RAPID7

Federal Information Security Management Act (FISMA)

Compliance Guide

A Compliance Guide by Rapid7

June 2012

FISMA Compliance guide

What is FISMA?

FISMA stands for the Federal Information Security Management Act (FISMA), a United States legislation signed in 2002 to underline the importance of information security to the economic and national security interests of the United States.

FISMA requires federal agencies to develop, document, and implement an information security program to safeguard their information systems including those provided or managed by another agency, contractor, or another third party.

Who must be FISMA compliant?

All government agencies, government contractors, and organizations that exchange data directly with government systems must be FISMA compliant. This may include such diverse entities as data clearinghouses, state government departments, and government military subcontractors in cases where data is exchanged directly with Federal government systems.

Who is responsible for FISMA compliance?

Agency program officials, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general.

What are the consequences of non-compliance?

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

- Significant administrative sanctions
- Unfavorable publicity
- Reduction of IT budget

What is the FISMA compliance framework?

The FISMA Implementation Project of NIST, the National Institute of Standards and Technology, develops and maintains a whole set of standards and guidelines to which IT federal systems must adhere to be FISMA compliant.

Key publications

The key publications for FISMA consist of two mandatory security standards and one specific guideline:

FIPS Publication 199: Standard for Security Categorization of Federal Information and Information Systems. It requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

FIPS Publication 200: Minimum security requirements for information and information systems. It covers seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.

Each security-related area falls into one of three general classes of security controls: management, operational, and technical.

Management

- Certification, Accreditation, and Security Assessments (CA)
- Planning (PL)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

Operational

- Awareness and Training (AT)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

Technical

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)

Note: The above security control classes and security-areas could be assimilated to the six domains and 12 requirements of PCI DSS.

NIST SP 800-53, Revision 4 (February 2012): Recommended Security Controls for Federal Information Systems and Organizations. This publication describes in detail the security controls associated with the designated impact levels of the organizational information systems.

Additional supporting publications

In addition to the above key publications, organizations subjected to compliance could benefit from a library of guidelines to support their compliance journey.

NIST SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories
NIST SP 800-18	Guide for Developing Security Plans for Federal Information Systems
NIST SP 800-30	Risk Management Guide for Information Technology Systems
NIST SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
NIST SP 800-59	Guide for Identifying an Information System as a National Security System
NIST SP 800-128	Guide for Security-Focused Configuration Management of Information Systems
NIST SP 800-137	Information Security Continuous Monitoring for Federal Information Systems and Organizations
OMB Memorandum M-10-15 and M-11-33	Define the use of CyberScope as the sole reporting mechanism for FISMA

How organizations can comply with FISMA

To comply with the federal standard, organizations must:

1. Determine the security category of their information system in accordance with **FIPS 199**, Standards for Security Categorization of Federal Information and Information Systems.
2. Derive the information system impact level from the security category in accordance with **FIPS 200.**
3. Apply the appropriately tailored set of baseline security controls in **NIST Special Publication 800-53**, Security Controls for Federal Information Systems and Organizations. Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in **Special Publication 800-53**. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission, business requirements and environments of operation.
4. Adhere to Department of Homeland Security (DHS) direction to report critical security metrics through CyberScope. Whereas the FISMA reporting process used to take place on annual basis, the current mandates require agencies to report security data on a monthly basis which allows security practitioners to make decisions using more information delivered more quickly than ever before.

How is FISMA compliance validated?

To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, chief information officers, chief information security officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency's information security program and report the results to Department of Homeland Security (DHS).

In this context, all departments and agencies are required to coordinate and cooperate with the Department of Homeland Security as it carries out its cybersecurity responsibility and activities, including:

- Overseeing the government-wide and agency-specific implementation of and reporting on cybersecurity policies and guidance.
- Overseeing and assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity.
- Overseeing the agencies' cybersecurity operations and incident response and providing appropriate assistance.
- Annually reviewing the agencies' cybersecurity programs.
- Developing analyses for the Office of Management and Budget (OMB) to assist in the development of the FISMA annual report. OMB uses this data to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

The compliance review and validation process consists in a three-step process:

1. **Data feeds directly from security management tools**
   On a monthly and quarterly basis, agencies must connect to CyberScope, the FISMA online compliance tool and feed data in the following areas:
   - Inventory
   - Systems and Services
   - Hardware
   - Software
   - External Connections
   - Security Training
   - Identity Management and Access
2. **Government-wide benchmarking on security posture**
   A set of questions on the security posture of the agencies will also be asked in CyberScope. All agencies, except micro-agencies, will be required to respond to these questions in addition to the data feeds described above.
3. **Agency-specific interviews**
   As a follow-up to the questions described above, a team of government security specialists will interview all agencies individually on their respective security postures.
   These interviews will be focused on specific threats that each agency faces as a function of its unique mission.

