RSI | Datasheet

FISMA

Compliance Services

The Federal Information Security Management Act (FISMA) is a federal law designed to enhance the cybersecurity posture of government agencies and supporting agencies. That includes federal agencies, departments, and subcontractors. Meeting FISMA requirements is critical for third-party vendors and contractors to keep doing business with the federal government. Ensuring FISMA compliance future-proofs your status as a contractor.

Subcontractors and vendors must provide proof of FISMA compliance via an annual assessment. Moreover, many non-governmental agencies and contractors implement FISMA because of the high levels of security and data security that it provides. Since you'll need to work directly with regulatory agencies throughout the FISMA compliance process, you'll want to partner with experienced cybersecurity and compliance experts like those at RSI Security.

Audit Preparation

You'll work closely with an RSI Security expert to help prepare for your annual FISMA assessment. We'll provide a customized audit preparation plan that you'll execute alongside a FISMA expert to prevent any unexpected surprises during your annual assessment. RSI Security's FISMA preparation services help you pass your audit with flying colors.

Tech Integration

Whether you operate in the cloud or on-premise, RSI Security's technical expertise will help integrate any tools and software necessary for FISMA compliance. FISMA puts forth specific requirements in the area of security controls, making the proper use of tools such as firewalls, malware detection, and threat monitoring software a can't skip step in FISMA compliance.

Security Assessment

Maintaining FISMA compliance is more than just satisfying auditors. It's part of a comprehensive approach to continuously improving your overall cybersecurity posture. Our experts will provide a full assessment of your cybersecurity posture and internal cyber hygiene practices to get you FISMA compliant and maintain the integrity of your data and systems.

Penetration Testing

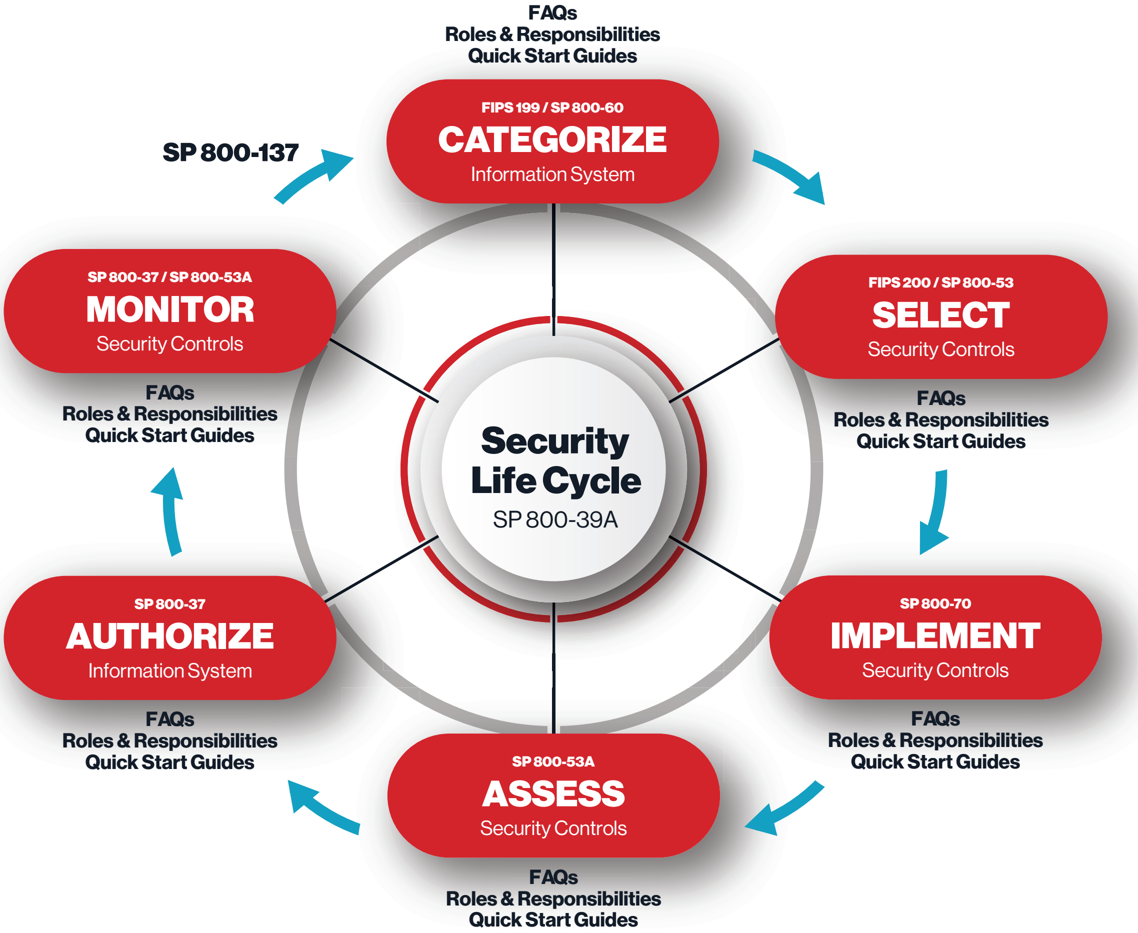
FISMA mandates continuous monitoring of cyber threats for organizations to becompliant. RSI Security provides costeffective penetration testing both as preparation for your audit and as a part of year-round monitoring and compliance efforts. Our penetration testing services will spot weak points in your systems and help shore them up pre and post FISMA audit.

