VARONIS

National Institute of Standards and Technology SP 800-53

Varonis compliance mapping for NIST 800-53 SP, rev. 5 for federal information systems

Contents

Overview of NIST SP 800-53

In 2002, Congress passed the Federal Information Security Management Act (FISMA), which requires federal organizations (and their contractors) to implement "information security protections commensurate with the risk and magnitude of the harm." FISMA also requires the National Institute of Standards and Technology (NIST) to develop its own standards and guidelines for helping federal organizations improve their security. A list of these publications can be found on the NIST website.

The overall idea is that federal organizations first determine the security category of their information system based on FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems — essentially deciding whether the security objective is confidentiality, integrity, or availability. Then the organization chooses from a set of baseline security controls in NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. In complying with FISMA, NIST gives organizations flexibility in choosing the security controls in 800-53, based on their own security goals.

Varonis is a comprehensive and flexible data security solution that can help you achieve compliance with your ongoing NIST 800-53 projects. The mapping in this document uses rev. 5 of NIST SP 800-53 (published in 2020).

How Varonis maps to NIST SP 800-53

The following table maps relevant 800-53 controls to specific Varonis solutions:

800-53 Control family	Description	How Varonis helps
Access Control (AC)	**Summary of relevant controls:**	**How Varonis helps:**
AC-2 Account Management	Organizations must: • Establish conditions for group and role membership • **Specify authorized users** of the information system, group and role membership, access authorizations (i.e., privileges), and other attributes (as required) for each account	By combining user and group information taken directly from Active Directory or other directory services, lightweight directory access protocol, networking information systems, or other directory services with a complete picture of the file system, Varonis DatAdvantage gives organizations a complete picture of their permissions structures.

		Both logical and physical permissions are displayed and organized, highlighting and optionally aggregating a new technology file system and share-permissions. Flag, tag, and annotate your files and folders to track, analyze, and report on users, groups, and data.
AC-3 Access Enforcement	Organizations **must enforce approved authorizations** for logical access to information and system resources in accordance with applicable access control policies.	Varonis can restrict access to certain information types, can assert and enforce application access, provides attribute-based access control, defines mechanisms for individual user access to personally identifiable information (PII), and can enable organizations to enforce mandatory and discretionary access control to data. Varonis does this by drawing on user and group information from directory services and automatically (or manually if needed) blocking or allowing access based on organizational access policies.
AC-6 Least Privilege	The organization must employ 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.	Varonis helps organizations not only define the policies that govern who can access and grant access to unstructured data, but also enforces the workflow and the desired action to be taken (i.e., allow, deny, allow for a certain time period, etc.).
AC-21 Information Sharing	Organizations must: • Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and **use restrictions where user discretion is required** • Employ organization-defined automated mechanisms or manual processes to assist users in **making information-sharing and collaboration decisions**	Varonis frees up your IT team by empowering business users to manage access to their team's data and applications. Users request access via an intuitive web form, and owners approve or deny by replying to an email. Varonis also provides recommendations driven by machine learning for who should and should not have access to data. The platform then handles all changes seamlessly behind the scenes once all approvals are met. Varonis also automatically prevents new access requests from being approved that would violate your business rules. We'll detect and notify you of any existing rule violations and autocorrect them.

