Mapping Rapid7 Capabilities to ISO 27002:2022 Controls

How Rapid7 Supports ISO 27002 Controls

TABLE OF CONTENTS

Introduction

If your organisation collects, uses, or processes data, there will always be information security risks and threats to watch out for. To guard against these risks, you should have an Information Security Management System (ISMS) to ensure the confidentiality, availability, and integrity of all information and information assets.

If you're looking for a comprehensive, global standard to tailor your security program, then ISO 27001 may be right for your organisation. ISO/IEC 27001 outlines how organisations can protect their information systematically and cost-effectively by adopting an Information Security Management System (ISMS) through an organised approach to maintaining confidentiality, integrity, and availability. It is based on identifying the potential threats to an organisation's information through risk assessment and implementing appropriate controls.

The ISO/IEC 27001 standard lists specific security controls for organisations to follow in Annex A. It doesn't provide details on implementation of these controls, however, and this is where ISO/IEC 27002 comes into play.

ISO/IEC 27002 provides guidance on the selection, implementation, and management of security controls based on an organisation's information security risk environment and acts as a supplement to ISO 27001.

It should be noted that organisations can be certified against ISO 27001 but not ISO 27002; ISO 27002 supports the certification against ISO 27001. 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.

Rapid7 products and services can help organisations address controls recommended in ISO 27002:2022 as follows:

> **InsightVM (IVM)** is a risk-based vulnerability management that focuses on remediation risk through remediating vulnerabilities. The solution helps organisations identify and classify their assets (5.9 and 5.13), understand their compliance with security policies (5.36, 8.16), identify and prioritise vulnerabilities (8.4, 8.7, 8.8, 8.9, 8.19), incorporate threat intelligence (5.7), and more. Rather than focusing on the number of vulnerabilities, enable your teams to prioritise based on exploitability and ease of exploitation, and easily define distinct work packages for resolver groups to resolve identified vulnerabilities vs creating a boat anchor CVSS report.

> **Metasploit Pro** is a penetration testing solution that can help organisations validate vulnerability exploitability (8.8, 8.30, 8.35), audit the effectiveness of network segmentation (8.22, 8.25, 8.29,8.31), conduct technical compliance tests (5.19, 5.36), and more.

> **InsightAppSec (IAS)** is a web application and API security solution that can help organisations test the security of web applications and associated APIs (5.22, 8.4, 8.12, 8.16, 8.24, 8.25, 8.28, 8.29, 8.30).

> **InsightCloudSec (ICS)** is a fully integrated cloud-native security platform (CNSP) that enables organisations to drive cloud security forward through continuous visibility, security, and compliance (5.9, 5.13, 5.15, 5.16, 5.18, 5.19, 5.23, 5.28, 5.36, 6.8, 8.2, 8.3, 8.4, 8.5, 8.7, 8.8, 8.9, 8.15, 8.16, 8.21, 8.22, 8.24, 8.25, 8..28, 8.29).

> **InsightIDR (IDR)** is an advanced SIEM/XDR solution that can help organisations monitor user access to the network (5.18,8.2, 8.21), centrally collect and analyse events (8.15), assist in incident response (5.25, 5.28), and more.

> **Managed Detection and Response (MDR)** is a fully managed service leveraging continuous threat detection by identifying known threats, certain unknown threats, and intruder movement from the endpoint to the cloud via Rapid7's own InsightIDR. The service combines unlimited/uncapped IR, breach investigations, and threat insight with sophisticated user and attacker behaviour analytics and is monitored and managed by Rapid7's world-class security analysts, with experience in hunting for dynamic threats and containing incidents to protect organisations (5.7, 5.23, 5.24, 5.25, 5.26, 6.8, 8.7).

> **Rapid7 Threat Command (TC)** is a complete external threat intelligence and brand protection solution delivering relevant, timely, and actionable threat intelligence to stakeholders (5.7). Clear, deep, and dark web sources multiply the ability to monitor and detect security incidents (8.16, 8.30), provide contextual information to help prevent threats from causing harm to organisations (7.5, 8.4, 8.7, 8.12, 8.23), and more.

> **InsightConnect (ICON)** is a security orchestration and automation tool that enhances the ability to streamline and accelerate highly manual, time-intensive processes 24 hours a day across all of Rapid7's offerings, as well as across hundreds of third-party technologies (5.6, 5.7, 5.16, 6.7, 8.18, 8.25).

> **Rapid7 Security Consulting Services (RCSS):** Rapid7 is recognised as a leader in the provision of security services and has built methodologies and frameworks to ensure consistent high-quality outcomes are achieved for customers. Rapid7 offers a broad spectrum of services with a depth built from experience and customer feedback. Service offerings include:

- **Security Advisory Services (RAS)** were designed with your realities in mind, built to help prioritise security initiatives, align them with the business, and get it all done yesterday.
  - Cyber Security Maturity Assessment (5.1, 5.35, 5.36, and more)
  - Security Program Development (5.1, 5.8, 5.13, 5.24, 5.37, and more)
  - Security Policy Development (5.1, 5.19, 5.25, 5.35, and more)
  - Merger & Acquisition (M&A) Assessment
- **Managed Services** experts can help quickly leverage security program investment by handling the operational requirements of incident detection and response, vulnerability scanning, and application security for you. Rapid7 Managed Services team offers regular assessments and concise reporting, enabling higher productivity and saving time and money.
  - Managed Vulnerability Management (MVM) (6.8, 8.8, 8.19, 8.16)
  - Managed Detection & Response (MDR)
  - Managed Application Security (MAS)
- **Detection and Response Services** will help keep a keen eye on your network's activity and ensure you have the right plan in place to respond when someone gets in.
  - Incident Response (IR) Program Development
  - Incident Response (IR) Services (5.24, 5.25, 5.26, 5.28)
- **Threat Intelligence Research** offers deep-dive investigation services and reports into external cyber threats, including incident response research, tactical attack or breach-related research, and strategic trend-based research (5.7, 8.7, 8.8, 8.16, 8.21, 8.30).
  - Data Breach Reports
  - Phishing Reports
  - OSINT/HUMINT Reports
  - Sector/Landscape Research
  - VIP Reports
  - Threat Intelligence IR
  - Social Media Reports
- **Penetration Testing (5.35, 8.8)**
- **IoT Security Testing Services**
- **Training and Certification**
  - Product and Skills Training
  - IT & Security Fundamentals

