Response</td>
</tr>
</tbody>
</table>

The organization:

(a) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

(b) Coordinates incident handling activities with contingency planning activities; and

(c) Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

IR-5 Incident Monitoring

The organization tracks and documents information system security incidents.

Incident Response

- Incident Detection
- Incident Mitigation

- Incident Analysis
IR-9 Information Spillage Response

The organization responds to information spills by:

(a) Identifying the specific information involved in the information system contamination;
(b) Identifying other information systems or system components that may have been subsequently contaminated.

Incident Response
- Incident Detection

Family: Personnel Security

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Control Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS-4 Personnel Termination</td>
<td>Access Control</td>
</tr>
</tbody>
</table>

The organization, upon termination of individual employment:

(a) Disables information system access within [Assignment: organization-defined time period];
(b) Terminates / revokes any authenticators / credentials associated with the individual;
(c) Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
(d) Retrieves all security-related organizational information system-related property;
(e) Retains access to organizational information and information systems formerly controlled by terminated individual; and
(f) Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Access Control
- Personnel Status Changes
**PS-5 Personnel Transfer**

The organization:

(a) Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

(b) Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];

(c) Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

(d) Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

---

**Family: Risk Assessment**

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Control Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-2 Security Categorization</td>
<td></td>
</tr>
</tbody>
</table>

The organization:

(a) Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

(b) Documents the security categorization results (including supporting rationale) in the security plan for the information system;

---

**Access Control**

- Personnel Status Changes

**Risk Assessment**

- Security Categorization
RA-3 Risk Assessment

The organization:

(c) Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

(d) Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; 

(e) Reviews risk assessment results [Assignment: organization-defined frequency];

(f) Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and

(g) Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Family: System and Information Integrity

<table>
<thead>
<tr>
<th>Control Description</th>
<th>Control Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI-4 Information System Monitoring</td>
<td></td>
</tr>
</tbody>
</table>

The organization:

(a) Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and
   2. Unauthorized local, network, and remote connections;

(b) Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
(c) Deploys monitoring devices:
   1. Strategically within the information system to collect organization-determined essential information; and
   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

(d) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

(e) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

(f) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

(g) Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

SI-12 Information Handling and Retention

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

System and Information Integrity
- Information Management and Retention
Control Processes

Control Processes Facilitated by Netwrix Auditor

From the compliance perspective, IT operations can be viewed and managed as a collection of control processes. Such processes allow focusing organizational efforts on a specific area of IT, enforcing certain policies, and establishing particular set of compliance controls. While control processes can be seen as separate entities for the purposes of implementation and management simplicity, in fact all these processes are deeply interconnected and often intrinsic to many regulations and best practices frameworks.

- Identification and Authentication
- 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-reference HR data with Active Directory user accounts in order to:</td>
<td>Active Directory State-in-Time reports</td>
</tr>
<tr>
<td>• Ensure that each user with a business need to access your information systems has a unique account.</td>
<td>• User Accounts</td>
</tr>
<tr>
<td>• Identify personal accounts that cannot be traced to a particular individual.</td>
<td></td>
</tr>
<tr>
<td>Review audit trails to check whether the use of shared accounts complies with your policies.</td>
<td>User Behavior and Blind Spot Analysis reports</td>
</tr>
<tr>
<td>• Logons by Single User from Multiple Endpoints</td>
<td></td>
</tr>
<tr>
<td>• Who = shared account</td>
<td>Interactive Search</td>
</tr>
</tbody>
</table>
|                                                                                          |   • Who = shared account
Correlate employee absence data (typically from HR) with the access audit trail to spot suspicious activity.

Active Directory – Logon Activity reports
- All Logon Activity
- Interactive Search
  - Action = Interactive Logon

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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 DirectoryChanges 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| Review the creation, modification and deletion of users and groups to spot:  
  - Unauthorized changes  
  - Identifiers that do not comply with the your naming standards and policies (e.g., no public, generic or reused identifiers) | Active DirectoryChanges reports
  - User Account Changes
  - Active DirectoryChanges 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.

