What You Need to Know About FISMA Compliance and Your GRC Tool

Table of Contents

Summary 3
Fundamentals for Fisma Compliance 3
Conducting Assessments and Authorizations 3
- Asset Enumeration 3
- Assessments 3
- Authorizations 3
- Continuous Monitoring 4
- Reporting 4

Additional Considerations 4
- Framework Updates 4
- Vulnerability Scanning 4
- Deployment and Buy-in 4

Conclusion 4
Additional Resources 4

Summary

This document provides a high-level overview of how a Governance, Risk and Compliance (GRC) platform can help your organization obtain and maintain Federal Information Systems Management Act (FISMA) compliance over the long term.

As your organization grows and its footprint increases, so does risk. While a small organization can get by with a few resources managing a few documents, eventually you reach a point where more time is spent maintaining discontiguous documentation instead of performing actual security. This is where a GRC platform is essential to getting greater efficiencies from your security resources.

Fundamentals for Fisma Compliance

To achieve "FISMA compliance" an organization must establish business processes to conduct security analysis, and then utilize that data to identify and manage their risk. This is an organization-wide effort involving everyone from the top down.

To successfully achieve FISMA compliance, business operations must be in-place, or at least defined. A GRC platform is not a silver bullet and it will not dictate an organization's business operations. However, it can help your organization manage and coordinate the complex risk management efforts surrounding business processes. As your organization's business processes are refined over time, your GRC tool should be able to grow with them.

Conducting Assessments and Authorizations

FISMA compliance requires that your organization follow a Risk Management Framework (RMF), which ultimately ends in obtaining and maintaining Authorizations to Operate (ATO) for each identified Security Boundary (i.e. "Systems"). Your GRC platform should help by cataloging Systems, assisting with conducting Assessments, and maintaining ATOs.

Primarily this is accomplished by identifying your assets and then conducting security assessments on those assets.

Asset Enumeration

The most fundamental task across many cyber security disciplines is identifying assets. An asset could be valuable information (data), hardware / devices, or software. Assets are typically discovered through some combination of network scanning tools and other business processes. Remember to leverage your existing resources such as your Accounting Department or Configuration Management Program to help collect this data.

Your GRC platform should help keep track of this information in a centralized fashion. It should be able to import and correlate asset data from your automated network scanners alongside any other incoming asset data entries (e.g. manual data entry). The tool should also facilitate a way to relate every asset to a formal security boundary. Any asset that is not related is a red flag indicating it may not be secured.

Assessments

Your GRC platform should support the collection of assessment data based on required controls and be able to generate reports summarizing results. As weaknesses are identified, perform a risk assessment to determine prioritization and remediation.

Look for a platform that comes out of the box with pre-defined workflows that will allow you to start conducting and collecting assessments based on controls defined in 800-53 Revision 4.

Authorizations

When an Authorizing Official (AO) issues an ATO they are providing formalized permission of a security boundary to run in the organization.

Your GRC platform should be able to provide risk summary information to help with the risk decisions process, and track dates and data related to the ATO. It could also facilitate obtaining the ATO as a business process and serve as the system of record holding this vital information.

Ideally, you would use the platform to signify Authorizations and record the terms and conditions of the ATO. Create workflows to help automate and track Authorizations. Enter ATO expiration dates so you can stay on top of on-going security responsibilities and reduce management overhead.

Continuous Monitoring

Once you have your ATO, you need to keep pace with re-assessment work so it does not build up into a major end-of-Authorization sprint. In a medium- to large-scale cybersecurity program, that can be a difficult and complex task to perform without a properly configured, data-driven tool.

A GRC platform should help keep track of control evaluations on an at-minimum annual basis. Use it to set due dates, assign, and track status per individual control. This will greatly assist your organization in keeping track of status and understanding what if anything is falling behind schedule.

Reporting

Throughout a system's security life cycle, key documents must be provided and made available at various levels of and points in time. For example, to obtain an Authorization to Operate (ATO) a Systems Security Plan (SSP), a list of POA&Ms, and Risk Analysis Report (RAR) must be provided to support the Authorizing Official (AO) in their Risk Decision process.

A GRC platform should be able to capture required data for these key documents, and generate the documents as-needed and with real-time data.

Look for a system that provides data in a variety of ways using customized searches, charts/dashboards, etc. in a snapshot format such as reports. The goal is to easily capture and report on summary security information.

Additional Considerations

Framework Updates

As cybersecurity practices mature, frameworks are constantly being updated. Your GRC platform should help you keep up with these changes as they are often required within a period of time to be considered compliant. Your system must be able to integrate and apply new frameworks into the organization's business processes.

Vulnerability Scanning

Vulnerability scanning is a vital part of an organization's ability to keep track of assets and their compliance levels. A GRC platform should be able to integrate information from these automated sources to support ongoing assessment efforts.

Deployment and Buy-in

Organizations often want everything up and running at once. Often when default configurations are deployed, but do not match exactly to business processes, confidence is lost in the product. This is true of any GRC platform. To help gain early wins and buy-in, consider phased deployments where the easiest use cases are implemented first. After production use is achieved and functioning, more advanced implementations would follow.

Conclusion

FISMA compliance is about identifying and managing your risk using the prescribed NIST Risk Management Framework. A properly established GRC solution will help your Cyber Security Program run more efficiently by enforcing risk management business processes with automation and collecting security information in a centralized fashion. Doing so removes management overhead, and provides more consistent results over manually managed processes.

Additional Resources

NIST Special Publication 800-37 Revision 1

About Rsam

Rsam is a leader in the field of Governance, Risk, and Compliance (GRC) solutions and is the fastest time-to-value GRC provider. The Rsam platform delivers unparalleled flexibility for companies to leverage out-of-the-box solutions and "Build Your Own" (BYO) applications for a wide range of GRC functional areas, including audit, business continuity management, compliance, enterprise risk, IT risk, incident management, operational risk, policy management, security risk intelligence, vendor risk management, regulatory change management and more. Learn more about Rsam at http://www.rsam.com