ISO 27002 is recommended as a great starting point for building secure systems and security programs. It shares many controls, processes, and strategies with other security frameworks, including CIS, NIST 800 series, Australian Information Security Manual (ISM), and the Protective Security Policy Framework (PSPF). While there is no direct alignment with other frameworks, certification in ISO 27001 supported by ISO 27002 controls provides strong assurance and many artefacts where other frameworks may apply.

Major changes from 27002:2013 to 27002:2022

Reviewed and Updated Controls

- Refinement of 4.1 Context
- Refinement of 4.2 Interested parties
- Refinement of 4.4 ISMS
- Refinement of 6.1.3 Risk treatment
- Refinement of 6.2 Objectives
- Addition of 6.3 Change management
- Refinement of 7.4 Communication
- Rewrite of 8.1 Operational planning
- Refinement of 9.1 Monitoring
- Splitting 9.2 into 9.2.1 General / 9.2.2 Audit program
- Splitting 9.3 into 9.3.1 General / 9.3.2 Input / 9.3.3 Output (and the addition of an extra topic)
- 10.1 Improvement and 10.2 Nonconformities have switched numbers (!)

Reorganisation of Categories

The controls have been reorganised into four categories instead of the earlier 14 domains as follows:

- 5. Organisational (37 controls)
- 6. People (8 controls)
- 7. Physical (14 controls)
- 8. Technological (34 controls)

Addition of 11 new controls

- Threat intelligence
- Information security for the use of cloud services
- ICT readiness for business continuity
- Physical security monitoring
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention
- Monitoring activities
- Web filtering
- Secure coding

A broad mapping of new controls to previous controls is outlined below.

ISO 27001:2022	ISO 27001:2013 equivalent
A.5.7 Threat intelligence	A.6.1.4 Contact with special interest groups
A.5.16 Identity management	A.9.2.1 User registration and de-registration
A.5.23 Information security for use of cloud services	A.15.x Supplier relationships
A.5.29 Information security during disruption	A.17.1.x Information security continuity
A.5.30 ICT readiness for business continuity	A.17.1.3 Verify, review and evaluate information security continuity
A.7.4 Physical security monitoring	A.9.2.5 Review of user access rights
A.8.9 Configuration management	A.14.2.5 Secure system engineering principles
A.8.10 Information deletion	A.18.1.3 Protection of records
A.8.11 Data masking	A.14.3.1 Protection of test data
A.8.12 Data leakage prevention	A.12.6.1 Management of technical vulnerabilities
A.8.16 Monitoring activities	A.12.4.x Logging and monitoring
A.8.23 Web filtering	A.13.1.2 Security of network services
A.8.28 Secure coding	A.14.2.1 Secure development policy

Detailed Controls Mapping

Below is a mapping of ISO 27002:2022 controls to the Rapid7 products and services that can address at least part of the requirements. Please refer to the ISO/IEC 27002:2022 document on www.iso.org for a complete description of each control and detailed requirements.

Control Description	Product/Service	How Rapid7 can help
5. Organisational Controls		
5.1 Policies for information security		
Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Cyber Security Maturity Assessment	**Rapid7** can help organisations build an effective security program taking into account their business strategy, compliance requirements, and the threat landscape.
	Security Program Development	**Rapid7** can help organisations rapidly create and deploy comprehensive security policies, standards, and guidelines.
	Security Policy Development	**Rapid7** can perform an assessment of an organisation's current state of controls, policies, and procedures, and identify tactical and strategic initiatives for improving security.
5.6 Contact with special interest groups		
The organisation should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	InsightConnect	**ICON** enables the building of workflows to automate the exchange of security information between organisations that extends beyond ingestion of Indicators of Compromise.
	Threat Command	**TC** collects threat intel from multiple specialist sources on global and organisation-specific threats while also supporting bidirectional sharing with applicable groups, such as ISACs and national CERTs..
	Rapid7 Memberships*	**Rapid7's** membership with the Cyber Threat Alliance (CTA) enables Rapid7 to include near real-time, high-quality cyber threat information, shared among member companies and organisations, as a default enrichment into all products and services.
5.7 Threat intelligence		
Information relating to information security threats should be collected and analysed to produce threat intelligence.	Threat Command	**TC** monitors open and closed sources, and considers specific details about an organisation, such as mentions of exploiting vulnerabilities known to exist in the organisation's environment, brand impersonation, phishing of the organisation's domains, VIP impersonation, etc. Incorporating the TIP module will integrate timely, relevant, and meaningful intelligence in support of stakeholders, regardless of their tactical, operational, or strategic requirements.
	InsightIDR	**IDR** uses integrated intel sources to trigger detections from Rapid7 curated attacker behaviour analytics and user behaviour analytics. IDR customers can import and share IOCs to other IDR customers through an integrated threat community.

