Comprehensive Visibility and Asset Inventory: First Step To FISMA Compliance

The Federal Information Security Management Act (FISMA) continues to be one of the most important pieces of cybersecurity legislation in the United States. FISMA is federal law that mandates federal agencies to develop, document, and implement an information security and protection program.

At the highest of levels, FISMA establishes a comprehensive yet flexible security framework to help agencies protect their users, systems, and data from these threats. The details of security implementation can vary from agency to agency based on the unique mission, sensitivity of data and systems, and the types of threats the organization faces. Yet while the details can be tailored to the needs of each agency, FISMA establishes a consistent approach and methodology that all organizations must follow.

FISMA requires annual compliance audits and the audit results are publicly available. While FISMA compliance is beyond the scope of any single security solution, the Ordr SCE provides an easy, efficient and highly flexible way for organizations to address a wide variety of FISMA requirements – starting with complete asset inventory. Complete asset inventory and its full visibility of every device connected to your network is critical for meeting FISMA compliance, as you cannot protect what you don't see. With a passive, and agentless deployment, organizations can establish visibility over all their connected devices including managed, unmanaged, IoT, and OT devices. This visibility ensures a full inventory of devices in the environment, the ability to find vulnerabilities, signs of compromise, anomalous behaviors and much more.

Real-time visibility and asset inventory is also foundational to augment vulnerability management solutions and Network Access Control (NAC). As an example, IoT/OT devices and their behaviors are not visible or understood by existing CDM or C2C NAC solutions, leaving asset inventory databases partial and incomplete. Ordr solves this problem.

In this document, we briefly look at what the FISMA law requires of organizations along with specific ways that Ordr can help achieve and document compliance.

Why Comply?

FISMA holds federal agencies accountable to secure government information. Failure to pass a FISMA security inspection can result in:

- Unfavorable publicity and visibility
- A reduction in their federal budget
- Administrative sanctions

FISMA Overview

FISMA was originally enacted in 2002 as Title III of the **E-Government Act**, and later amended as part of the **Federal Information Security Modernization Act of 2014**. The law lays out the requirements for federal agencies to develop, implement, and maintain information security practices commensurate with the unique mission and risks of each agency. This notably extends to outside entities such as contractors or other agencies that interact with an agency's data and systems.

The **FISMA Implementation Project** defines the goal of the law as follows:

The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

It is ultimately the responsibility of each agency to identify the unique risks of the organization and develop security processes and controls that are appropriate to the level of risk. As such, FISMA does not define a single immutable checklist for compliance. Instead, the law defines an overarching Risk Management Framework (RMF) that can be applied to any federal agency. The details of the RMF are defined in **NIST Special Publication 880-37 Rev 2**.

This document defines several key phases in the implementation of the RMF per SP 800-37:

Prepare: Prepare to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.

Categorize: Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.

Select: Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.

Implement: Implement the controls and describe how the controls are employed within the system and its environment of operation.

Assess: Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.

Authorize: Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.

Monitor: Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

While the RMF defines the overall process, the specific security controls are defined in a separate special publication, **NIST SP 800-53**. The most current finalized version, SP 800-53 Rev 4 defines 18 families of controls such as Access Control (AC), Risk Assessment (RA), and Incident Response (IR). Within each family, the document defines a variety of specific controls, actions, and activities that can be used to protect agency systems and data.

The following sections examine how the Ordr SCE can be applied both to the Risk Management Framework as defined in SP 800-37 as well as specific security controls defined in SP 800-53.

The RMF and the Need for Technology Neutral Visibility

The Risk Management Framework establishes the overarching requirements and process for FISMA compliance. The RMF is notably broad and thorough. Instead of diving into individual controls or technologies, the RMF lays out a model that applies to all an agency's technology systems. Organizations need to know the risk of every system, select, and implement appropriate controls, verify that the selected controls are working as intended, and monitor for ongoing changes. This creates a need for ongoing visibility and security insight into a wide range of technologies, which organizations will need to plan for.