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

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

Account Management Audit

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| Review user logons and resource access on a regular basis to spot abnormal account use and violations of account use policy. | Activity Summary email notifications  
User Behavior and Blind Spot Analysis reports  
- Temporary User Accounts  
- Recently Enabled Accounts  
- Access to Archive Data  
- Data Access Surges  
- Activity Outside Business Hours  
- Failed Activity Trend |
- Logons by Multiple Users from Single Endpoint
- Logons by Single User from Multiple Endpoints
- Non-owner Mailbox Access

### Review user access to sensitive and regulated data to detect access policy violations

#### Data Discovery and Classification reports
- Activity Related to Sensitive Files and Folders

#### Predefined alerts
- Logon to a Specific Machine alert
- Logon Attempt to a Disabled Account alert
- Multiple Failed Logons alert

#### Interactive Search
- Who = suspicious account

### Enable designated security personnel to respond promptly to potential access abuse.

#### Predefined alerts
- Logon to a Specific Machine alert
- Logon Attempt to a Disabled Account alert
- Multiple Failed Logons alert

#### 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that users are added security groups and access roles in accordance with the least privilege principle and only with proper authorization.</td>
<td>- Active Directory Changes reports</td>
</tr>
<tr>
<td></td>
<td>- Security Group Membership Changes</td>
</tr>
<tr>
<td></td>
<td>- Azure AD reports</td>
</tr>
<tr>
<td></td>
<td>- Group Membership Changes in Azure AD</td>
</tr>
<tr>
<td></td>
<td>- Active Directory State-in-Time reports</td>
</tr>
<tr>
<td></td>
<td>- Group Members</td>
</tr>
<tr>
<td></td>
<td>- Effective Group Membership</td>
</tr>
<tr>
<td></td>
<td>- Users and Computers - Effective Group Membership</td>
</tr>
<tr>
<td></td>
<td>- Windows Server State-in-Time reports</td>
</tr>
<tr>
<td></td>
<td>- Local Users and Groups</td>
</tr>
</tbody>
</table>

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.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory Changes reports</td>
<td>- Administrative Group Membership Changes</td>
</tr>
<tr>
<td>User Behavior and Blind Spot Analysis reports</td>
<td>- Temporary Users in Privileged Groups</td>
</tr>
<tr>
<td>Windows Server Changes reports</td>
<td>- Local Users and Groups Changes</td>
</tr>
<tr>
<td>Active Directory State-in-Time reports</td>
<td>- Administrative Group Members</td>
</tr>
<tr>
<td>Windows Server State-in-Time reports</td>
<td>- Members of Local Administrators Group</td>
</tr>
<tr>
<td>Oracle Database reports</td>
<td>- Privilege Management</td>
</tr>
<tr>
<td>SQL Server reports</td>
<td>- All SQL Server Activity by Object Type (Object Type = Server Role</td>
</tr>
<tr>
<td>Predefined alerts</td>
<td>- Group Membership Changes</td>
</tr>
</tbody>
</table>
## Personnel Status Changes

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| Review audit trails to confirm that the user accounts of temporary and terminated employees are disabled or removed in all information systems and applications according to your policy. | Active Directory Changes reports  
  - User Account Changes  
  - User Account Status Changes |

Review current access permissions of transferred or reassigned employees with particular attention on sensitive and regulated data to ensure they do not exceed their new job requirements.

- Active Directory Changes reports
- User Account Changes
- Active Directory State in Time reports
- Users and Computers - Effective Group Membership
- Data Discovery and Classification reports
- Sensitive File and Folder Permissions Details

## Access Enforcement

Ensure user permissions comply with your access control policies.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| Review access permissions for sensitive information assets involving data owners 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  
  - Object Permissions By Object  
  Data Discovery and Classification reports  
  - Sensitive Files and Folders by Owner  
  - Sensitive File and Folder Permissions Details |

Audit and alert on changes to permissions in order to promptly spot any improper or authorized modifications.