	Managed Detect and Response	**MDR** expands on the threat community by having access to Rapid7's expanded intel collections for additional context and activity attribution during triage, investigation, and response.
	InsightVM	**IVM** ingests data points that provide threat intel for organisation-relevant risk scoring and correlation of potential and current exploitation against vulnerabilities detected within the organisation.
	InsightConnect	**ICON** enables the building of workflows to automate the exchange of security information between organisations that extends beyond ingestion of Indicators of Compromise.
	Threat Intel Research	**TIR** offers deep-dive investigation services and reports into external cyber threats, including incident response research, tactical attack or breach-related research, and strategic trend-based research.
5.8 Information security in project management		
Information security should be integrated into project management.	Security Program Development	**Rapid7** can help organisations rapidly create and deploy comprehensive security policies, standards, and guidelines.
5.9 Inventory of information and other associated assets		
An inventory of information and other associated assets, including owners, should be developed and maintained.	InsightVM	**IVM** discovers assets and enables tagging with contextual information, including asset owner, location, criticality, and custom tags. This information can also be shared with CMDB for more accurate inventory information.
	InsightIDR	**IDR** automatically detects the primary user of each asset.
	InsightCloudSec	**ICS** automatically detects cloud resources and can use tags and metadata for assigning system owner details.
5.13 Labelling of information		
An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Security Program Development	**Rapid7** can help organisations rapidly create and deploy comprehensive security policies, standards, and guidelines.
	InsightVM	**IVM** discovers assets and enables tagging with contextual information, including asset owner, location, criticality, and custom tags.
	InsightIDR	**IDR** enables assets to be tagged as critical and provide increased alerting of critical assets.
	InsightCloudSec	**ICS** automatically detects cloud resources, and can use tags and metadata to add contextual information such as system owner.

5.15 Access control		
Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	InsightIDR	**IDR** can partially help with this control by monitoring access to key applications and systems. This enables alerting on unauthorised or suspicious access in both the cyber and physical worlds.
	InsightCloudSec	**ICS** provides the ability to create a policy baseline using custom Insights (rules) mapped to organisational access and security policy. Along with the ability to alert on IAM that contravenes policy, the platform can automatically reconfigure controls to align with the approved baseline. The platform can assess user permissions and identify overly excessive and unused permissions, enabling the application of more appropriate access policies.
5.16 Identity management		
The full life cycle of identities should be managed.	InsightIDR	**IDR** collects and attributes activity to a user identity, including users sharing accounts or elevating their privileges. IDR also considers the status and role of an identity when assessing activity.
	InsightConnect	**ICON's** tight integration with other Rapid7 products expands their ability to automate. For example, ICON integration into HR tools enables IDR to prioritise triggering custom alerts on staff who have been terminated or submitted their resignation.
	InsightCloudSec	**ICS** records and collects all events and identifies threats across single or multi-cloud environments, and is able to identify unused accounts and accounts for identities that are no longer required. "Bots" allow the platform to alert and/or disable as required by organisation policy.
5.18 Access rights		
Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.	InsightIDR	**IDR** provides visibility into all user accounts, including local, domain, and cloud services accounts. IDR automatically detects accounts and assets that are shared between multiple users; when a user last logged in, what service authenticated the login, and the login location; and any privileged activity. Aggregating all these details combined with baselining user and asset activity means IDR provides granular and high-fidelity visibility.
	InsightIVM	**IVM** automatically scans the entire network to identify systems that are configured with default credentials or weak passwords and don't meet industry standard access standards.
	InsightCloudSec	**ICS** Access Explorer focuses on identity and access governance controls, reducing excessive cloud entitlements and streamlining least-privilege access controls across cloud environments. ICS provides full visibility of access levels, and enforces best practices and organisation policy (such as reducing overly permissive access) while automating remediation on improper permission combinations.

5.19 Information security in supplier relationship

Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Security Policy Development	**R7** can help create policies and procedures for managing suppliers and third-parties as part of our policy development services, which enables the rapid creation and deployment of comprehensive security policies, standards, and guidelines.
	Threat Command	**TC** Third Party Risk is able to provide reporting on the risk posed by existing or proposed suppliers. This reporting can be incorporated into an organisation's processes.
	InsightCloudSec	**ICS** is able to continuously assess open-source libraries used in production workloads to detect installed packages with known vulnerabilities. Integration into CI/CD pipeline mitigates the risk of introducing known vulnerabilities into production.
	InsightIDR	**IDR** detection and response for vendor accounts with compromised credentials or with suspicious activity is an important component to managing information security with suppliers.

5.22 Monitoring, review, and change management of supplier services

The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Threat Command	**TC** enables organisations to run periodic reports based on tests that identify the level of risk posed by existing or proposed third parties. The reports help organisations understand if the third party has aligned to contractual security controls and regulations. Monitoring and alerting of third-party breaches enhances TC's support of this control.
	InsightAppSec	**IAS** can be used to dynamically scan new applications, upgrades, and new versions to identify vulnerabilities.

5.23 Information security for use of cloud services

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.	InsightCloudSec	**ICS** provides the ability to create custom Insights (rules) based on business and information security best practices. The platform also provides an out-of-the-box Insight library based on industry best practices, including Essential Eight and Information Security Manual (ISM).
	InsightVM	**IVM** provides tools to understand the risk of compute assets based on detected vulnerabilities and report against the allocated metrics on configuration, mitigation, and patching efforts, highlighting levels of success and compliance.
	InsightIDR	**IDR** enables collection of security events and alerts from multiple cloud services, such as MS Azure, AWS, GCP, and other SaaS services such as OKTA, Mimecast, and many more. Once aggregated, the curated analytics detections and investigations workbench simplifies investigations of cloud security incidents, identifying breaches of policy as well as supplying the evidence linked to MITRE for attribution.
	Managed Detection and Response	**MDR** Customer Advisors (CA) are experienced security professionals that act as an extension of your team and can provide sound advice on the use of cloud and other services within the context of your organisation, industry trends, and accepted recommended practices.