AC-23 Data Mining Protection	Organizations must employ **data mining prevention and detection** techniques for data storage objects to detect and protect against unauthorized data mining.	Varonis alerts to meaningful deviations from normal data access activity and flags it for review or automatically enforces policy. If a user who normally accesses 10-20 folders a day suddenly accesses 1,000 folders in a day or downloads the contents of those folders onto an external drive, Varonis can revoke data access for that user quickly or send an alert to your security team.
AC-24 Access Control Decisions	Organizations must establish procedures or implement mechanisms to **ensure access control decisions are applied to each access request** prior to access enforcement.	Varonis provides an automated workflow for data access requests that puts data owners in charge of data access, enabling you to actively maintain least-privilege access. Additionally, the platform schedules automated entitlement reviews to ensure access permissions are current.
Awareness and Training (AT)	**Summary of relevant controls:**	**How Varonis helps:**
AT-2 Literacy Training and Awareness	The organization must: • Provide **security and privacy literacy training** to system users • Incorporate lessons learned from internal or external **security incidents or breaches** into literacy training and awareness techniques	Varonis's complimentary Cyber Resiliency Assessment and our complimentary incident response team can assist in training your team to respond to the latest evolutions of the threat landscape. In the event of a data breach, our incident response team can help you respond to the attack and will provide recommendations to improve detection and response at the conclusion of your working session. The cyber resiliency team can measure your data exposure and stress-test your security stack against the latest adversary tactics and tradecraft, strengthening your security posture and helping to train your security team.
Audit and Accountability (AU)	**Summary of relevant controls:**	**How Varonis helps:**
AU-2 Event Logging	Organizations must: • Determine that the information system can audit information systems • **Coordinate the security audit with other organizational entities** requiring audit information to enhance mutual support and to help guide the selection of auditable events	Varonis helps organizations examine and audit the use of ordinary and privileged access accounts to detect and prevent abuse. With a continual audit record of all files, email, SharePoint, and Directory Services activity, DatAdvantage provides visibility into users' actions. The log can be viewed interactively or via email reports. DatAdvantage can also identify when users have administrative rights they do not use or need and provides a way to remove excess privileges without impacting the business safely.
AU-3 Content of Audit	Organizations must ensure that audit records contain information that	

Reports	establishes the following: • **What** type of event occurred • **When** the event occurred • **Where** the event occurred • **Source** of the event • **Outcome** of the event • **Identity** of any individuals, subjects, or objects/entities associated with the event	
AU-6 Audit Review, Analysis, and Reporting	Organizations must: • **Review and analyze** information system audit records • Report findings to appropriate personnel.	
AU-10 Non-repudiation	Ensure that the information system protects against an individual (or process) **falsely denying having performed file copies, moves, or deletes**.	

AU-13 Monitoring for Information Disclosure	Organizations must:
	• **Monitor open-source information** and/or information sites for evidence of unauthorized disclosure of organizational information
	• If an information disclosure is discovered:
	  ○ **Notify** designated personnel
	  ○ **Take action** in accordance with organizational plan	

Assessment, Authorization, and Monitoring (CA)	**Summary of relevant controls:**	**How Varonis helps:**
CA-6 Authorization	Organizations must employ a joint authorization process that includes **multiple authorizing officials** from the same organization.	Varonis provides data access governance by automating access control requests. We let business users manage access to their team's data and applications, and users can request access via an intuitive web form. Varonis handles all changes behind the scenes once all approvals are met with any elevated privileges required.

CA-7 Continuous Monitoring	Organizations must ensure **risk monitoring** is an integral part of the continuous monitoring strategy.	Our perimeter edge detection continuously monitors your perimeter telemetry and correlates it with data access to stop infiltration and data exfiltration. We also provide continuous monitoring of your data inside your network and correlate data activity with sensitivity and permissions to ascertain risk and alert on suspicious behavior.
Configuration Management (CM)	**Summary of relevant controls:**	**How Varonis helps:**
CM-4 Impact Analysis	Organizations must **analyze changes to the information system** to determine potential security impacts prior to change implementation.	Varonis provides actionable intelligence on where excess file permissions and group memberships can be safely removed without affecting normal business processes. Varonis also provides the ability to model and simulate permissions changes in its sandbox so they can be tested without affecting the production environment.
Contingency Planning (CP)	**Summary of relevant controls:**	**How Varonis helps:**
CP-4 Contingency Plan Testing	Organizations must employ specified **testing mechanisms** to systems or system components to disrupt and adversely affect the system or system components.	Our complimentary Cyber Resiliency Assessment allows you to test your security stack against a series of adversarial tactics, evaluating if your organization can investigate an incident and recover quickly. We will test your organization on attack vectors such as malicious file downloads, DNS tunneling, password spraying, Kerberoasting, ransomware, and more.
Incident Response (IR)	**Summary of relevant controls:**	**How Varonis helps:**
IR-2 Incident Response Training	Organizations must provide incident response training on how to **identify and respond to a breach.**	The Varonis Incident Response Team is a group of in-house cybersecurity analysts that can assist in responding to incidents reported by Varonis alerts, without charge. The team can assist with forensic analysis of data breaches, containment, eradication, and recovery, and most importantly, can help train your security team by making recommendations to improve future detection and response.
IR-3 Incident Response Testing	Organizations must require qualitative and quantitative data from testing to determine the effectiveness of incident response. They must work to **continuously improve incident response** processes by capturing incident response metrics that	