How Rapid7 can help

Rapid7 has extensive experience partnering with federal departments and agencies to help them meet their regulatory requirements. Rapid7 provides full end-to-end security solutions and services for government agencies and subcontractors to help them meet FISMA compliance using security control classes defined in FIPS 200 and described in detail in NIST SP 800-53 Revision 4.

Rapid7 Nexpose is a security risk intelligence solution that proactively supports the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting, and mitigation.

In the context of FISMA, Nexpose helps agencies to:

- Get a clear sense of the Real Risk posed by identified IT vulnerabilities and misconfigurations across your organization (RA)
- Quickly focus on items that pose the greatest risk (RA)
- Maintain the inventory of your systems, services, and applications (SA)
- Detect and report unauthorized software (SA)
- Perform comprehensive unified vulnerability scanning of all vital systems including networks, operating systems, web applications, databases, enterprise applications, and custom applications (RA)
- Efficiently identify misconfigurations and vulnerabilities so they can meet security policies, laws, and regulations (CM)
- Monitor software installation policies (SA)
- Audit users and groups on your systems (PS)
- Discover accounts that were terminated (PS)
- Manage remediation plans (SI)
- Support incident responses by providing details on vulnerabilities and misconfigurations that were exploited, as well as remediation steps to prevent future exploits (IR)
- Validate enforcement of access restrictions (AC)
- Test external and internal boundaries defenses (SC)
- Deliver auditable and reportable events on vulnerabilities throughout the infrastructure (AU)

In addition, Nexpose users can meet FISMA requirements by creating CyberScope reports based on USGCB and FDCC checklists. Federal agencies and contractors must use certified CyberScope solutions in order to submit their monthly FISMA reports.

Rapid7 Metasploit Pro is a penetration testing solution helping the enterprise vulnerability management program and test how well their perimeter holds up against real world attacks.

In the context of FISMA, Metasploit Pro helps agencies to:

- Test their technical external and internal defenses, policies, and procedures (CA+SC)
- Validate the level of exploitability of identified vulnerabilities (CA+RA)
- Support their incident responses plan by providing details on vulnerabilities and misconfigurations that were exploited, as well as remediation steps to prevent future exploits (IR)
- Survey hosts for use of approved authentication measures (IA)
- Audit password length and complexity and authentication methods (IA)
- Test the efficiency of their access control systems and policies (AC)

Rapid7 Consulting service helps agencies to:

- Perform formal risk assessments and assist in writing documentation to meet FISMA requirements (RA)
- Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities (RA+CA+SA)
- Conduct a vulnerability analysis on the information system (RA)
- Perform a full PCI Gap Analysis including Penetration Testing and Social Engineering to evaluate your daily security controls, determine if security policies are being followed in actual day-to-day operations, identifies gaps in your security program, and provide guidance on developing missing control policies and procedures required to secure information systems and data from external threats (RA+CA+SA+PL+PE+MP+CP+MA+IA+AC+SC+AU)
- Support the development and writing of security plan (PL)
- Provide customizable security awareness training to users of your organizational information systems (AT)
- Provides vulnerability management security training and certification to managers and users of organizational information systems (AT)
- Recommend best practices to optimize data security, including usage of two-factor authentication for remote access to the network, secure dial-in service, terminal access controls with tokens, or VPNs with individual certificates (IA+AC)

	Nexpose	Metasploit	Consulting Service
Management			
Risk Assessment (RA)	x	x	x
System and Services Acquisition (SA)	x		x
Certification, Accreditation, and Security Assessments (CA)		x	x
Security Planning (PL)			x
Operational Controls			
Personnel Security (PS)	x		x
Physical and Environmental Protection (PE)			x
Media Protection (MP)			x
Contingency Planning (CP)			x
Configuration Management (CM)	x		x
System and Information Integrity (SI)	x		x
Maintenance (MA)			x
Awareness Training (AT)			x
Incident Response (IR)	x	x	x
Technical Controls			
Identification and Authentication (IA)		x	x
Access Controls (AC)	x	x	x
System and Communications Protection (SC)	x	x	x
Audit and accountability (AU)	x		x

Rapid7 solutions for FISMA compliance

The section goes into detail about FISMA's seventeen security requirements and **how Rapid7 Nexpose, Metasploit Pro, and Consulting Services help agencies and federal contractors become FISMA compliant**.