5.24 Information security incident management planning and preparation

The organisation should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Incident Response Services	**Rapid7** can perform an assessment of the organisation's current preparedness and help develop an incident response plan. This engagement can be tailored to include tabletop exercises, breach readiness, or a compromise assessment to confirm your environment is clean (or not).
	Managed Detection and Response	**MDR** uses proven workflow and practices to provide uncapped IR and DFIR. Organisations can leverage the work Rapid7 has already conducted in IR management and planning to build these processes. Onboarding with MDR allows customers to leverage a model that includes the establishment of roles and responsibilities, IR procedures, and targeted regular and ad-hoc reporting.

5.25 Assessment and decision on information security events

The organisation should assess information security events and decide if they are to be categorised as information security incidents.	InsightIDR	**IDR** uses attacker and behavioural analytics, mapped to MITRE techniques, for detecting and alerting on high-fidelity security incidents. The curated analytics speed up assessment of security events by providing instant user context and attribution, evidence aligned with MITRE ATT&CK, and incident investigation tools, such as the ability to query endpoints and trigger response workflows.
	Managed Detection and Response	**MDR** analysts triage raised alerts within InsightIDR, determining if the events constitute a security incident to be further investigated by the MDR SOC team, categorising the incident, and assigning a severity. MDR can automatically respond to an incident based on categorisation and priorities agreed on between Rapid7 and the organisation. In the event of major incidents or potential zero days, MDR includes uncapped Digital Forensics Incident Response.
	Security Policy Development	**R7** can help create policies and procedures for assessing and categorising security incidents, incorporating organisation- and industry-specific rules and legislation.
	Incident Response Services	**R7** can evaluate your environment (technology, people, and process), report on your current IR capabilities, and offer relevant, business-based recommendations to help you meet your IR program goals.

5.26 Response to information security incidents

Information security incidents should be responded to in accordance with the documented procedures.	Incident Response Services	**InsightIDR** can help organisations with all stages of incident response from readiness, analysis, and detection to containment and remediation, as well as program development.
	Managed Detection and Response	**MDR** service provides unlimited and uncapped incident response and DFIR as part of the service deliverables. The customer and Rapid7 collaborate to determine when a proactive containment response is permitted against assets and/or identities, and to help mature organisational security incident response processes.
	Security Policy Development	**R7** can help create policies and procedures for responding to events assessed as security incidents, incorporating organisation- and industry-specific rules and legislation.

5.28 Collection of evidence

The organisation should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	InsightIDR	**IDR** provides the ability to map findings to an interactive timeline and produce a final report for communication. Additionally, evidence is collated within the IDR investigation workbench with attribution of recent times and dates.
	Managed Detection and Response	**MDR** service provides detailed incident findings reports, per validated each incident that clearly articulates the analysis and all gathered evidence from all related sources. Activities and timelines are tracked as investigations progress to finalisation.
	InsightCloudSec	**ICS** collects cloud event data and automatically provides the ability to map cloud security findings to an interactive timeline and produce a report for communications.
	Incident Response Services	**Rapid7** can help organisations develop an incident response plan and define evidence collection and documentation processes.
	Threat Intel Research	**TIR** offers deep-dive investigation services and reports into external cyber threats, including incident response research, tactical attack or breach-related research, and strategic trend-based research.

5.35 Independent review of information security

The organisation's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Cyber Security Maturity Assessment	**Rapid7** can help organisations build an effective security program, taking into account their business strategy, compliance requirements, and the threat landscape.
	Security Policy Development	**Rapid7** can perform an assessment of an organisation's current state of controls, policies, and procedures, and identify tactical and strategic initiatives for improving security.
	Penetration Testing	**PT** team will simulate a real-world attack on your networks, applications, devices, and/or people to demonstrate the security level of your key systems and infrastructure and show you what it will take to strengthen it.

5.36 Compliance with policies, rules and standards for information security

Compliance with the organisation's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	InsightVM	**IVM** provides policy compliance checks that are out-of-the-box collections of industry benchmark checks (e.g., CIS) focused on industry hardening standards, providing coverage for many of your check requirements. It also enables customers to create custom compliance checks that align to your organisational policies.
	InsightCloudSec	**ICS** provides compliance packs that are out-of-the-box collections of related Insights focused on industry requirements and standards for all of your resources. It also enables customers to create custom organisations information security compliance policies.
	Cyber Security Maturity Assessment	**Rapid7** can help organisations build an effective security program, taking into account their business strategy, compliance requirements, and the threat landscape.

