COMPLIANCE BRIEF: ISO 27001 STANDARDS

OVERVIEW

The ISO 27000 set of standards comprises several well-known and published standards as well as some earmarked numbers all of which collectively aim to address information security. Specifically ISO 27001 is the specification for an Information Security Management System (ISMS) and replaces the long standing BS7799-2. ISO 27002 is the replacement to the well known ISO 17799 and delineates controls which may be applied to meet the goals of ISO 27001. This paper addresses how Varonis software can help organizations meet the directives of the ISO standards.

Background

The International Standards Organization (ISO) is the largest developer of standards in the world. Its membership includes the national standards bodies of countries around the world including the Americas, Europe and Asia. The standards are developed by committees of technical experts and undergo much scrutiny and revision prior to publication. ISO 27001 is the result of such an effort and represents updating and augmentation of the BS 7799-2 standard. ISO 27001 aims to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System" (ISMS). ISO 27002 also outlines controls for information security, but discusses in greater detail the components that make up an ISMS. While once separate, ISO 27001 and 27002 are now seen as complementary. Entities may use the combined guidance to construct an ISMS is commensurate with the organization's size and risk tolerance. Ultimately, companies that implement the ISO 27000 guidance certify their ISMS to ISO 27001.

Who is Covered By ISO 27001

All organizations, businesses, government groups, academic institutions and non-profits interested in implementing a framework for the long term protection of their information assets may apply the guidelines and certification requirements of the ISO 2700 standards.

Specifically entities may use ISO 27001 to:

- Formulate security requirements and objectives
- Ensure that security risks are cost effectively managed
- Comply with laws and regulations
- Ensure that the specific security objectives of an organization are met
- Implement new information security management processes
- Determine the degree of compliance with the policies, directives and standards adopted by an organization
- Provide relevant information about information security policies, directives, standards and procedures to
- Customers and business partners as well as other organizations with whom they interact
- Implement business-enabling information security

How Varonis Applies to ISO 27001 Initiatives

Varonis provides a comprehensive system for meeting the information protection controls as they apply to unstructured and semi-structured data, that is, the contents of file servers and SharePoint servers. In particular, Varonis solutions ensure that access and use of sensitive and important personal data residing on these servers are automatically ratcheted down to need-to-know, and that use of sensitive data is continuously monitored so that organizations have an accurate audit of data use and user access behavior at all times.

Specifically, Varonis has created a fully integrated suite of five products which furnish a complete framework for managing, securing and reporting on all aspects of unstructured and semi structured data use.
They are: DatAdvantage for Windows, UNIX, and SharePoint, Data Classification Framework (DCF) and DataPrivilege.

VARAONIS DATADVANTAGE FOR WINDOWS, UNIX, AND SHAREPOINT

The Varonis DatAdvantage software solutions for Windows, UNIX, and SharePoint aggregate user, data and access event information from directories and file servers. Sophisticated analytics applied to the collected information show detailed data use and determine rightful access based on business need.

Specifically, and in a non-intrusive way, Varonis:

- Protects data by recommending removal of overly permissive access controls
- Restricts unstructured data access to those with a business need for that data
- Tracks and monitors every user's every file touch
- Re-computes access controls to account for changes in roles and file server contents
- Identifies likely business data owners

VARAONIS DATA CLASSIFICATION FRAMEWORK

The Varonis Data Classification Framework installs as a layer on top of DatAdvantage, and overlays data classification information for sensitive files contained within the monitored file and SharePoint servers.
The DCF will:

- Identify sensitive files based on known patterns, strings, or dictionary contents
- Incrementally scan only new and modified files after initial baseline
- Target and prioritize scans based on permissions exposure, activity, density and other metrics
- Identify areas of high risk: those folders and SharePoint sites that are overexposed with respect to permissions AND contain considerable sensitive data

VARAONIS DATAPRIVILEGE

DataPrivilege makes it possible to transition the responsibility of data entitlement management from IT to business owners without any infrastructure changes or business disruption. DataPrivilege brings together data owners and data users in a forum for communicating, authorizing and activating entitlements.