Visibility of All Devices

As agencies approach FISMA compliance, it is important to note that the Risk Management Framework is explicitly **technology neutral**. In other words, the steps required for compliance apply to all agency systems. For example, NIST SP 800-37 calls out the following:

> *All information systems process, store, or transmit some type of information. For example, information about the temperature in a remote facility collected and transmitted by a sensor to a monitoring station, location coordinates transmitted by radio to a controller on a weapons system, photographic images transmitted by a remote camera (land/satellite-based) to a server, or health IT devices transmitting patient information via a hospital network, require protection…Therefore, cloud-based systems, industrial/process control systems, weapons systems, cyber-physical systems, applications, IoT devices, or mobile devices/ systems, do not require a separate risk management process but rather a tailored set of controls and specific implementation details determined by applying the existing RMF process.*

The RMF reiterates this explicitly by stating:

> *The terms system, system element, enabling system, other systems, and the environment of operation are agnostic with respect to information technology (IT) and operations technology (OT).*

Takeaways and Ordr Benefits:

While the RMF recognizes that different controls may be required for different types of technologies, the overall process and requirements remain the same. This can present a significant challenge given that many agencies lack consistent visibility into all their various systems such as IoT and OT devices.

Ordr can address this issue by providing visibility into all connected devices including IT, OT, and IoT devices. Instead of implementing and maintaining multiple tools and processes for different segments and device types, Ordr provides a centralized and consistent view into the technology environment. Additionally, device inventory, monitoring, auditing is continuously maintained and fully automated, without the need for additional operational and manual efforts from staff.

The Role of Visibility in the RMF

The Risk Management Framework's seven steps repeatedly shows the importance that visibility plays in FISMA compliance. The **Prepare**, **Categorize**, **Assess**, and **Monitor** steps all directly depend on an agency having continuous insight into their environments. The following tasks provide some key examples and how the Ordr SCE can apply:

TASK	NOTES	HOW ORDR HELPS
Task P-3	Agencies must perform a risk assessment that "***considers the totality of risk from the operation and use of its information systems.***" This can include how a device is connected to other systems and the types of information that is exchanged, and how systems are segmented from other internal and external systems.	Ordr automatically discovers, inventories and monitors all connected devices including all connections between systems. This lets staff easily see how all devices are interconnected and can recommend and even create new segmentation policies automatically.
Task P-7	Sets requirement for an "effective organization-wide continuous monitoring strategy." This is needed to maintain visibility into the security posture of systems and to verify the efficacy of controls.	Ordr continuously monitors the environment and traffic for all connected devices. The solution can verify the segmentation controls are implemented appropriately and identify signs of compromise.
Task C-1	Sets requirements to categorize each system. This cover a wide variety of information including: descriptive name of the system and system identifier; system version or release number; manufacturer and supplier information; purpose of the system and missions/business processes supported; how the system is integrated into the enterprise architecture; authorization boundary; network connection rules for communicating with external systems; interconnected systems and identifiers for those systems.	Ordr automatically classifies a wide range of devices based on their type and operational characteristics. The platform can also provide details into each device including manufacturer, device and operating system versions, and other details. The platform also maintains a flow genome of each device and the systems it communicates with and types of traffic.
Task A-2	The assessment phase is designed to ensure that the selected controls are implemented and operating as intended and providing the appropriate levels of security. Assessment plans rely heavily on documentation established in the "security and privacy plans, program management control documentation, and common control documentation." Thus, to complete Assessment tasks, agencies will need to be able to document the work from previous steps.	Ordr once again can provide visibility into the environment and document the agency environment and the processes used to maintain ongoing visibility into system inventory, risk assessment, and connectivity.
Task M-1	Requires organizations to "monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system."	Ordr continuously monitors devices and can report on changes to the device or its connectivity. This can include proactively identifying devices with vulnerabilities that may need authorized changes or can identify unexpected changes such as unusual behaviors or connectivity to new systems or external devices.
Task M-2	Organizations must "assess all controls on an ongoing basis. Ongoing assessment of the control effectiveness is part of the continuous monitoring activities of the organization."	The continuous automated nature of the Ordr platform ensures that visibility and assessment is an ongoing process. Teams can be alerted to vulnerabilities, anomalies, or signs of compromise, and can take automated action to mitigate observed risk.