	5.37 Documented operating procedures		
	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	Security Program Development	**Rapid7** can help organisations rapidly create and deploy comprehensive security policies, standards, guidelines and procedures.
		Security Policy Development	**Rapid7** can perform an assessment of an organisation's current state of controls, policies, and procedures, and identify tactical and strategic initiatives for improving security.
6. People Controls	**6.7 Remote working**		
	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.	InsightIDR	**IDR** provides a lightweight agent enabling collection of relevant security data from devices, even when not connected to the corporate network. In addition, IDR also collects from cloud authentication and VPN sources, which IDR combines with other collected events to enableUBA analytics to detect and alert on suspicious and unusual behaviour.
		InsightVM	**IVM** can assess the configuration of devices with the shared Insight Agent to ensure endpoints have appropriate configurations as defined by security policy.
		InsightConnect	**ICON** can trigger automation workflows based on IDR detections and IVM findings to enforce organisational security policy and incident response actions and ensure the security of information when personnel are working remotely.
	6.8 Information security event reporting		
	The organisation should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	InsightIDR	**IDR** has curated analytics to detect and report on suspicious and anomalous behaviours. The curated analytics are based on attacker and user techniques researched by threat intel analysts, investigations by consulting IR experts, and investigations performed for Rapid7 Managed Detection and Response customers.
		Managed Detection and Response	**MDR** provides comprehensive reporting on completion and any IR/DFIR. Regular cadence engagements between the MDR CA and customers and the ability of customers to access IDR all ensure that customers are always up to date on environment security events.
		InsightVM	**IVM** provides comprehensive details on vulnerabilities that exist within organisation assets through agent and/or network scanning. Results can be monitored through live dashboards or physical reports.
		Managed Vulnerability Management	**MVM** allows customers to access the IVM instance used by Rapid7 MVM analysts for near-real-time visibility of vulnerabilities across the organisation. MVM CA is regularly in contact with customers to talk through discovered vulnerabilities discovered in the environment.
		InsightCloudSec	**ICS** threat findings is a multi-cloud capability that curates threat detections from customer resources. Organisations can automatically report to appropriate channels once the suspected security events are captured.
		Security Policy Development	**Rapid7** can perform an assessment of an organisation's current state of controls, policies, and procedures.

7. People Controls	**7.4 Physical security monitoring**		
	Premises should be continuously monitored for unauthorised physical access.	InsightIDR	**IDR** is able to collect log data from physical access devices such as proxy readers, sensors, and cameras. Flexible alerting capabilities can enhance any existing monitoring system by adding analytics and aligning detections and reporting to organisational policy.
8. Technological controls	**8.1 User endpoint devices**		
	Information stored on, processed by or accessible via user endpoint devices should be protected.	Security Policy Development	**Rapid7** can perform an assessment of an organisation's current state of controls, policies, and procedures, and identify tactical and strategic initiatives for improving security.
	8.2 Privileged access rights		
	The allocation and use of privileged access rights should be restricted and managed.	InsightCloudSec	**ICS** provides the ability to scan multiple cloud accounts' identities using the least-privilege access (LPA) feature to identify and restrict overly privileged access rights and reconfigure to align with an organisation's cloud access policy baseline.
		InsightVM	**IVM** enables secure configuration assessments of IT assets against widely used industry benchmarks such as CIS and STIG, as well as custom internal policies such as ensuring that systems are configured to log all privileged access, or that privileged accounts can't perform non-privileged tasks.
		InsightIDR	**IDR** utilises the Rapid7 Insight Agent to collect account audit events from endpoints, directory servers, and can also collect from Privileged Access Management (PAM) solutions. This enables detection of privileged activity in breach of policy, including shared privileged accounts, privilege escalations, or non-privileged activity from privileged accounts. IDR provides flexible access options such as SSO and 2FA, and combined with granular RBAC support, this means that IDR can align with organisations' privileged access requirements.
	8.3 Information access restriction		
	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	InsightCloudSec	**ICS** Insights (rules) compliance packs can be customised to meet organisational access control policy to alert and remediate out of policy access configurations back into policy compliance.
		InsightIDR	**IDR** includes behavioural and attacker analytics and deception technology such as honeypots, honey creds and honey files. These capabilities provide detection, alerting, and response for unusual, suspicious, and malicious user activity. File integrity and access monitoring round out flexible capabilities supporting information access restriction.
	8.4 Access to source code		
	Read and write access to source code, development tools and software libraries should be appropriately managed.		**The Insight Platform** integrates into the CI/CD pipeline to restrict the deployment of infrastructure and services, monitor access to repositories, collect audit logs, and detect unauthorised events.

	InsightIDR	**IDR** - Monitor and report suspicious access and change events.
	InsightVM	**IVM** - Report on the vulnerabilities in Dev, Test, and Pre-prod assets prior to going live.
	InsightAppSec	**IAS** - Stop deployment of risky webapps during the SDLC.
	InsightCloudSec	**ICS** - Stop deployment of cloud resources that fail to meet security policy, including containers.
	Threat Command	**TC** - Through monitoring of clear and closed web sources, detect and alert on instances of leaked code to allow for potential remediation.
8.5 Secure authentication		
Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	InsightCloudSec	**ICS** automatically identifies cloud identities without secure authentication technologies and access restrictions. Organisations can report against non-compliant cloud identities and also remediate them appropriately.
	InsightIDR	**IDR** collects authentication events from MFA tools and solutions, cloud providers, VPN solutions, and PAMs that are correlated against curated ABA and UBA detections, as well as custom alerts. These detections and alerts can trigger automated responses to disable a user and so on. Contextual enrichment of events such as geo ip information extends visibility to authentication locations, delivering the ability to alert based on authentication locations.
8.7 Protection against malware		
Protection against malware should be implemented and supported by appropriate user awareness.	InsightIDR	**IDR** uses curated detection/behavioural detections powered by Insight Agent (EDR), device logs, antivirus detections/actions, and Insight Network Sensor and Threat Intel to alert on malware attempting to execute malicious techniques. Built-in playbooks can quarantine and respond to detected malware to halt or reduce any impact.
	Managed Detection and Response	**MDR's** unlimited and uncapped incident and breach response enables MDR's highly skilled SOC and DFIR analysts to investigate and potentially respond to detected malware. Onboarding of MDR includes a compromise assessment to determine if there is malware or a persistent threat within the network prior to MDR go-live. If malware is discovered, the IR/DFIR teams roll into action.
	Threat Command	**TC** adds organisation-specific intel from the clear and dark web to enhance IDR's detections, further increasing the fidelity and context to alerts.
	InsightVM	**IVM** provides visibility into the risk from current vulnerabilities in the environment, along with supporting the prioritisation and automated implementation of mitigation solutions. Configuration and software audit checks can also performed: • URL filtering and reputation enabled • Email clients are configured to block certain attachments • Anti-malware software is installed and enabled