Varonis DataPrivilege allows you to implement a cohesive data entitlement environment, thereby raising accountability and reducing risk. Upon implementation, DataPrivilege provides:

- Automated Entitlement Reviews
- Automated Authorization Workflows
- Data protection by reducing errors in entitlement management
- Business need-to-know access control by enabling data owners to make informed decisions
- Access approval rationale history for refinement and improvement
- Policy and workflow enforcement for consistency and greater security

Mapping Requirements to Varonis

The following is a table containing sections of the ISO 27001 controls framework. Where applicable an explanation is provided as to how Varonis DatAdvantage and DataPrivilege software can help organizations meet the ISO 27001 directive with regard to unstructured data residing on UNIX and Windows file servers or network attached storage devices. It should be noted that the information in the table is a small subset of the functionality afforded organizations by Varonis software for comprehensive unstructured and semi structured data governance.

Clause Requirement	Sec	Control Objective/Control	Description
Asset Management	7.1	Responsibility for Assets	
	7.1.1	Inventory of assets	Varonis shows all directory and file share contents mapping users to data and vice versa
	7.1.2	Ownership of Assets	Varonis shows which persons are the likely business owners of a given data set or folder
	7.1.3	Acceptable use of assets	Varonis audits all the file share data by username, filename and action taken on the data, and identifies abnormally excessive access activity
	7.2	Information classification	
	7.2.1	Classification Guidelines	Varonis provides the ability to classify data based on business guidelines and ensures that proper controls are in place based on that classification
Communications and Operations Management	10.1	Operational Procedures and Responsibilities	
	10.1.2	Change Management	Varonis tracks all changes to file systems including modifications of access controls and security settings
	10.1.3	Segregation of Duties	Varonis helps enforce least privilege access by furnishing the list of persons who should have their data access permissions revoked and providing the means to enforce that access
	10.2	Third Party Service Delivery Management	

Clause Requirement	Sec	Control Objective/Control	Description
	10.2.2	Monitoring and review of third party serves	Varonis can help monitor and audit third-party system activity on unstructured and semi structured data
	10.3	System Planning and Acceptance	
	10.3.1	Capacity management	Varonis shows all inactive and orphaned data and its size so that file shares and network attached storage space can be used efficiently, sending unused assets to less expensive archive storage
	10.10	Monitoring	
	10.10 1	Audit logging	Varonis provides a detailed and searchable audit log of all unstructured and semi structured data use on file systems and network attached storage
	10.10.2	Monitoring system use	Varonis provides detailed activity analysis of unstructured file access on monitored file systems
Access Control	11.1	Business Requirement for Access Control	
	11.1.1	Access control Policy	Varonis allows the enforcement of an access control policy by ensuring that business owners accept or reject recommendations for permissions revocations
	11.2.4	Review of user access rights	Varonis gives the means to conduct a full in depth data entitlement review by which all user privileges to data is reported. It also provides reports of historical access rights to data sets showing any trends toward overly permissive access
	11.6	Application access control	
	11.6.1	Information access restriction	Varonis can provide excess access information to help an organization adhere to proper access controls
Information Security Incident Management	13.1	Reporting information Security Events and Weaknesses	

Clause Requirement	Sec	Control Objective/Control	Description
	13.1.1	Reporting Information security events	Varonis will report on anomalous file share data access activity for individuals who exceed their normal or average level of access. Overly rigorous access will generate an alert and a report of the type of activity which will automatically be forwarded to stakeholders like data business owners or IT operations personnel
	13.1.2	Reporting security weaknesses	Varonis will report on data which has weakened security through global groups (everyone, authenticated users, etc.) or otherwise excessive access, as well as users and groups which have excess access
	13.2	Management of Information Security Incidents and Improvements	
	13.2.3	Collection of evidence	The Varonis log of all file touches can be referenced in support of forensic analysis of data use ad activity
Compliance	15.1	Compliance with Legal Requirements	
	15.1.2	Intellectual Property Rights (IPR)	Varonis helps organizations comply with initiatives to ensure least privilege access to regulated data. The system analyzes data access patterns and continually recommends that those without business need to data have their privileges revoked
	15.1.3	Protection of organizational records	Varonis helps protect sensitive and important information by ensuring that access is continually monitored and that access controls are warranted
	15.1.4	Data Protection and privacy of personal information	With Varonis compliance officers and auditors can receive regular reports of data use and access activity of privileged and protected information to ensure compliant use and safekeeping