- Predefined alerts  
  - File Share Permissions Changed  
  - Object Permissions Changed in Active Directory  
  - Security Changes on Windows Server  
- Activity Summary email notifications
**Least Privilege**

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regularly review access rights granted to users and roles to ensure users have only the permissions they need to do their jobs.</td>
<td><img src="image" alt="User Behavior and Blind Spot Analysis reports" /></td>
</tr>
</tbody>
</table>
|  | • Excessive Permissions
|  | ![Active Directory Changes reports](image)
|  | • Object Security Changes
|  | • Security Group Changes
|  | ![Active Directory State-in-Time reports](image)
|  | • Account Permissions in Active Directory
|  | • Object Permissions in Active Directory
|  | • Users and Computers - Effective Group Membership
|  | ![Group Policy Changes reports](image)
|  | • User Rights Assignment Policy Changes
|  | • Security Settings Changes
|  | ![Exchange Server reports](image)
|  | • Mailbox Delegation and Permissions Changes
|  | ![File Servers Activity reports](image)
|  | • Permissions Changes
|  | ![File Servers State-in-Time reports](image)
|  | • Account Permissions
|  | • Excessive Access Permissions
|  | • Object Permissions by Object
|  | ![Windows Server Changes reports](image)
|  | • File Share Changes
| 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](image)
|  | • 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](image)
|  | • Who = privileged account
|  | ![Windows Server User Activity reports](image)
|  | • 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| Review detailed remote access logon events along with AD logon activity. | Interactive Search  
  - (Object Type = RADIUS Logon)  
  Netwrix Auditor Add-on for RADIUS Server |
| 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor wireless connections to your networks.</td>
<td>Netwrix Auditor Add-on for Cisco Network Devices</td>
</tr>
</tbody>
</table>
| 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.

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

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

Audit Record Generation

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

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

Audit Record Retention

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>AuditArchive™, a two-tiered storage that provides:</td>
</tr>
<tr>
<td></td>
<td>- SQL Server audit database for operational reporting (data is stored for 180 days by default)</td>
</tr>
<tr>
<td></td>
<td>- Separate file-based archive for long-term storage of audit data (data is stored for 10 years by default)</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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 Cisco Network Devices  
Netwrix Auditor Add-On for Linux Systems  
Netwrix Auditor Add-On for Privileged User Monitoring on Linux and Unix Systems  
Netwrix Auditor Add-On for RADIUS Server  
Data-in API, which enables creation of add-ons for integrating Netwrix Auditor with other systems and applications |

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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.

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

### Session Audit
Capture user activity for audit purposes.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| Record user activity in mission-critical systems. | Windows Server User Activity reports  
- User activity video recording (available even for systems and applications that do not produce logs) |

### Response to Audit Processing Failures
Monitor for audit processing failures and take corrective actions to restore normal audit capturing process.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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  
- 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  
Interactive Search  
- Source = Windows Server  
- Source = Policy  
- Source = Netwrix API |

Identify inappropriate or unapproved changes (e.g., installation of non-approved software).

Alert designated security personnel to critical change events to enable timely response.
### Access Restrictions for Changes
Establish and enforce logical access restrictions associated with changes to the information system.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| Ensure that information system configuration is limited to authorized users by reviewing privileged security groups and monitoring changes to their membership. | ![Icon] Windows Server State-in-Time reports  
- Members of Local Administrator Group  
- Local Users and Groups  

![Icon] Windows Server Changes reports  
- Local Users and Groups Changes  

![Icon] Predefined alerts  
- User Added to Windows Server Administrative Group |

### User-Installed Software
Control and monitor user-installed software.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| 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. | ![Icon] Windows Server State-in-Time reports  
- Windows Server Configuration Details  
- Installed Software |
Incident Response

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

Incident Detection

Detect security incidents in a timely manner.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
</table>
| Regularly review user activity (system logons, resource access, configuration changes)   | Behavior Anomalies Discovery  
  - Top users with behavior anomalies  
  - Detailed trail of user anomalous behavior  
  User Behavior and Blind Spot Analysis reports  
  - Temporary User Accounts  
  - Recently Enabled Accounts  
  - Access to Archive Data  
  - Data Access Surges  
  - Activity Outside Business Hours  
  - Failed Activity Trend  
  - Logons by Multiple Users from Single Endpoint  
  Data Discovery and Classification reports  
  - Activity Related to Sensitive Files and Folders |
| to spot abnormal behavior that could lead to a security breach.                         | 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                 |
| Configure alerts to automatically notify designated security staff of a potential incident, 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 |
**Incident Analysis**
Investigate suspected security and privacy incidents that are detected.