FIG 1A: BEFORE ORDR

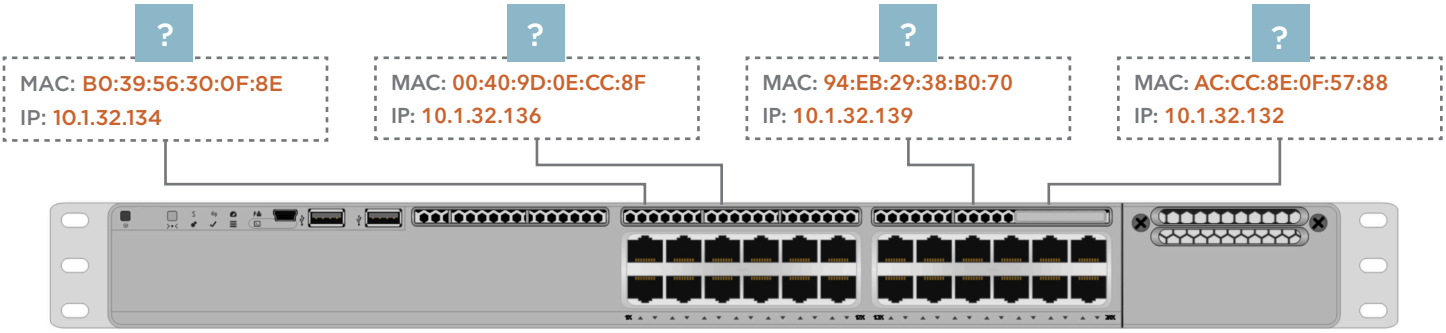
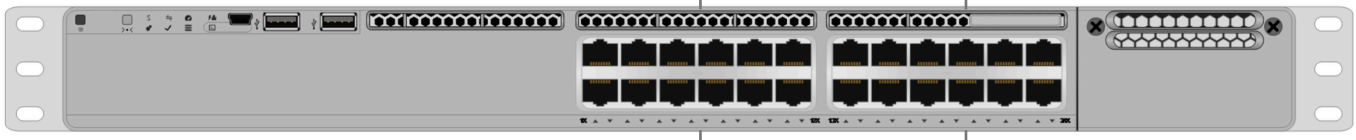


FIG 1B: AFTER ORDR

MAC: B0:39:56:30:0F:8E
IP: 10.1.32.134
MANUFACTURER: GE Vingmed Ultrasound
MODEL NAME: Vivid E95
S/N: SN17233674
OS TYPE: Windows XP
SW Version: VividE95:202.61.0
PHI: YES
MDS2 FORM LOADED: YES
FLOWS: 5 Internal / 3 External: Baselined: Normal
VULNERABILITIES: 2 FDA / 1 ICS-CERT
SEGMENT: MED-VLAN (107)
INTERNET TAG: FW-PANW-GE-ULTRASOUND

MAC: 00:40:9D:0E:CC:8F
IP: 10.1.132.136
MANUFACTURER: Baxter
MODEL NAME: 35700BAX
S/N: 8235274
OS TYPE: PumpOS
SW Version: v6.05
PHI: YES
FLOWS: 6 Internal / 0 External: Baselined: Normal
VULNERABILITIES: 2 FDA / 1 ICS-CERT
RIPPLE20 VULN: True
SEGMENT: PUMP-VLAN (56)
INTERNET TAG: FW-PANW-NO-INTERNET



MAC: 94:EB:29:38:B0:70
IP: 10.1.32.139
MANUFACTURER: Zebra Tech Inc.
MODEL NAME: QLn420
S/N: ZE807716524
OS TYPE: Android
SW Version: 2.4r.0
PHI: NO
PASSWORD ALARM: Default Manufacturer Password
FLOWS: 4 Internal / 2 External: 2 Malicious Flow
VULNERABILITIES: 2 ICS-CERT
URGENT 11 VULN: TRUE
SEGMENT: VLAN (14)
INTERNET TAG: FW-PANW-PRINT