Management Controls

Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Associated detailed security controls:

RA-1	Risk Assessment Policy and Procedures
RA-2	Security Categorization
RA-3	Risk Assessment
RA-5	Vulnerability Scanning

Use Rapid7 Nexpose to:

- Get top-down visibility of risk to your assets and business operations enabling your agency to organize and prioritize thousands of assets and quickly focus on the items that pose the greatest risk.
- Get a clear map of the Real Risk posed by the identified vulnerabilities across your organization's IT landscape. Nexpose is the only product that includes real exploit and malware intelligence combined with CVSS base scores, temporal scoring, environment considerations (e.g., any mitigating controls in place), and asset criticality for risk classification.
- Make the inventory of your systems, services, and installed applications using the latest fingerprinting technologies.
- Provides an automated mechanism to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials through automated alerts.
- Perform comprehensive unified vulnerability scanning of all vital systems including networks, operating systems, web applications, databases, enterprise applications, and custom applications.
- Generate easy-to-use detailed reports combined with role-based access controls to allow organizations to share information easily.
- Provides an automated mechanism to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

Use Rapid7 Consulting Services to:

- Perform formal risk assessments and assist in writing documentation to meet FISMA requirements.
- Conduct a vulnerability analysis on information systems.
- Perform penetration testing on information systems based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.
- Perform a full PCI gap analysis, including penetration testing and social engineering to evaluate your daily security controls, determine if security policies are being followed in actual day-to-day operations, identify

gaps in your security program, and provide guidance on developing missing control policies and procedures required to secure information systems and data from external threats.

System and Services Acquisition (SA)

Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect outsourced organizational information, applications, and/or services.

Associated detailed security controls:

SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	System development Life Cycle
SA-4	Acquisitions Process
SA-5	Information System Documentation
SA-8	Security Engineering Principles
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing
SA-12	Supply Chain Protection
SA-14	Critical Information System Components
SA-15	Development Process, Standards, and Tools
SA-16	Developer-Provided Training
SA-17	Developer Security Architecture and Design
SA-18	Tamper Resistance and Detection
SA-19	Anti-Counterfeit

Use Rapid7 Consulting Services to:

- Perform an independent analysis and penetration testing against delivered information systems, information system components, and information technology products.
- Evaluate your security controls, identifies gaps in your security program, determines if security policies are being followed in actual day-to-day operations, and provides guidance on developing missing control policies and procedures required to secure private data from unauthorized access.

Use Rapid7 Nexpose to:

- Make an inventory of all systems and software.
- Monitor software installation policies and report on illegal software installed on user systems.

Certification, Accreditation, and Security Assessments (CA)

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Associated detailed security controls:

CA-1	Security Assessment and Authorization Policies and Procedures
CA-2	Security Assessments
CA-3	Information System Connections
CA-5	Plan of Action and Milestones
CA-6	Security Authorization
CA-7	Continuous Monitoring

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure private data from unauthorized access.
- Perform your external and internal penetration testing to determine if a hacker could access and steal protected data. Penetration testing includes network-layer and application-layer tests. Penetration testing is conducted using Nexpose in conjunction with a variety of specialized tools including Metasploit, the leading open-source penetration testing platform with the world's largest database of public, tested exploits.

Use Rapid7 Nexpose in conjunction with Metasploit Pro to:

- Self-conduct assessment of your technical defenses, policies and procedures in your information systems.

Security Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Associated detailed security controls:

PL-1	Security Planning Policy and Procedures
PL-2	System Security Plan
PL-4	Rules of Behavior
PL-7	Security Concept of Operations
PL-8	Security Architecture

Use Rapid7 Consulting Services to:

- Support the development and writing of a security plan.
- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure private data from unauthorized access.