About the RMF

Step #1:

Maintain Information System Inventory

Identification and documentation are necessary for the adequate recording of system inventories. These inventories must include the following information: description, manufacturer, model number, date of purchase or lease when deployed when the hardware was last updated, a record of maintenance or repairs, a record of service, and disposition.



Step #2:

Categorize Information Systems

Use the inventory from the first step; the next is to evaluate risk categorization to identify systems that hold sensitive data. The Federal Processing Standard 199 (FIPS 199) categorizes the risk of a system by confidentiality, integrity, and availability. Each of these measures is then ranked as low, medium, or high to identify the necessary security measures to avoid compromise. This risk register is the input to create the system security plan as outlined in step three.

Step #3:

Maintain a System Security Plan

Using the risk register, create a required plan of security controls and policies and a plan of action with milestones with timetables for implementation of new controls. This security plan must be reviewed and updated regularly.

Step #4:

Utilize Security Controls

Leveraging the security plan created in step three, SP 800-53 acts as a catalog of security controls to select appropriate controls to protect your systems. The requirements listed in NIST SP 800-53 apply to "all components of an information system that process, store, or transmit federal information."

There is a range of security controls discussed, including:

- *Risk Assessment.*
- *Certification, Accreditation, and Security Assessments.*
- *System Services and Acquisitions.*
- *Security Planning.*
- *Configuration Management.*
- *System and Communications Protection.*
- *Personnel Security.*
- *Awareness and Training.*
- *Physical and Environmental Protection.*
- *Media Protection.*
- *Contingency Planning.*
- *System and Information Integrity.*
- *Incident Response.*
- *Identification and Authentication.*
- *Access Control.*
- *Accountability and Audit.*

An important note is that not all controls apply, and only those relevant to your type of system are needed. The selection of controls must meet the necessary and defined standards applicable.

Step #5:

Conduct Risk Assessments

After selecting and implementing controls, it is necessary to assess the controls you are using to determine if there are any gaps in your process or additional controls needed for complete coverage. NIST SP 800-30 outlines how to conduct risk assessments. You need to protect everything from individuals to assets and operations. This risk assessment should be rigorous to ensure adequate security measures are in place.

Step #6:

Certification and Accreditation

After tweaking your controls and completing the necessary documentation, you need to get your system controls certified and accredited to show that they function correctly. Once this review is deemed complete and you pass, your information system will be accredited. The certification process is outlined in NIST SP 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems.”

The four primary phases of the certification and accreditation process are planning, certification, accreditation, and continuous monitoring.

Step #7:

Continuous Monitoring

The final phase necessary is continuous monitoring of the security controls and systems for modifications and changes. Types of monitoring include **configuration management, file integrity monitoring, vulnerability scanning, and log analysis.**

The RSI Security Difference

Personalization

RSI Security takes a personalized, hands-on approach to each and every client. Our approach to FISMA compliance is to get all of our clients certified in record time, with minimal stress, at an affordable cost basis.

Systemization

Our FISMA compliance and cybersecurity experts have in-depth knowledge of each level of FISMA compliance and can help operationalize FISMA security control requirements within your organization.

Expertise

Finally, RSI Security has years of experience and expertise working with government bodies, agencies, and bureaus of all shapes and sizes. No matter where you’re doing business with the federal government, RSI Security can help you reach FISMA compliance quickly and painlessly.

About RSI Security

RSI Security is the nation’s premier information security and compliance provider dedicated to helping organizations achieve risk-management success. We work with some of the world’s leading companies, institutions, and governments to ensure their information safety and compliance with the applicable regulations.

We also are a security and compliance software ISV and stay at the forefront of innovative tools to save assessment time, increase compliance, and provide additional safeguard assurance. With a unique blend of software-based automation and managed services, RSI Security can assist all sizes of organizations in managing IT governance, risk management, and compliance efforts (GRC).