

# ISO 27002 COMPLIANCE GUIDE

How Rapid7 Can Help You Achieve Compliance  
with ISO 27002

# CONTENTS

Introduction	2
Detailed Controls Mapping	3
About Rapid7	8

# INTRODUCTION

If you're looking for a comprehensive, global framework to tailor your security program, then ISO 27002 may be right for your organization. Compliance doesn't equal security, but standards such as ISO 27002 can be a helpful tool for demonstrating your security posture to internal and external stakeholders. You can even opt to get certified by the International Organization for Standardization (ISO) to provide additional reassurance to customers and partners. Like any best practices around security controls, you'll get the most out of ISO 27002 if you read between the lines to understand the intent behind each guideline. We recommend you use the standard as a starting point and, where possible, go beyond the minimum requirements to take your security program to the next level.

## What is ISO 27002?

ISO 27002 is an internationally recognized standard designed for organizations to use as a reference for implementing and managing information security controls. The standard is intended to be used with ISO 27001, which provides guidance for establishing and maintaining information security management systems. Many organizations use ISO 27001 and 27002 in conjunction as a framework for showing compliance with regulations where detailed requirements are not provided, for example Sarbanes-Oxley Act (SOX) in the U.S. and the Data Protection Directive in the EU. Published in October 2013, the latest version of ISO 27002 covers 14 security controls areas (numbered from 5 to 18), with implementation guidance and requirements for each specific control.

## How Rapid7 Can Help

Rapid7 products and services can help organizations address controls recommended in ISO 27002 as follows:

- **InsightVM** is a vulnerability management solution that can help organizations identify and classify their assets (8.1 and 8.2), audit password policies (9.2.4, 9.3.1, 9.4.3), identify and prioritize vulnerabilities (12.6.1), and more.
- **Metasploit** is a penetration testing solution that can help organizations validate vulnerability exploitability (12.6.1), audit the effectiveness of network segmentation (13.1.3), conduct technical compliance tests (18.2.3), and more.
- **InsightAppSec** is a web application security solution that can help organizations test the security of web applications (14.2.3, 14.2.8, 14.2.9).
- **InsightIDR** is an advanced SIEM solution that can help organizations monitor user access to the network (9.1.2, 9.2.3, 9.2.5), collect and analyze events (12.4.1, 12.4.2, 12.4.3), assist in incident response (16.1.4, 16.1.7), and more.

Rapid7 can provide **Security Consulting Services** to perform an assessment of an organization's current state of controls against the ISO 27002 framework and identify gaps in their security program. Rapid7 can also develop and review security policies (5.1.1, 5.1.2), conduct penetration tests (14.2.8, 14.2.9, 18.2.3), respond to security incidents (16.1.5, 16.1.7), and more.

# DETAILED CONTROLS MAPPING

Below is a mapping of ISO 27002 controls to the Rapid7 products and services that can address at least part of the requirements. Please refer to the ISO/IEC 27002:2013 document on [www.iso.org](http://www.iso.org) for a complete description of each control and detailed requirements.