Operational Controls

Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Associated detailed security controls:

PS-1	Personnel Security Policy and Procedures
PS-2	Position Categorization
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-6	Access Agreements
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions

Use Rapid7 Nexpose to:

- Audits users and groups on your systems.
- Discovers accounts that were terminated and review results either in the UI or in a report format, and then use the data to feed your information access and management policies.

Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Associated detailed security controls:

PE-1	Physical and Environmental Protection P1 Policy and Procedures
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
PE-4	Access Control for Transmission Medium
PE-5	Access Control for Output Devices
PE-6	Monitoring Physical Access
PE-8	Visitor Access Records
PE-9	Power Equipment and Cabling
PE-10	Emergency Shutoff

PE-11	Emergency Power
PE-12	Emergency Lighting
PE-13	Fire Protection
PE-14	Temperature and Humidity Controls
PE-15	Water Damage Protection
PE-16	Delivery and Removal
PE-17	Alternate Work Site
PE-18	Location of Information System Components
PE-19	Information Leakage
PE-20	Port and I/O Device Access

Use Rapid7 Consulting Services to:

- Evaluate your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and provide guidance on developing missing control policies and procedures required to secure private data from unauthorized access.

Media Protection (MP)

Organizations must: (i) protect information contained in organizational information systems in printed form or on digital media; (ii) limit access to information in printed form or on digital media removed from organizational information systems to authorized users; and (iii) sanitize or destroy digital media before disposal or release for reuse.

Associated detailed security controls:

MP-1	Media Protection Policy and Procedures
MP-2	Media Access
MP-3	Media Marking
MP-4	Media Storage
MP-5	Media Transport
MP-6	Media Sanitization
MP-7	Media Use
MP-8	Media Downgrading

Use Rapid7 Consulting Services to:

- Evaluate and document your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to- day operations, and recommend ways to address any deficiencies.

Contingency Planning (CP)

- Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post- disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Associated detailed security controls:

CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan

CP-3	Contingency Training
CP-4	Contingency Plan Testing and Exercises
CP-6	Alternate Storage Site
CP-7	Alternate Processing Site
CP-8	Telecommunications Services
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
CP-11	Predictable Failure Prevention
CP-12	Alternate Communications Protocols
CP-13	Safe Mode

Use Rapid7 Nexpose to:

- Ensure continuous logging of historical scan data showing a device's previous state.
- Use automated utility to save duplicates of data to a backup server.

Use Rapid7 Consulting Services to:

- Audit your recovery plans to identify any gaps that should be addressed in order to successfully backup and restore systems, and establish procedures to ensure business process continuity and private protection while operating in emergency mode.

Configuration Management (CM)

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems; (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems; and (iii) monitor and control changes to the baseline configurations and to the constituent components of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Associated detailed security controls:

CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configuration
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-5	Access Restrictions for Change
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inventory
CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions
CM-11	User-Installed Software

Use Rapid7 Nexpose to:

Efficiently identify misconfigurations and vulnerabilities so you can meet security policies, laws and regulations by providing:

- Single-scan capabilities: Nexpose simultaneously scans for vulnerabilities and configuration issues.
- Broad security configuration assessment coverage: Nexpose supports policies for the United States Government Configuration Baseline (USGCB) as well as those policies as defined in Federal Desktop Core Configuration (FDCC).
- Validate security configuration compliance against a broad range of systems including Windows, IBM AS/400, Oracle, Lotus Notes/Domino and Unix. For Windows policies, standard Microsoft security template files can be imported into Nexpose. For other systems, XML-based configuration policies can be defined.
- Extensibility and an advanced policy engine: Nexpose's Advanced Policy Engine has been built from the ground up to natively support industry standard XCCDF and OVAL content, enabling users to use existing content libraries and processes to extend Nexpose. All policy templates, including the FDCC and USGCB templates in Nexpose can be fully customized and new templates can be created or imported. Nexpose will integrate with external configuration and patch management systems via vendor drop down or Nexpose open API.
- Detailed compliance reporting at your fingertips: The Policies tab in Nexpose provides real-time compliance statistics at the policy and rule level to quickly gauge compliance across your organization. For more detailed reports, use the Policy Evaluation report, or include Policy Evaluation report section in custom reports. Additionally, Nexpose automates CyberScope reporting on misconfigurations which is a mandate as part of the monthly FISMA reporting requirements.