	InsightCloudSec	**ICS** provides visibility into the risk from current vulnerabilities in the cloud environment, along with supporting the prioritisation and automated implementation of mitigation solutions.
	Cyber Security Maturity Assessment	**Rapid7** can help organisations build an effective security program, taking into account their current policy and technical controls to determine their existing protections from malware, and guiding them to maturing protections against malware.
	Threat Intelligence Research	**TIR** offers deep-dive investigation services and reports into external cyber threats, including incident response research, tactical attack or breach-related research, and strategic trend-based research.
8.8 Management of technical vulnerabilities		
Information about technical vulnerabilities of information systems in use should be obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	InsightCloudSec	**ICS** delivers agentless vulnerability assessments of cloud assets that continuously analyse the production environment against software vulnerabilities. This capability can be integrated into the CI/CD pipeline and fail deployments with unacceptable risk based on risk tolerances. Through the triggering of Bots, legacy or deployments can be remediated automatically.
	InsightVM	**IVM** can continuously evaluate internal and external assets against an ever-evolving collection of vulnerabilities and mitigation solutions, covering software and IP-enabled devices. Support for automated discovery of external assets using Project Sonar and internal assets using integrations with DHCP, Azure, AWS, etc., gives almost real-time tracking of assets for vulnerability assessment and visibility. Remediations can be automated, and mitigation effort status monitored and reported on in near-real-time.
	Managed Vulnerability Management	**MVM** provides automated scanning and monitoring by experienced vulnerability management analysts, utilising the Rapid7 InsightVM platform.
	Metasploit Pro	**MS Pro** automatically tests the exploitability of discovered vulnerabilities to demonstrate exposure for prioritisation.
	InsightIDR	**IDR** correlates vulnerability data with event logs to provide additional device context to incidents, improving the efficiency of investigation processes and aiding analyst investigation assessments.
	Penetration Testing	**PT** team will simulate a real-world attack on your networks, applications, devices, and/or people to demonstrate the security level of your key systems and infrastructure and show you what it will take to strengthen it.
	Threat Intelligence Research	**TIR** offers deep-dive investigation services and reports into external cyber threats, including incident response research, tactical attack or breach-related research, and strategic trend-based research.

8.9 Configuration management		
Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	InsightCloudSec	**ICS** automatically identifies all the cloud assets and their respective configurations, and businesses can easily monitor, review, and export any deviations from best practices.
	InsightVM	**IVM** includes the ability to check and report on configurations against industry standards such as CIS, PCI, and ISM, as well as build custom configuration check templates.
	Managed Vulnerability Management	**MVM** provides automated scanning and monitoring of environment configurations by experienced analysts, utilising the Rapid7 InsightVM policy management capabilities of the Insight Agent and network scanner.
8.12 Data leakage prevention		
Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Threat Command	**TC** finds and mitigates threats by proactively monitoring thousands of sources across the clear, deep, and dark web. It provides actionable, real-time information on threats outside an organisation's infrastructure, including the potential disclosure of an organisation's sensitive information. With automated remediation, customers have visibility into tailored threats and can make informed decisions.
	Threat Investigation Services	**TC** deep-dive intelligence investigation services add visibility into external threats, which inform the suitable preventative controls to implement to mitigate the risk of data leakage.
	InsightIDR	**IDR** curated detections use technique-based detection indicators to detect malicious activity early in the kill chain. Combined with automated response capabilities, this allows IDR to efficiently prevent many data leakage incidents.
	InsightAppSec	**IAS** can be used to dynamically scan applications and APIs on a scheduled basis to identify vulnerabilities and mitigate opportunities for data leakage.
8.15 Logging		
Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	InsightIDR/Managed Detection and Response	**IDR** draws on multiple methods for collecting security events from almost any source type. Agent-based, agentless, and traffic inspection provide complete network logging and visibility. Source events are aggregated in Rapid7's ISO 27001-certified Insight Platform where they are then correlated against curated attacker and user behaviour analytics and custom alerts.
	InsightCloudSec	**ICS** agentless log collection is powered by APIs, aggregating events from multiple cloud providers in near-real-time, and also supports the ingestion and analysis of vendor-specific security alerting capabilities, such as AWS Guard Duty and Azure Defender for Cloud, and if detected can invoke responses using inbuilt automation.

8.16 Monitoring activities

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	InsightIDR	**IDR** employs a robust library of detections based on Rapid7-curated attacker technique and user behaviour analytics, which are continuously correlated against a consolidated store of security events from endpoints, network, and log sources. Both on-prem and cloud sources are supported. Built-in workflows allow automated responses to align with recommended practices and organisation security policies.
	Managed Detection and Response	**MDR** analysts triage alerts and will pivot into an investigation as required. MDR provides unlimited and uncapped IR and Breach response 24 x 7 x 365 days a year, regardless of incident severity.
	InsightCloudSec	**ICS** performs real-time collection and monitoring of cloud resources in single or multi-cloud environments. ICS quickly assesses an organisation's security, vulnerability, and compliance posture to deliver a normalised view of security and compliance in multi-cloud environments.
	InsightVM	**IVM** actively monitors an IP-based asset's risk to the organisation, providing a real risk score based on multiple vulnerability characteristics. Agents and network scanning collect vulnerability information that is analysed and populates live dashboards for monitoring and visibility.
	Managed Vulnerability Management	**MVM** provides automated scanning and monitoring by experienced vulnerability management analysts, utilising the Rapid7 InsightVM platform.
	Threat Command	**TC** can integrate with vulnerability tools, including IVM, to add clear, deep, and dark web monitoring for organisation-specific vulnerabilities and mentions, adding organisation-specific context to scoring and risk to the organisation.
	InsightAppSec	**IAS** can be used to dynamically scan new web applications, upgrades, and new versions to identify vulnerabilities.
	Threat Intelligence Research	**TIR** offers deep-dive investigation services and reports into external cyber threats, including incident response research, tactical attack or breach-related research, and strategic trend-based research.