MAC: AC:CC:8E:0F:57:88
IP: 10.1.32.132
MANUFACTURER: Axis Comm AB
MODEL NAME: AxisComm-P3364
S/N: N/A
OS TYPE: Linux3.2
SW Version: N/A
PHI: NO
FLOWS: 2 Internal / 8 External: Baselined: RISK
2 Malicious Flows - CHINA - port 21
VULNERABILITIES: 3 ICS-CERT
SEGMENT: UNKNOWN
INTERNET TAG: NONE

Figure 1: Visibility before Ordr (1a) and after Ordr (1b)

These tasks provide some specific examples of the role visibility plays in the RMF and FISMA compliance. The overarching requirement is that organizations have the responsibility to know about all the devices in their environments, their security posture, and their relationship to other devices and systems in the environment. The need to achieve this visibility in an ongoing and continuous way that applies to all devices including IT and OT can be a considerable challenge for most agencies. Ordr can vastly simplify these challenges by offering a simple, automated system that maintains visibility and security context for all connected systems.

Ordr and FISMA Security Controls

While the NIST SP 800-37 provides the overall security framework, SP 800-53 provides the detailed security and privacy controls needed to achieve compliance. SP 800-53 contains 18 families of controls covering just under a thousand individual controls. Naturally, organizations are not required to implement all possible controls. Instead agencies are free to select the controls that are appropriate to their mission based on the processes laid out by the RMF.

The Ordr SCE contains a variety of capabilities that likewise can apply to a variety of controls defined in SP 800-53. This section provides a high-level overview of Ordr's capabilities and how they map to the overall families of controls. However, this list should not be considered exhaustive and questions regarding specific controls should be directed to an agency's assessors or an Ordr representative.

CONTROL FAMILY	OVERVIEW	HOW ORDR APPLIES
Access Control (AC)	The AC group covers a wide range of controls governing how data and systems are accessed. This includes identity-based controls, implementation of Least Privilege, and more.	Ordr automatically maps the connectivity of all devices, allowing security teams to how devices are communicating. Traditional identity-based controls may not be ideal for OT and IoT devices, and Ordr can automatically identify the type and purpose of devices, identify the key services they require to function, and automatically develop and implement segmentation policies to ensure functionality with least privilege.
Assessment and Monitoring (CA)	The CA family covers a wide range of assessment, authorization, and monitoring capabilities. This includes the need for organizations to review and authorize the interconnections between systems both internally and externally. CA also defines the need for a continuous monitoring program of controls.	Ordr automatically learns the flow genome of each connected device in the environment. Staff can easily review how devices are connected including the types of protocols used. The platform can automatically create and enforce segmentation policies to minimize the unnecessary interconnections between devices. The platform continuously monitors traffic and behavior of all devices and can alert to changes or abnormal behavior.
Configuration Management (CM)	The CM family sets the need for baselining of device configurations including "communication and connectivity-related aspects of the system". CM controls also include the need to verify that security and privacy controls are functioning properly.	The Ordr platform automatically baselines the communication patterns of devices and can alert on changes and anomalies. The platform can also audit for connected devices using weak or open passwords.