System and Information Integrity (SI)

Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Associated detailed security controls:

SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-5	Security Alerts, Advisories, and Directives
SI-6	Security Function Verification
SI-7	Software, Firmware, and Information P1 Integrity
SI-8	Spam Protection
SI-9	Information Input Restrictions
SI-10	Information Input Validation
SI-11	Error Handling
SI-12	Information Output Handling and Retention

SI-14	Non-Persistence

Use Rapid7 Nexpose to:

- Get a clear map of the Real Risk posed by the identified vulnerabilities across your organization's IT landscape. Nexpose is the only product that includes real exploit and malware intelligence combined with CVSS base scores, temporal scoring, environment considerations (e.g., any mitigating controls in place), and asset criticality for risk classification.
- Get a detailed, sequenced remediation roadmap with time estimates for each task which can then be managed either through Nexpose's built-in ticket system or through a leading help desk system such as Remedy, Peregrine, Tivoli, or CA.

Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Associated detailed security controls:

MA-1	System Maintenance Policy and Procedures
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-4	Non-Local Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance

Use Rapid7 Consulting Services to:

- Evaluate and document your security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to- day operations, and recommend ways to address any deficiencies.

Awareness Training (AT)

Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Associated detailed security controls:

AT-1	Security Awareness and Training Policy and Procedures
AT-2	Security Awareness
AT-3	Security Training
AT-4	Security Training Records

AT-5	Contacts with Security Groups and Associations

Use Rapid7 Consulting Services to:

- Provide customizable security awareness training to users of your organizational information systems.
- Provide vulnerability management security training and certification to managers and users of organizational information systems requiring knowledge and technical abilities to detect and validate vulnerabilities on the IT infrastructure, determine the associated risk severity, write IT risks reports, apply mitigations through remediation and control.

Use the Rapid7 community, SecurityStreet, to:

- Stay up-to-date with the latest development in the vulnerability management and information security areas.

Incident Response (IR)

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Associated detailed security controls:

IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training
IR-3	Incident Response Testing and Exercises
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting
IR-7	Incident Response Assistance
IR-8	Incident Response Plan
IR-9	Information Spillage Response

User Rapid7 Nexpose and Metasploit Pro to:

Support your incident responses by providing details on vulnerabilities and misconfigurations that were exploited, as well as remediation steps to prevent future exploits.

Technical Controls

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Associated detailed security controls:

IA-1	Identification and Authentication Policy and Procedures

IA-2	Identification and Authentication (Organizational Users)
IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-6	Authenticator Feedback
IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non- Organizational Users)
IA-9	Service Identification and Authentication
IA-10	Alternative Authentication
IA-11	Adaptive Identification and Authentication
IA-12	Reauthentication

Use Rapid7 Customized Policy Compliance Framework to:

- Set up automated monitoring access controls, including number of login attempts, password length, allowable special characters, and other login ID access control policies.

Use Rapid7 Metasploit Pro to:

- Survey hosts for use of approved authentication measures.
- Audit password length and complexity and authentication methods.

Use Rapid7 Consulting Services to:

- Recommend best practices to optimize data security, including usage of two-factor authentication for remote access to the network, secure dial-in service, terminal access controls with tokens, or VPNs with individual certificates.
- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies.

Access Controls (AC)

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Associated detailed security controls:

AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-7	Unsuccessful Login Attempts
AC-8	System Use Notification
AC-9	Previous Logon (Access) Notification
AC-10	Concurrent Session Control
AC-11	Session Lock

AC-14	Permitted Actions without Identification or Authentication
AC-16	Security Attributes
AC-17	Remote Access
AC-18	Wireless Access
AC-19	Access Control for Mobile Devices
AC-20	Use of External Information Systems
AC-21	Collaboration and Information Sharing
AC-22	Publicly Accessible Content
AC-23	Data Mining Protection
AC-24	Access Control Decisions
AC-25	Reference Monitor Function

Use Rapid7 Nexpose to:

- Leverage our customized policy compliance framework to set up automated monitoring access controls (including adherence to policies for role-based access) to validate enforcement of access restrictions.

Use Rapid7 Metasploit Pro to:

- Test the efficiency of your access control systems and policies.