Clause Requirement	Sec	Control Objective/Control	Description
	15.1.5	Prevention of misuse of information processing facilities	Varonis significantly reduces the risk of data loss and misuse by continually maintaining access controls that are restrictive to business need to know
	15.2	Compliance with Security Policies and Standards and Technical compliance	
	15.2.1	Compliance with security policy	Varonis can ensure that only business owners manage data authorizations, and further allow auditors and compliance personnel to monitor the process
	15.2.2	Technical compliance checking	Varonis tools can enable the regular audit of compliance standards on monitored systems
	15.3	Information System Audit Considerations	
	15.3.1	Information System Audit controls	Varonis provides reporting detail on all aspects of data use and file share use including those actions taken by domain administrators

Varonis and ISO 27002

While ISO 27001 provides standards for data governance against which an organization can be certified and audited,ISO 27002 provides best practices for an organization to follow. The following table maps out specific ways that Varonis products can help an organization enact ISO 27002 controls.

Clause Requirement	Sec	Control Objective/Control	Description
Corporate Security Management Objectives	6.1	Establish an internal security organization	
	6.1.18	Carry out a risk assessment whenever there is a business need to allow external parties to access your information	Varonis products can help quickly identify operational risk with regard to file system and SharePoint data
	6.1.19	Make sure that your risk assessments examine security implications whenever there is a need to allow external parties to access your information	Varonis can help show exactly what access will be granted to users and groups
Organizational Asset Management Objectives	7.1	Establish responsibility for your organization's assets	Varonis provides reporting detail on all aspects of data use and file share use including those actions taken by domain administrators
	7.1.1	Protect your organization's assets	Varonis products provide visibility into who can access data, enabling the protection of data and proper access control
	7.1.2	Use controls to protect your assets.	
	7.1.3	Account for your organization's assets	
	7.1.4	Nominate owners for all organizational assets	Varonis products provide the ability to intelligently identify and assign owners to data based on detailed activity analysis
	7.1.5	Make nominated owners responsible for protecting your organization's assets	
	7.1.6	Assign responsibility for the maintenance of asset controls	

Clause Requirement	Sec	Control Objective/Control	Description
	7.1.7	Make your asset owners responsible for protecting your organization's assets even though owners may have delegated the responsibility for implementing controls	
	7.2	Use an information classification system	
	7.2.1	Provide an appropriate level of protection for your organization's information	The Varonis Data Classification Framework extends the IDU Framework by incorporating content classification information produced by looking within files to find key words, phrases and patterns (i.e., regular expressions) that are of interest to the organization
	7.2.2	Establish an informational classification system	
	7.2.3	Use your classification system to define security levels	
	7.2.4	Specify how much protection is expected at each level	
	7.2.5	Assign a security priority to each information security level	
	7.2.6	Use your organization's information classification system to specify how information should be protected at each level	
	7.2.7	Use your organization's information classification system to specify how information should be handled at each level	
Communications and Operations Management Objectives	10.4	Protect against malicious and mobile code	
	10.4.4	Detect the introduction of malicious code and unauthorized mobile code	Activity analysis can indicate possible malicious and unauthorized code
	10.9	Protect electronic commerce services	
	10.9.6	Protect the availability of information that is published using publicity accessible systems	Permissions visibility can help protect the availability of information