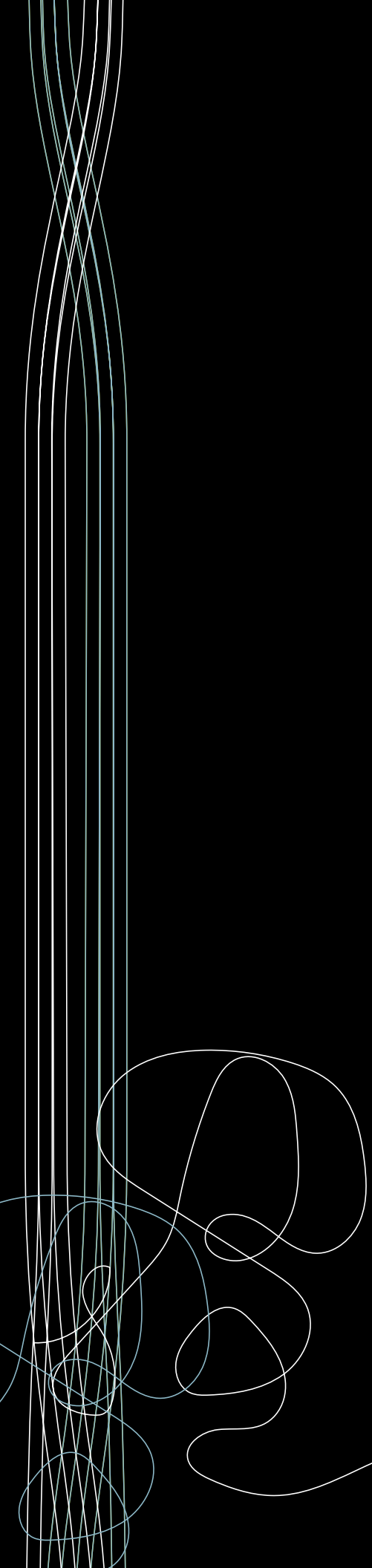
CONTROL FAMILY	OVERVIEW	HOW ORDR APPLIES
Incident Response (IR)	The IR family includes the need to automatically monitor, track, analyze, and respond to security incidents. Specific controls are dedicated to the automated collection of forensic data and the automated reconfiguration of devices such as router and firewall rules and ACLs	Ordr provides alerting of a variety of events including indicators of compromise as well as anomalous or suspicious device behavior. The platform additionally integrates with a variety of additional tools such as SIEMs and IT service management (ITSM) platforms to facilitate the response and resolution of events. The platform can also automatically create segmentation rules for affected devices and push those rules to firewalls.
Risk Assessment (RA)	The RA group defines a variety of needs related vulnerability scanning as well as responses for response processes to mitigate detected risk.	Ordr performs a continuous risk assessment of the environment based on observed vulnerabilities and threat-based indicators of risk. The solution includes a built-in vulnerability scanner and optionally integrates with other 3rd party vulnerability scanners. Ordr also ingest data from a variety of external sources such as industry-specific recall databases to identify devices that pose a particular risk. Devices that are recalled, vulnerable, or show signs of compromise can be automatically isolated based on company policy.
System Communication Protection (SC)	The SC group is one of the largest in SP 800-53. This includes a variety of controls including the access and flow control, establishing boundary protections, and dynamic isolation and segregation capabilities.	Ordr automatically learns and documents the flow genome of all connected devices and can highlight potential problems. The solution also shows the flow of information relative to internal boundaries such as VLANs as well as external connections. Next the platform can automatically isolate and segregate on a per device basis based on its unique needs and changing risk profile.
System and Information Integrity (SI)	The SI family is another large group covering several security controls. This includes controls dedicated to flaw remediation, a system-wide IDS, and the analysis of traffic patterns to identify signs of threats or potential exfiltration.	The Ordr platform continuously monitors the environment to detect both known and unknown signs of threats. The solution includes a built-in network intrusion and malware detection system. This can include the detection of threats based on the behavior of threats as well as established IOCs such as malicious IP addresses or URLs. The system can likewise ingest data from external intelligence feeds to facilitate the detection and response to threats. Once threats are detected the system can integrate with firewalls and other enforcement tools to dynamically isolate the affected device.

Conclusions

FISMA requires organizations to take a comprehensive approach to the security and protection of agency assets. And while the details of compliance will vary from agency to agency, the core requirements remain consistent. At a minimum, each agency will need visibility into the risk and security posture of their various IT and OT systems. This insight is essential to select controls that are appropriate for the agency and its unique mission. Once controls are defined and deployed, organizations will need to ensure that the controls are operating as intended, while monitoring the environment for changes on an ongoing basis.

The Ordr SCE provides a highly efficient way for organizations to meet many of the fundamental requirements set out in the Risk Management Framework as well as deliver on a wide range of specific security controls. Naturally, the expansive nature of FISMA means that no single solution will address all or even most of the requirements established by the law. However, Ordr provides a simple, low friction approach to security that brings technology neutral visibility into devices, finds weaknesses, risks, and threats, and can take action to segment and isolate devices as needed based on policy or as a response to incidents.

If you would like to learn more about the Order SCE, please contact the team at **www.ordr.net** or **info@ordr.net**.



ōrdr

info@ordr.net
www.ordr.net

2445 Augustine Drive Suite 601
Santa Clara, CA 95054