8.18 Use of privileged utility programs

The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	InsightIDR	**IDR** can natively monitor program executions on endpoints and trigger an alert and/or remediation when unauthorised users run an authorised tool, or vice versa.
	InsightConnect	**ICON** can support IDR for the creation of more complex workflows for restricting or reacting to the unauthorised execution of privileged utility programs. This is simplified by the breadth of plugins, workflows, and sources included in the Extensions Library.

8.19 Installation of software on operational systemss

Procedures and measures should be implemented to securely manage software installation on operational systems.	InsightIDR	**IDR** native endpoint monitoring combines with Fie Integrity (FIM) and Access Monitoring (FAM) for the detection of unauthorised installation, access, or execution in breach of organisation policy and procedures. Application allowlisting can also send violations to IDR, which can create alerts for investigation.

	InsightVM	**IVM** is able to perform configuration checks using industry standard frameworks like CIS, CSF, PCI, etc., and report which controls do not meet requirements. Policy can be customised to align to the organisation's security policy. Checks for third-party application allowlisting software installs can be configured, and alerted on when the software is not found.
8.21 Security of network services		
Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	InsightCloudSec	**ICS** automatically identifies and reports against weak cloud network services and can continuously report against best practices around network security rules.
	InsightVM	**IVM** is able to perform configuration checks using industry standard frameworks like CIS, CSF, PCI, etc., and report which controls do not meet requirements. Policy can be customised to align to the organisation's security policy. Goals/SLAs help you reduce overall risk and improve the security of an environment. This capability tracks remediation efforts or asset configuration by setting goals/SLAs and defining metrics to measure against those goals/SLAs, all within the InsightVM platform.
	InsightIDR	**IDR** provides the ability to monitor configurable network zones and access policies, and alerts on violation of these policies.
	Threat Intelligence Research	**TIR** offers deep-dive investigation services and reports into external cyber threats, including incident response research, tactical attack or breach-related research, and strategic trend-based research.
8.22 Segregation of networks		
Groups of information services, users and information systems should be segregated in the organisation's networks.	InsightIDR	**IDR** can perform alerting on traffic in breach of network security policy. Detections can use data from traffic flow as well as from a diverse set of supported event sources.
	InsightCloudSec	**ICS** can enforce organisation security policy, ensuring cloud environments are appropriately segregated and when configuration drift is detected, automatically remediate and alert. Integration into CI/CD allows ICS to fail infrastructure that does not meet policy, as well as detail the steps needed to meet policy and permit deployment.
	Metasploit Pro	**MS Pro** automates the task of testing whether network segmentation is operational and effective.
8.23 Web filtering		
Access to external websites should be managed to reduce exposure to malicious content.	Threat Command	**TC** detects external organisation-specific threats and, combined with the breadth of OSINT collected by the Threat Intel Platform (TIP) module, can proactively protect the organisation and its users by updating web inspection/filtering tools and blocking policies.
	InsightIDR	**IDR** is able to detect and alert on attempted access to known bad websites as provided by TC TIP and IDR's threat community. Custom alerts can report on any activity from historical events matching newly discovered intel.
	InsightVM	**IVM** checks the configuration of every Windows workstation to ensure that URL filtering and website reputation scanning are enabled.

8.24 Use of cryptography		
Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	InsightCloudSec	**ICS** can alert on poor or missing cryptographic implementation across multiple cloud providers based on recognised industry practices, as well as enforce organisation cryptographic policy. “Bots” power the ability to customise near-real-time response actions.
	InsightVM	**IVM** can use custom configuration or recognised industry standards templates to check on good crypto configuration. Templates for PCI, CIS, etc., can be used or modified to simplify getting visibility.
	InsightAppSec	**IAS** includes a number of passive and active attack modules to dynamically test for accepted encryption within app deployments. Through integration with CI/CD pipeline tools, IAS can fail and report on ineffective use of cryptography.
8.25 Secure development life cycle		
Rules for the secure development of software and systems should be established and applied.	Security Policy Development	**Rapid7** can perform an assessment of an organisation’s current state of controls, policies, and procedures, and identify and develop practical and effective rules, policy, and procedures for a secure development lifecycle.
		Rapid7 products integrate at all stages of development to ensure the development and deployment of secure systems and applications. CI/CD integration adds gates to processes before deployment can be approved:
	InsightCloudSec	**ICS** - Policy baseline configuration enforcement across multiple supported clouds, including IAM, containers, and Kubernetes vulnerability management.
	InsightAppSec	**IAS** - Dynamically scan new applications, upgrades, and new versions to identify vulnerabilities.
	InsightVM	**IVM** - Analyse solutions for vulnerabilities and configuration, while also providing risk scoring that considers any active vulnerability exploitation on the internet. Scanning and supporting automated patching helps ensure secure solutions are developed.
	Metasploit	**MS Pro** - Through community-driven exploit modules, MS Pro can provide high confidence an application or solution is or is not exploitable or high risk.
	InsightIDR	**IDR** can monitor development environments for anomalous or malicious activity through curated attacker and user behaviour analytics. This ensures the integrity of development activities and products.
	InsightConnect	**ICON** has tight integrations with Rapid7 products to add almost unlimited orchestration and automation capabilities. This means that organisations can build more effective and efficient secure processes into their development lifecycle.
8.28 Secure coding		
Secure coding principles should be applied to software development.	InsightAppSec	**IAS** can be used to dynamically scan new applications, upgrades, and new versions to identify vulnerabilities, and provide detailed evidence and testing reasoning to application developers, assisting to enhance knowledge of secure coding practices and speed of future application development projects.