	are accurate, consistent, and in a reproducible format.	Additionally, our complimentary Cyber Resiliency Assessment can help you comply with the incident response requirements of NIST SP 800-53 by stress-testing your security stack against the latest adversary tactics and tradecraft.
IR-4 Incident Handling	Organizations must: • Establish and maintain an integrated **incident response team** that can be deployed to any location identified by the organization • **Analyze malicious code** and/or other residual artifacts remaining in the system after the incident • Analyze anomalous or suspected **adversarial behavior**	
IR-5 Incident Monitoring	Organizations must **track and document incidents.**	
IR-6 Incident Reporting	Organizations must: • Require personnel to report suspected incidents to the organizational **incident response team** within the organization-defined timeframe • Report incident information to **organization authorities**	
IR-7 Incident Response Assistance	Organizations must have an **incident response support resource**, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.	
IR-9 Information Spillage Response	Organizations must respond to information spills by: • **Assigning** designated personnel with responsibility for responding to information spills • **Identifying** the specific information involved in the system contamination • **Alerting** relevant personnel of the information spill using a method of communication not associated with the spill • **Isolating** the contaminated system or system component • **Eradicating** the information from the contaminated system or component	

	• **Identifying** other systems or system components that may have been subsequently contaminated • **Performing** any additional actions specified by the organization	
Program Management (PM)	**Summary of relevant controls:**	**How Varonis helps:**
PM-5 System Inventory	Organizations must require development and periodic update of an inventory of all **programs and systems that process PII.**	Data inventory and auditing is Varonis' bread and butter. Classify sensitive data and visualize risk to your sensitive data by correlating data sensitivity and permissions. With Varonis, you can easily provide an audit trail of where all your PII lives.
P-6 Measures of Performance	Organizations must develop, monitor, and report on the results of **information security and privacy measures** of performance.	Varonis provides out-of-the-box and custom reports that detail key risk indicators, effective permissions, user and group changes, data usage trends, security incidents, and more. Run reports on-demand or email them on a schedule.
PM-10 Authorization Process	Organizations must: • Designate individuals to fulfill specific **roles and responsibilities** within the organizational risk management process • Integrate the authorization processes into an organization-wide **risk management program**	Varonis helps organizations not only define the policies that govern who can access and grant access to unstructured data, but also enforces the workflow and the desired action to be taken (i.e., allow, deny, allow for a certain time period, etc.).
PM-12 Insider Threat Program	Organizations must implement an insider threat program that includes a cross-discipline **insider threat incident handling team**.	Varonis enables organizations to identify and mitigate the risks of insider threats through its ability to continuously remediate excessive permissions to sensitive data. Varonis monitors and normalizes user activity to establish baseline behavioral profiles and uses behavioral-based threat models that alert on unusual, risky, or malicious insider activity.
PM-16 Threat Awareness Program	Organizations must employ an **automated means** of sharing threat intelligence information.	Our data-centric user behavior analytics detects anomalous data access and alerts on meaningful deviations in behavior, and reports can be sent to anyone within the agency.