Control Category	Control Description	Product/Service	How Rapid7 Can Help
<b>5. INFORMATION SECURITY POLICIES</b>			
<b>5.1 Management direction for information security</b>			
5.1.1 Policies for information policy	Define, approve, and communicate a set of policies for information security.	<ul style="list-style-type: none"> <li>Security Program Development</li> </ul>	<ul style="list-style-type: none"> <li>Rapid7 can help organizations build an effective security program taking into account their business strategy, compliance requirements, and the threat landscape.</li> </ul>
5.1.2 Review of the policies for information security	Review policies at planned intervals or if significant changes occur.	<ul style="list-style-type: none"> <li>Cyber Security Maturity Assessment</li> </ul>	<ul style="list-style-type: none"> <li>Rapid7 can perform an assessment of an organization's current state of controls, policies, and procedures, and identify tactical and strategic initiatives for improving security.</li> </ul>
<b>8. ASSET MANAGEMENT</b>			
<b>8.1 Responsibility for assets</b>			
8.1.1 Inventory of assets	Identify organizational assets and maintain an inventory of these assets.	<ul style="list-style-type: none"> <li>InsightVM</li> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightVM enables assets to be tagged with contextual information, including assigning an asset owner.</li> <li>InsightIDR automatically detects the primary user of each asset.</li> </ul>
8.1.2 Ownership of assets	Assign an asset owner for assets maintained in the inventory.	<ul style="list-style-type: none"> <li>InsightVM</li> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightVM enables assets to be tagged with contextual information, including assigning an asset owner.</li> <li>InsightIDR automatically detects the primary user of each asset.</li> </ul>
<b>8.2 Information classification</b>			
8.2.1 Classification of information	Classify information and assets in terms of value, criticality and sensitivity.	<ul style="list-style-type: none"> <li>InsightVM</li> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightVM enables assets to be tagged with contextual information, including classifying an asset's criticality.</li> <li>InsightIDR enables assets to be tagged as critical.</li> </ul>
<b>8.3 Media handling</b>			
8.3.1 Management of removable media	Implement procedures to manage the use of removable media.	<ul style="list-style-type: none"> <li>InsightVM</li> </ul>	<ul style="list-style-type: none"> <li>InsightVM can measure part of this control by providing the ability to audit whether autoplay is allowed on devices.</li> </ul>

<b>9. ACCESS CONTROL</b>			
<b>9.1 Business requirements of access control</b>			
9.1.2 Access to networks and network services	Limit user access to the network and monitor use of network services.	<ul style="list-style-type: none"> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightIDR provides ability to monitor configurable network zones and access policies, and alerts on violation of these policies.</li> </ul>
<b>9.2 User access management</b>			
9.2.3 Management of privileged access rights	Restrict and control allocation and use of privileged access rights.	<ul style="list-style-type: none"> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightIDR monitors use of administrative accounts, and alerts on new admin accounts and account privilege escalation.</li> </ul>
9.2.4 Management of secret authentication information	Control allocation of passwords and change default vendor passwords.	<ul style="list-style-type: none"> <li>InsightVM</li> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightVM automatically scans the entire network to identify systems that are configured with default credentials.</li> <li>InsightIDR automatically detects accounts that are shared between multiple users.</li> </ul>
9.2.5 Review of user access rights	Review user access rights at regular intervals and after any changes.	<ul style="list-style-type: none"> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightIDR provides visibility of all user accounts, including local, domain, and cloud services accounts.</li> </ul>
<b>9.3 User responsibilities</b>			
9.3.1 Use of secret authentication information	Ensure users are following the organization's password policies.	<ul style="list-style-type: none"> <li>InsightVM</li> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightVM provides fully customizable policy scanning to audit passwords for minimum complexity and length.</li> <li>InsightIDR automatically detects user credentials that may have been compromised in third-party breaches.</li> </ul>
<b>9.4 System and application access control</b>			
9.4.1 Information access restriction	Restrict access to information and applications based on access control policy.	<ul style="list-style-type: none"> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightIDR can partially help with this control by monitoring access to key applications, and alerting on unauthorized or suspicious usage.</li> </ul>
9.4.2 Secure log-on procedures	Control access to systems and applications by a secure log-on procedure.	<ul style="list-style-type: none"> <li>InsightVM</li> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightVM can measure part of this control by providing the ability to audit account lockout configurations, including maximum failed log-on attempts.</li> <li>InsightIDR automatically detects unauthorized access, and alerts on brute force attempts and unusual authentication activity.</li> </ul>
9.4.3 Password management system	Password management systems should ensure quality passwords.	<ul style="list-style-type: none"> <li>InsightVM</li> <li>Metasploit</li> </ul>	<ul style="list-style-type: none"> <li>InsightVM provides ability to audit password policy configurations, including complexity, expiry, re-use and encryption.</li> <li>Metasploit tests password quality with online brute-force attacks, offline password cracking, and credentials re-use.</li> </ul>