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

**Incident Mitigation**
Respond quickly to a security incident to mitigate its effects.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automate the triggering of incident response procedures upon detection of suspicious activity to ensure timely response and remediation.</td>
<td>Netwrix Auditor Add-On for ServiceNow Incident Management</td>
</tr>
</tbody>
</table>
| Quickly revert unauthorized changes to accounts and configuration.                       | Predefined change reports
- Before and after details
Object Restore for Active Directory tool                                                |
Risk Assessment

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

Risk Assessment

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examine the configuration of your information systems using common security best practices and identify risks that may require mitigation in the following areas:</td>
<td>IT Risk Assessment reports</td>
</tr>
<tr>
<td>• Account management</td>
<td>• IT Risk Assessment: Users and Computers</td>
</tr>
<tr>
<td>• Data governance</td>
<td>• IT Risk Assessment: Data</td>
</tr>
<tr>
<td>• Security permissions</td>
<td>• IT Risk Assessment: Permissions</td>
</tr>
<tr>
<td>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.</td>
<td>Data Discovery and Classification reports</td>
</tr>
<tr>
<td></td>
<td>• Overexposed Files and Folders</td>
</tr>
<tr>
<td></td>
<td>• Most Accessible Sensitive Files and Folders</td>
</tr>
<tr>
<td></td>
<td>• Sensitive Files Count by Source</td>
</tr>
<tr>
<td></td>
<td>• File and Folder Categories by Object</td>
</tr>
</tbody>
</table>

Security Categorization

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform automated discovery of relevant types of sensitive and regulated data in unstructured data repositories (file shares) in order to prioritize data protection measures.</td>
<td>DDC Collector Console that enables you to adjust predefined data categorization rules or define new rules</td>
</tr>
</tbody>
</table>
System and Information Integrity

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

Information System Monitoring

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Behavior Anomalies Discovery</td>
</tr>
<tr>
<td></td>
<td>• List of users with the most behavior anomalies</td>
</tr>
<tr>
<td></td>
<td>• Detailed trail of each user’s anomalous actions</td>
</tr>
<tr>
<td>Configure alerts to automatically notify designated security staff of a potential attack or unauthorized activity.</td>
<td>Predefined alerts</td>
</tr>
<tr>
<td></td>
<td>• User Account Locked Out</td>
</tr>
<tr>
<td></td>
<td>• User Added to AD Administrative Group</td>
</tr>
<tr>
<td></td>
<td>• User Added to Windows Server Administrative Group</td>
</tr>
<tr>
<td></td>
<td>• Unrestricted Access to the File Share</td>
</tr>
<tr>
<td></td>
<td>Custom alerts based on either a triggering event or a defined threshold</td>
</tr>
</tbody>
</table>
**Information Management and Retention**
Manage and retain sensitive personal information in accordance with applicable laws, regulations and operational requirements.

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that personally identifiable and other sensitive information in the organizational data repositories is appropriately secured, including protection against unauthorized disclosure or accidental loss</td>
<td>Data Discovery and Classification reports</td>
</tr>
<tr>
<td>Monitor for personally identifiable and other sensitive information in the organizational data repositories, which exceeds its legitimate retention time.</td>
<td>Data Discovery and Classification reports</td>
</tr>
<tr>
<td>Establish processes and procedures to support customers wishing to exercise their data subject rights:</td>
<td><strong>DDC Collector Console</strong> that enables you to locate personal data instances</td>
</tr>
</tbody>
</table>
|   • Right of access  
   • Right to rectification  
   • Right to erasure (right to be forgotten)  
   • Right to portability | |

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

<table>
<thead>
<tr>
<th>How to Implement Control</th>
<th>Applicable Netwrix Auditor Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor file and document repositories for sensitive information in order to apply appropriate de-identification, redaction or similar measures to mitigate the risk of unauthorized data access.</td>
<td>Data Discovery and Classification reports</td>
</tr>
</tbody>
</table>

• Sensitive Files Count by Source  
• File and Folder Categories by Object
About Netwrix

Netwrix Corporation was first to introduce visibility and governance platform for on-premises, hybrid and cloud IT environments. More than 160,000 IT departments worldwide rely on Netwrix to detect insider threats on premises and in the cloud, pass compliance audits with less expense and increase productivity of IT security and operations teams. Founded in 2006, Netwrix has earned more than 100 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security intelligence to identify security holes, detect anomalies in user behavior and investigate threat patterns in time to prevent real damage.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

For more information, visit www.netwrix.com

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

---

**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

[Contact Netwrix](netwrix.com/social)