PM-17 Protecting Controlled Unclassified Information on External Systems	Organizations must: • Establish policies and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored, or transmitted on **external systems**, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards • **Review and update the policy** and procedures regularly, within intervals as defined by the organization	Varonis caters to federal agencies with policies to classify controlled unclassified information (CUI). Once CUI is identified, we can auto-enforce your data governance policies by quarantining sensitive files with open access, archiving sensitive data, or migrating data cross-platform or cross-domain.
PM-22 Personally Identifiable Information Quality Management	Organizations must develop and document organization-wide policies and procedures for: • **Reviewing** for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle • **Correcting** or deleting inaccurate or outdated PII • **Disseminating** notice of corrected or deleted PII to individuals or other appropriate entities • **Allowing appeals** of adverse decisions on correction or deletion requests	Varonis enables rapid response to Data Subject Access Requests (DSARs) by surfacing personal information across cloud and on-prem files with a fast and powerful search. From there, you can export a user's data as a CSV file to send them a copy, correct the information at the data source, or delete data. Additionally, you can set policies to automatically delete sensitive data, Secret and Top-secret data, and PII after a specified retention period.
PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research	Organizations must: • Develop, document, and implement **policies and procedures** that address the use of personally identifiable information for internal testing, training, and research • **Limit or minimize** the amount of PII used for internal testing, training, and research purposes • **Authorize the use of PII** when such information is required for internal testing, training, and research • **Review and update policies and procedures** within the timeframe designated by the organization	Varonis creates a visual map of your data estate and sensitive data — both on-premises and in the cloud — and identifies who has access to it and whether they should have access. When users have access to data they shouldn't, Varonis quietly revokes access on the backend without disrupting productivity.

PM-27 Privacy Reporting	Organizations must: • Develop privacy reports and **disseminate them** to organizational oversight bodies and designated internal privacy personnel to demonstrate accountability with statutory, regulatory, and policy privacy mandates • **Review and update privacy reports** within the timeframe designated by the organization	Varonis helps organizations examine and audit the use of ordinary and privileged access accounts to detect and prevent abuse. With a continual audit record of all files, email, SharePoint, and Directory Services activity, Varonis correlates data sensitive with permissions to give you a full view of your data privacy posture. The log can be viewed interactively or via email reports.
PM-31 Continuous Monitoring Strategy	Organizations must develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs, including: • **Ongoing monitoring** of organizationally defined metrics in accordance with the continuous monitoring strategy • **Correlating and analyzing of information** generated by control assessments and monitoring • **Developing actions** to address results of the analysis of control assessment and monitoring information • **Reporting the security and privacy status** of organizational systems	Varonis continuously maps permissions and monitors data activity to identify excessive access, policy violations, and suspicious behavior — providing a full audit trail of activity for investigation and analysis. We use user entity and behavior analytics (UEBA) to identify risky behavior and provide recommendations on where excessive access should be removed. With Varonis, you can configure automated responses to stop threats in their tracks as soon as they are detected. Through detailed dashboards, reports, and playbooks, admins can easily identify and report on where sensitive data is at risk and create response plans to proactively reduce risk to sensitive data and respond to potential threats.
PII Processing and Transparency (PT)	**Summary of relevant controls:**	**How Varonis helps:**
PT-2 Authority to Process PII	Organizations must: • **Determine and document** the authority that permits the processing of personally identifiable information, and restrict the processing of this information to only authorized purposes • **Attach data tags** containing defined permissible processing to defined elements of PII	Varonis enables organizations to label PII and restrict access to it so that only authorized personnel can view and process the data. Admins can use Varonis to create custom automation rules that fit your PII processing policies that automatically moves PII from out-of-policy locations as soon as it detects a violation.
PT-3 Personally Identifiable Information Processing Purposes	Organizations must require **data tags to support tracking of processing purposes** by conveying the purposes along with the relevant elements of PII throughout the system.	