Use Rapid7 Consulting Services to:

- Identify gaps in your security program, determines if security policies are being followed in actual day-to-day operations (i.e. policies for maintaining least privilege, segregation of duties, and patching on databases containing private data), and provides guidance on developing missing control policies and procedures required to secure private data from external and internal threats.
- Recommend best practices to optimize data security, including system access policies to limit access to system components and sensitive data to only those whose job role absolutely requires such access.
- Evaluate and document security controls, identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations, and recommend ways to address any deficiencies

System and Communications Protection (SC)

Organizations must: (i) monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

Associated detailed security controls:

SC-1	System and Communications Protection Policy and Procedures
SC-2	Application Partitioning
SC-3	Security Function Isolation
SC-4	Information in Shared Resources
SC-5	Denial of Service Protection
SC-6	Resource Availability
SC-7	Boundary Protection
SC-8	Transmission Integrity

SC-9	Transmission Confidentiality
SC-10	Network Disconnect
SC-11	Trusted Path
SC-12	Cryptographic Key Establishment and Management
SC-13	Cryptography Protection
SC-14	Public Access Protections
SC-15	Collaborative Computing Devices
SC-16	Transmission of Security Attributes
SC-17	Public Key Infrastructure Certificates
SC-18	Mobile Code
SC-19	Voice Over Internet Protocol
SC-20	Secure Name /Address Resolution Service (Authoritative Source)
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Name/Address Resolution Service
SC-23	Session Authenticity
SC-24	Fail in Known State
SC-25	Thin Nodes
SC-26	Honeypots
SC-27	Operating System-Independent Applications
SC-28	Protection of Information at Rest
SC-29	Heterogeneity
SC-30	Concealment and Misdirection
SC-31	Covert Channel Analysis
SC-32	Information System Partitioning
SC-34	Non-Modifiable Executable Programs
SC-35	Technical Surveillance Countermeasures P0 Survey
SC-36	Honeyclients
SC-37	Distributed Processing and Storage
SC-38	Malware Analysis
SC-39	Out-of-Band Channels
SC-40	Operations Security
SC-41	Process Isolation
SC-42	Wireless Link Protection

Use Rapid7 Nexpose and Metasploit Pro to:

- Test your external and internal boundaries defences.

Use Rapid7 Consulting Services to:

- Identify gaps in your security program, determine if security policies are being followed in actual day-to-day operations for the protection of organizational communications at the external boundaries and key internal boundaries of the information systems, and provide guidance on developing missing control policies and procedures required to secure sensitive data from external and internal threats.

Audit and accountability (AU)

Organizations must create, protect and retain information system audit records to the extend needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity and ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Associated detailed security controls:

AU-1	Audit and Accountability Policy and Procedures
AU-2	Auditable Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-6	Audit Review, Analysis, and Reporting
AU-7	Audit Reduction and Report Generation
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-10	Non-repudiation
AU-11	Audit Record Retention
AU-12	Audit Generation
AU-13	Monitoring for Information Disclosure
AU-14	Session Audit
AU-15	Alternate Audit Capability
AU-16	Cross-Organizational Auditing

Use Rapid7 Nexpose to:

- Deliver auditable and reportable events on vulnerabilities throughout the infrastructure.
- Provide records to what occurred, sources of events and outcomes of events related to vulnerabilities using:
  - Remediation reports with step-by-step instructions on how to address vulnerabilities.
  - Centralized console to manage vulnerability content and events throughout information systems.
- Allow for expanded storage via integrated relational database.
- Provide rich reporting functionality for reporting and analysis as well as alert systems that could be configured based on status and vulnerability severity.
- Integrate with several other security products such as IDS and IPS and penetration tools.
- Provide time stamps for vulnerability data.
- Provide role-based access controls to limit vulnerability information to appropriate party.

About Rapid7

Rapid7 is the leading provider of security risk intelligence. Its integrated vulnerability management and penetration testing products, **Nexpose** and **Metasploit**, empower organizations to obtain accurate, actionable and contextual intelligence into their threat and risk posture. Rapid7's solutions are used by more than 2,000 enterprises and government agencies in more than 65 countries, while the Company's free products are downloaded more than one million times per year and enhanced by the more than 125,000 members of its open source security community.

Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a "Top Place to Work" by the Boston Globe. Its products are top rated by Gartner®, Forrester® and SC Magazine. The Company is backed by Bain Capital Ventures and Technology Crossover Ventures.

For more information about Rapid7, please visit http://www.rapid7.com.