Clause Requirement	Sec	Control Objective/Control	Description
	10.10	Monitor information processing systems facilities	
	10.10.1	Monitor information processing systems in order to detect unauthorized activities	Varonis records every file system event, which enables the software to provide detailed activity analysis. This can help detect system problems as well as be used to verify controls
	10.10.2	Record your information security events	
	10.10.3	Use operator logs to detect information system problems	
	10.10.6	Use system monitoring to check how effective controls are	
	10.10.7	Use system monitoring to verify that information processing activities comply you're your organization's access policy	
Information Access Control Management Objectives	11.1	Control access to information	
	11.1.1	Control access to your organization's information	Varonis products can help ensure that access controls are in place and effective
	11.1.2	Make sure that your information access controls meet your organization's business requirements	
	11.1.3	Make sure that your information access controls meet your organization's security requirements	
	11.2	Manage user access rights	
	11.2.1	Control authorized access to information systems	Varonis can help identify excess permissions to better maintain proper authorization for access to file systems
	11.2.2	Prevent unauthorized access to information systems	

Clause Requirement	Sec	Control Objective/Control	Description
	11.2.4	Ensure that your access allocation procedure controls allstages of the users' access life cycle from initial user registration to final deregistration	
	11.2.5	Ensure that your access allocation procedure pays special attention to the allocation of privileged access rights which allow users to override normal system controls	
	11.3	Encourage good access practices	
	11.3.1	Prevent unauthorized user access to your information and information processing facilities	Varonis can help identify excess permissions so you can better maintain proper authorization for access to file systems
	11.3.2	Prevent information and information processing facilities from being exposed to possible loss or damage	
	11.3.3	Prevent the theft of information and information facilities	Activity analysis can help identify anomalous user behavior to help prevent data theft
	11.3.4	Ask authorized users to help you control access to your information systems and information processing facilities	DataPrivilege automatically involves data owners and business stakeholders in access control processes, including authorization and ongoing review of access
	11.3.5	Make authorized users responsible for helping you to control access to information and information processing facilities	
	11.3.6	Make users aware of what they must do to control access	
Systems Development and Maintenance Objectives	12.4	Protect and control your organization's system files	
	12.4.1	Ensure the security of your organization's system files	Permissions visibility, detailed audit information, and data classification helps protect and control system files
	12.4.2	Control access to your organization's system files	

Clause Requirement	Sec	Control Objective/Control	Description
	12.4.5	Make sure that sensitive or critical data is not exposed in test environments	
Information Security Incident Management Objectives	13.1	Report information security events and weaknesses	
	13.1.1	Make sure that information system security incidents are promptly reported	Varonis can provide automatic, data-driven reports to data owners and IT
Compliance Management Objectives	15.1	Comply with legal requirements	
	15.1.1	Make sure that your information systems comply with all relevant statutory security requirements	
	15.1.2	Make sure that your information systems comply with all relevant regulatory security requirements	
	15.1.3	Make sure that your information systems comply with all relevant contractual security requirements	
	15.1.5	Operate your information systems in compliance with all relevant statutory, regulatory, and contractual security requirements	
	15.1.6	Manage your information systems in compliance with all relevant statutory, regulatory, and contractual security requirements	
	15.2	Perform security compliance reviews	
	15.2.1	Make sure that your systems comply with your organization's security policies	Varonis products provide detailed audit information of file system activity, helping an organization to comply with security policies
	15.2.2	Make sure that your systems comply with your organization's security standards	
	15.2.3	Review the security of your information systems	

Clause Requirement	Sec	Control Objective/Control	Description
	15.2.4	Make sure that your information security reviews are carried out on a regular basis	
	15.2.5	Review the security of your information systems by examining how well they comply with security policies	
	15.2.6	Audit your technical platforms and information systems by examining how well they comply with relevant security implementation standards	
	15.2.7	Audit your technical platforms and information systems by examining how well they comply with documented security control requirements	
	15.3	Carry out controlled information system audits	
	15.3.1	Perform audits of your information systems	Varonis provides detailed audit information on all file system and authorization activity

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 INSTALLATION

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 Nürnberg T +49(0) 911 8937 1111 **E** sales-germany@varonis.com **W** sites.varonis.com/de