## 12. OPERATIONS SECURITY

### 12.2 Protection from malware

12.2.1 Controls against malware	Implement detection and prevention controls to protect against malware.	<ul style="list-style-type: none"> <li>• InsightVM</li> <li>• InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>• InsightVM scans every Windows workstation to check that: <ul style="list-style-type: none"> <li>• URL filtering and website reputation scanning are enabled;</li> <li>• E-mail clients are configured to block certain attachments;</li> <li>• Anti-malware software is installed, enabled and up-to-date.</li> </ul> </li> <li>• InsightIDR detects known malicious processes on endpoints, and identifies unauthorized software that is rare or unique.</li> </ul>
---------------------------------	-------------------------------------------------------------------------	-------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 12.4 Logging and monitoring

12.4.1 Event logging	Record user activities, exceptions, faults, and information security events.	<ul style="list-style-type: none"> <li>• InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>• InsightIDR collects logs, correlates events by user, machine and IP, and analyzes for anomalies and suspicious activities.</li> </ul>
12.4.2 Protection of log information	Protect log information against tampering and unauthorized access.	<ul style="list-style-type: none"> <li>• InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>• InsightIDR saves logs from various sources in a secure, offsite location, and alerts on event log files being deleted.</li> </ul>
12.4.3 Administrator and operator logs	Log and review system administrator and operator activities regularly.	<ul style="list-style-type: none"> <li>• InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>• InsightIDR provides visibility of all administrator activities, including local, domain and cloud service admin accounts.</li> </ul>

### 12.6 Technical vulnerability management

12.6.1 Management of technical vulnerabilities	Evaluate the organization's exposure to vulnerabilities and address associated risks.	<ul style="list-style-type: none"> <li>• InsightVM</li> <li>• Metasploit</li> <li>• InsightIDR</li> <li>• Managed Services</li> </ul>	<ul style="list-style-type: none"> <li>• InsightVM automatically scans the entire network for vulnerabilities and prioritizes for remediation based on risk.</li> <li>• Metasploit automatically tests the exploitability of vulnerabilities to demonstrate exposure for prioritization.</li> <li>• InsightIDR correlates vulnerability data with event logs to provide additional user context to incidents.</li> <li>• Rapid7 can provide a fully-managed, cloud-based vulnerability management service operated on a monthly or quarterly basis.</li> </ul>
------------------------------------------------	---------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## 13. COMMUNICATIONS SECURITY