PT-7 Specific Categories of PII	Organizations must: • **Apply processing conditions** for specific categories of personally identifiable information • **Establish specific requirements** (as defined by federal policy) for processing social security numbers • **Take steps to eliminate unnecessary uses** of social security numbers and other sensitive information and observe any specific requirements that apply	Varonis goes beyond regular expressions to accurately classify specific categories of PII such as social security numbers, driver's license numbers, addresses, phone numbers, etc. across petabytes of unstructured data with only a few false positives. Automatically apply persistent sensitivity labels to encrypt, obfuscate, or enforce data risk management on specific categories of PII and other sensitive data.
Risk Assessment (RA)	**Summary of relevant controls:**	**How Varonis helps:**
RA-3 Risk Assessment	The organization must: • **Use all-source intelligence** to assist in the analysis of risk • Determine the **current cyber threat environment** on an ongoing basis • Employ **advanced automation** and analytics capabilities to predict and identify risks	Varonis provides a free Data Risk Assessment to help you determine the exposure of your sensitive data, during which you will be able to test our product in your own environment.
RA-5 Vulnerability Monitoring and Scanning	The organization: • **Scans for vulnerabilities** in the information system and hosted applications • **Analyzes vulnerability scan reports** and results from security control assessments	Varonis gives organizations visibility into data content, providing intelligence on where sensitive data resides across its file systems. By integrating file classification information and presenting it in the Varonis DatAdvantage interface, Varonis enables actionable intelligence for data governance — including prioritized reports showing where sensitive content is highly concentrated and over-exposed, and an audit trail of all Active Directory activity. Varonis gives organizations context around the sensitive content that we find.

System and Communication Protection	Summary of relevant controls:	How Varonis helps:
SC-4 Information in Shared System Resources	Organizations must **prevent unauthorized and unintended information transfer** via shared system resources.	With Varonis, you can automatically detect internal and external threats with behavioral-based alerting. Varonis proactively alerts you to threats to your data, like abnormal access to sensitive data, privilege escalation attempts, or unusual file upload/download activity. Varonis stops malicious actors in real time with automated responses, blocking bad actors from exfiltrating, deleting, or modifying your data.
SC-28 Protection of Information at Rest	Organizations must protect the **confidentiality and integrity of sensitive information** as defined by the organization when the data is at rest.	With Varonis, you can reduce your attack surface without human intervention. Varonis shows you where sensitive and regulated data is concentrated and automatically remediates overexposure — getting you to least privilege without human intervention.
System Information Integrity Monitoring (SI)	**Summary of relevant controls:**	**How Varonis helps:**
SI-4 System Monitoring	Organizations must: • Monitor the system to **detect attacks and indicators of compromise** • Identify **unauthorized use** of the system • Invoke internal monitoring capabilities or deploy monitoring devices to gain **visibility into sensitive and critical information** • **Analyze** detected events and anomalies • **Adjust** the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the nation	With our data-centric user behavior analytics and the network edge telemetry we consume, you receive a full picture of how data is moving around your network and who is attempting to access it. We detect suspicious VPN, DNS, and web activity and correlate that information with user behavior data to deliver meaningful alerts regarding threats to your data. Varonis stops data exfiltration, malware infiltration, and more.

SI-12 Information Management and Retention	The organization must use techniques to **dispose of, destroy, or erase information** when it is no longer needed	Varonis can archive or delete stale and risky data, aiding in enforcing privacy policies that require stale PII to be deleted.
SI-18 Personally Identifiable Information Quality Operations	The organization must: • Employ data tags to **automate the correction or deletion of PII** across the information lifecycle • **Correct or delete PII** upon request by individuals or their designated representatives	Label PII with tags such as CCPA or HIPAA to ensure PII and other types of sensitive data are deleted on schedule when no longer needed. Varonis can help you comply with data subject access requests, and we instantly surface and collect the information you need for DSARs, right to be forgotten, or e-discovery. Our DSAR form uses sophisticated logic on the backend to ensure you get accurate results and avoid false positives. We surface PII using highly accurate rulesets, using more than just simple text matching.

Schedule a free Data Risk Assessment.

Varonis can help manage your security risk and comply with NIST 800-53 by implementing least-privilege access to your data, monitoring your data for potential threats, and automatically generating comprehensive audit records. To learn more about how Varonis can help you comply with NIST 800-53, sign up for a free Data Risk Assessment, during which you can try out our products with no commitment and with full support from our team.

Our complimentary assessment run by expert forensics and incident response analysts will help you find and classify data across on-premises and cloud data stores, measure and report on data exposure, and alert on suspicious access to your data.

Contact us

About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on-premises and in the cloud: sensitive files and emails; confidential customer, patient, and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analyzing data, account activity, and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and has thousands of customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.