COMPLIANCE BRIEF: FISMA

OVERVIEW

The Federal Information Security Management Act (FISMA) contains provisions for how government agencies must audit and report on their information systems, including servers which contain unstructured and semi-structured data. In 2010, the Office of Management and Budget (OMB) released a memo (M-10-15) detailing the reporting requirements for government agencies with regard to FISMA. This memo lays out specific instructions for reporting, including instructions for an agency's "privacy management systems." Varonis solutions directly address many of these requirements. The OMB requires that agencies "need to be able to continuously monitor security-related information from across the enterprise in a management and actionable way." In order to accomplish this, the OMB states that agencies need to automate security-related information, develop automated risk models, and apply those models to vulnerabilities and threats identified by security management tools. Varonis can greatly assist an organization is meeting these goals.

Automated Risk Model

FISMA requires that government agencies develop an automated risk model that provides "greater visibility and focus on their most significant vulnerabilities at any time." These requirements apply to all information systems within an agency, including file servers containing unstructured and semi-structured data. Varonis can help an agency meet specific FISMA reporting requirements in the following ways:

Definition	Requirements	How Varonis Addresses It
Adequate Security	Security is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. Systems must provide appropriate confidentiality, integrity, and availability through operational and technical controls.	By providing complete visibility into permissions and file events, as well as where sensitive content resides, Varonis can identify where sensitive content is over-exposed, where unauthorized access is taking place, and how to remediate excess access.

General Support System	An interconnected set of information resources under the same direct management control which shares common functionality.	Varonis provides administrators the ability manage unstructured data on Windows, UNIX, NetApp, and EMC Celerra file servers as well as SharePoint repositories all within a single management interface.
Information Security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality, and availability.	Varonis provides actionable intelligence on exactly who can access and who is accessing content so that information can be properly protected.
Significant Deficiency	A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems. As required in FISMA, agencies are to report any significant deficiency in policy, procedure, or practice.	By identifying sensitive content as well as where content is over-exposed, Varonis provides visibility into where unstructured and semi-structures information systems may contain significant deficiencies so that they can be properly reported and corrected.
System Assessment	A comprehensive assessment of the management and operation and technical security controls in an information system to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.	Varonis DatAdvantage and DataPrivilege provide complete auditing of file system events, process reviews and workflow controls, which help agencies implement information security policies and demonstrate that policies are operating as intended.

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.

FREE 30-DAY ASSESSMENT

WITHIN HOURS OF INSTALLATION
You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

WITHIN A DAY OF INSTALLATIONS
Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

WITHIN 3 WEEKS OF INSTALLATION
Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.

[START YOUR FREE TRIAL]

WORLDWIDE HEADQUARTERS
1250 Broadway, 31st Floor, New York, NY 10001 T 877-292-8767 **E** sales@varonis.com **W** www.varonis.com

UNITED KINGDOM AND IRELAND
Varonis UK Ltd., Warnford Court, 29 Throgmorton Street, London, UK EC2N 2AT T +44 0207 947 4160 **E** sales-uk@varonis.com **W** www.varonis.com

WESTERN EUROPE
Varonis France SAS, 13-15 rue Jean Jaures (1er Etage) 92800 Puteaux T +33 184 88 56 00 **E** sales-france@varonis.com **W** sites.varonis.com/fr

GERMANY, AUSTRIA AND SWITZERLAND
Varonis Deutschland GmbH, Welserstrasse 88, 90489 Nurnberg T +49(0) 911 8937 1111 **E** sales-germany@varonis.com **W** sites.varonis.com/de

Compliance Brief: FISMA