### 13.1 Network security management

13.1.3 Segregation in networks	Segregate groups of information services, users and systems on networks.	<ul style="list-style-type: none"> <li>• Metasploit</li> <li>• InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>• Metasploit automates the task of testing whether network segmentation is operational and effective.</li> <li>• InsightIDR provides ability to monitor configurable network zones and access policies, and alerts on violation of these policies.</li> </ul>
--------------------------------	--------------------------------------------------------------------------	--------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>13.2 Information transfer policies and procedures</b>			
13.2.1 Information transfer policies and procedures	Protect the transfer of information through all types of communication facilities.	<ul style="list-style-type: none"> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightIDR can partially help with this control by providing visibility into usage of cloud-based communications or storage services.</li> </ul>
<b>14. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE</b>			
<b>14.2 Security in development and support process</b>			
14.2.3 Technical review of applications after operating platform changes	Review and test business critical applications when operating platforms change.	<ul style="list-style-type: none"> <li>InsightAppSec</li> </ul>	<ul style="list-style-type: none"> <li>InsightAppSec can be used to dynamically scan applications when operating platforms change to identify vulnerabilities.</li> </ul>
14.2.8 System security testing	Conduct testing of security functionality during development.	<ul style="list-style-type: none"> <li>InsightAppSec</li> <li>Penetration Testing Services</li> </ul>	<ul style="list-style-type: none"> <li>InsightAppSec integrates with continuous integration tools to identify vulnerabilities within the development lifecycle.</li> <li>Rapid7 can perform manual penetration testing on web and mobile applications to identify security weaknesses.</li> </ul>
14.2.9 System acceptance testing	Conduct acceptance testing for new information systems, upgrades and new versions.	<ul style="list-style-type: none"> <li>InsightAppSec</li> <li>Penetration Testing Services</li> </ul>	<ul style="list-style-type: none"> <li>InsightAppSec can be used to dynamically scan new applications, upgrades and new versions to identify vulnerabilities.</li> <li>Rapid7 can perform manual penetration testing on web and mobile applications to identify security weaknesses.</li> </ul>
<b>16. INFORMATION SECURITY INCIDENT MANAGEMENT</b>			
<b>16.1 Management of information security incidents and improvements</b>			
16.1.1 Responsibilities and procedures	Establish responsibilities and procedures for response to security incidents.	<ul style="list-style-type: none"> <li>Incident Response Program Development</li> </ul>	<ul style="list-style-type: none"> <li>Rapid7 can perform an assessment of the organization's current preparedness and help develop an incident response plan.</li> </ul>
16.1.4 Assessment of and decision on information security events	Assess events to decide if they are to be classified as security incidents.	<ul style="list-style-type: none"> <li>InsightIDR</li> </ul>	<ul style="list-style-type: none"> <li>InsightIDR uses behavioral analytics to detect security incidents and speeds up assessment of security events by providing instant user context and incident investigation tools.</li> </ul>
16.1.5 Response to information security incidents	Respond to security incidents according to documented procedures.	<ul style="list-style-type: none"> <li>Incident Response Services</li> </ul>	<ul style="list-style-type: none"> <li>Rapid7 can help organizations with all stages of incident response from analysis and detection to containment and remediation.</li> </ul>
16.1.7 Collection of evidence	Define and apply procedures for identification and collection of evidence.	<ul style="list-style-type: none"> <li>InsightIDR</li> <li>Incident Response Services</li> </ul>	<ul style="list-style-type: none"> <li>InsightIDR provides ability to map findings to an interactive timeline and produce a final report for communication.</li> <li>Rapid7 can help organizations develop an incident response plan and define evidence collection and documentation processes.</li> </ul>

## 18. COMPLIANCE

### 18.2 Information security reviews

18.2.1 Independent review of information security	Review approach to managing information security at planned intervals.	<ul style="list-style-type: none"><li>• Cyber Security Maturity Assessment</li></ul>	<ul style="list-style-type: none"><li>• Rapid7 can perform an assessment of an organization's current state of controls, policies and procedures, and identify tactical and strategic initiatives for improving security.</li></ul>
18.2.3 Technical compliance review	Review compliance with policies and standards regularly.	<ul style="list-style-type: none"><li>• InsightVM</li><li>• Metasploit</li><li>• Penetration testing services</li></ul>	<ul style="list-style-type: none"><li>• InsightVM provides auditing and reporting capabilities for assessing compliance with security policies and standards.</li><li>• Metasploit allows organizations to simulate real-world attacks and test effectiveness of security controls.</li><li>• Rapid7 can perform penetration tests on network infrastructure and applications to test the security of information systems.</li></ul>



# ABOUT RAPID7

Rapid7 (NASDAQ:RPD) is trusted by IT and security professionals around the world to manage risk, simplify modern IT complexity, and drive innovation. Rapid7 analytics transform today's vast amounts of security and IT data into the answers needed to securely develop and operate sophisticated IT networks and applications. Rapid7 research, technology, and services drive vulnerability management, penetration testing, application security, incident detection and response, and log management for thousands of organizations around the globe. To learn more about Rapid7 or join our threat research, visit [www.rapid7.com](http://www.rapid7.com).