	InsightCloudSec	**ICS** delivers agentless vulnerability assessments and cloud posture assessments of cloud resources that continuously analyse the environment(s) for vulnerabilities. This capability can be integrated into the CI/CD pipeline and fail deployments with unacceptable risk based on risk tolerances. Through the triggering of Bots, legacy or deployments can be remediated automatically.
8.29 Security testing in development and acceptance		
Security testing processes should be defined and implemented in the development life cycle.	InsightAppSec	**IAS** integrates with continuous integration tools to identify vulnerabilities within the development lifecycle.
	InsightVM	**IVM** vulnerability and policy checks can be integrated into SDLC processes, shifting security left and enabling technical and misconfiguration vulnerabilities to be detected and remediated early in the SDLC.
	InsightCloudSec	**ICS** supports continuous and agentless scanning of cloud resources, including the ability to fail cloud deployments that do not meet policy and/or contain vulnerable images or unacceptable configurations.
	Rapid7 Advisory Services	**RAS** can perform a penetration test to simulate a real-world attack on your networks, applications, devices, and/or people to demonstrate the security level of your key systems and infrastructure.
	MetaSploit Pro	**MS Pro** automatically tests the exploitability of discovered vulnerabilities to demonstrate exposure for prioritisation. Integration into IVM allows for validation of a vulnerability pre- and post-remediation.
8.30 Outsourced development		
The organisation should direct, monitor and review the activities related to outsourced system development.	InsightAppSec	**IAS** scanning can be added as a requirement to outsourcing contracts to ensure secure apps are being developed and required controls are being met.
	Threat Command	**TC** enables organisations to run periodic reports based on tests to identify and understand if the outsourcer has aligned to contractual security controls and regulations.
	Metasploit Pro	**MS Pro** allows organisations to simulate real world attacks and test effectiveness of security controls.
	Threat Intelligence Research	**TIR** offers deep-dive investigation services and reports into external cyber threats, including incident response research, tactical attack or breach-related research, and strategic trend-based research.
8.31 Separation of development, test and production environments		
Development, testing and production environments should be separated and secured.	InsightIDR	**IDR** provides the ability to monitor configurable network zones and access policies, and alerts on violation of these policies.
	Metasploit Pro	**MS Pro** automates the task of testing whether network segmentation is operational and effective.

Links and Reference to Further Information

International Organization of Standards (ISO) References

ISO 27001:2022: https://www.iso.org/standard/82875.html

ISO 27002:2022: https://www.iso.org/standard/75652.html

Rapid7 Product & Service References

Rapid7 Home: https://rapid7.com

Rapid7 Insight Trial Registration: https://www.rapid7.com/trial/insight/

InsightVM (IVM): https://www.rapid7.com/products/insightvm/

InsightIDR (IDR): https://www.rapid7.com/products/insightidr/

InsightAppSec (IAS): https://www.rapid7.com/products/insightappsec/

InsightCloudSec (ICS): https://www.rapid7.com/products/insightcloudsec/

InsightConnect (ICON): https://www.rapid7.com/products/insightconnect/

Metasploit Pro: https://www.rapid7.com/products/metasploit/

Threat Command (TC): https://www.rapid7.com/products/threat-command/

Rapid7 Advisory Services: https://www.rapid7.com/services/security-consulting/security-advisory-services/

Penetration Testing: https://www.rapid7.com/services/security-consulting/penetration-testing-services/

IoT Security Testing: https://www.rapid7.com/services/security-consulting/iot-security-services/

IR Services: https://www.rapid7.com/services/security-consulting/incident-response-services/

Threat Intelligence Research Services: Contact us at https://rapid7.com

Managed D&R (MDR): https://www.rapid7.com/services/managed-services/managed-detection-and-response-services/service-overview/

Managed Vulnerability Management (MVM): https://www.rapid7.com/services/managed-services/vulnerability-management/

Managed Application Security (MAS): https://www.rapid7.com/services/managed-services/managed-appsec/

Rapid7 Open Source and Free

Velociraptor - Digital Forensics and IR (DFIR): https://www.velocidex.com/

Recog Project - Network fingerprinting DB: https://github.com/rapid7/recog/

Metasploit - Free pentest tool: https://www.metasploit.com/

Rapid7 Research - Research programs and reports/webinars: https://www.rapid7.com/research/

Project Sonar - Internet-wide scanning: https://www.rapid7.com/reasearch/project-sonar/

Video overview of Project Sonar: https://share.vidyard.com/watch/LUsNP3eGSYBd3G4wPrWoP8?

Project Heisenberg - Global low-interaction honeypots : https://www.rapid7.com/research/project-heisenberg/

- Video overview of Project Heisenberg: https://share.vidyard.com/watch/uy26LJqSzyyfPUbraJS3mA?

Project Doppler - Reveals hard-to-discover exposures: https://www.rapid7.com/research/project-doppler/

- Video overview of Project Doppler: https://share.vidyard.com/watch/5pKPRRqhiYZfQa5Ep7TQwH?

Rapid7 Labs Open Data Project - Project Sonar data for security researchers: https://opendata.rapid7.com/

AttackerKB - Security forum for analysing threats: https://attackerkb.com/

Rapid7 Online Product Documentation: https://docs.rapid7.com

Rapid7 Academy - Free intro training videos: https://academy.rapid7.com

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organisations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

To learn more about Rapid7 or join our threat research, visit

www.rapid7.com