RAPID7

COMPLIANCE GUIDE

CPS 234

| How Rapid7 solutions can help

TABLE OF CONTENTS

What is CPS 234?

CPS 234 builds upon previous prudential standards. It ensures your organisation has sufficient security measures in place with regard to the criticality and sensitivity of information you hold. In short, it imposes greater cybersecurity obligations.

The financial sector is one of the more prominent targets for such attacks. It is the second-largest source of data breaches[1], having notified OAIC of 42[2] system breaches, putting them behind only health service providers in this regard. And, with the average cost[3] of a data breach in Australia sitting at $2.5 million, incidents can get very expensive.

Financial services organisations are also most likely to attribute 'hacking' to a data breach. Of the 91 data breaches attributed to hacking between February 2018 and June 2019, 17 incidents (about 18 percent) occurred in the finance and/or superannuation sector. The next highest was the healthcare sector, with 10 breaches.

Why is CPS important?

CPS 234 is a direct response to the changing threat landscape and the increased rise of incidents across an array of technologies used by financial services organisations. Over recent years, the sector has been far more susceptible to payments and card fraud, attacks on critical infrastructure and financial data, mobile OS/app vulnerabilities, and supply chain attacks to name just a few.

Yet, the cyber security posture of financial services organisations needs considered balancing. To drive better outcomes, such as increased revenue, advocacy and operational efficiency, it needs to provide better experiences to both employees and customers through innovative technology. But to do so, means opening up more applications and workloads to potential risk in order to achieve this.

Similarly, major stakeholders, including the executive team, board, shareholders, customers and regulators have great expectations for the watertight protection of the organisation's information assets. Getting the right balance is somewhat of a juggling act.

[1] Taken from data between April and June 2019

[2] Taken from data between April and June 2019

[3] 2017 Ponemon Cost of Data Breach study

How Rapid7 helps you become CPS 234 compliant

Overview

To help you understand your obligations more deeply, we have published this detailed guide of the CPS 234 regulation and how our solutions can help. It details individual components of the regulation, and how you can meet those obligations across an array of products you may or may not currently have.

The headline obligations of CPS 234 include:

1. **Roles and responsibilities:** Set out your information security related roles and responsibilities.
2. **Information security capability:** Includes the totality of your resources, skills and controls.
3. **Policy framework:** Must be proportionate to your exposure to threats.
4. **Information asset identification and classification:** With reference to their criticality and sensitivity.
5. **Implementation of controls:** Contemplate an asset's vulnerabilities and threats, criticality and sensitivity, and life-cycle stage, as well as the potential consequences of a cybersecurity incident.
6. **Incident management:** Mechanisms in place to detect and respond to threats in a timely manner, as well as specific response plans.
7. **Testing control effectiveness:** Carry out appropriate testing of the security controls protecting your data.
8. **Internal audit:** Review the effectiveness and the design of all information security controls.
9. **APRA notification:** Must be notified no later than 72 hours after you become aware of an information security incident.

Rapid7 Solutions for CPS 234 Compliance

This section details the CPS 234 security requirements and how Rapid7 products and services help organisations become and remain compliant.

Information security requirements for all APRA-regulated entities	InsightVM	InsightIDR	InsightOps	InsightAppSec	Managed Detection and Response	Managed Vulnerability Management	Managed Application Security	Proserve & Partner	InsightConnect
Roles and responsibilities	Y	Y	Y	Y	Y	Y	Y	Y	
Information security capability	Y	Y	Y	Y	Y	Y	Y	Y	
Policy framework	Y	Y	Y	Y	Y	Y	Y	Y	
Information asset identification and classification	Y								
Implementation of controls	Y	Y	Y	Y	Y	Y			Y
Incident management	Y	Y	Y	Y				Y	Y
Testing control effectiveness						Y	Y	Y	
Internal audit								Y	
APRA notification		Y	Y	Y					

Roles and responsibilities:

Set out the information security related roles and responsibilities

13	**The Board[1] of an APRA-regulated entity (Board) is ultimately responsible for the information security of the entity. The Board must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.[2]** **[1] For an RSE licensee, a reference to the Board is to be read as a reference to the Board of directors or group of individual trustees of an RSE licensee, as applicable. 'Group of individual trustees' has the meaning given in subsection 10(1) of the SIS Act.** **[2] A reference to the Board in the case of a foreign ADI, is a reference to the senior officer outside Australia.**
How Rapid7 helps	Our **Insight cloud platform** gives you the visibility, analytics, and automation to unite your teams, work faster and smarter. Our solutions give security, IT, and DevOps teams one-click access to: • network visibility • asset and application vulnerability management • breach detection and threat hunting • centralised log management • penetration testing • phishing simulation **Vulnerability management solutions** These include industry-leading vulnerability management, web application security testing and attack simulation products. They provide comprehensive, yet prioritised, visibility into potential cyber risks across your IT environment. Remediation Projects are also available to ensure these risks are easily mitigated. **Incident detection and response solutions** We help you rapidly detect and respond to cyber security incidents and breaches across on-prem and remote assets. No matter if they are physical, virtual or cloud assets, including those associated with the behaviors of their users. **IT analytics and automation solutions** These quickly allow you to gain visibility into your IT environment and facilitate automated workflows to eliminate repetitive, manual and labor-intensive tasks. All of the above combine to collect massive amounts of data. And, when combined with our core analytics and machine-learning-driven user behavioral analytics, simplify the task of identifying and responding to potential breaches.
14	**An APRA-regulated entity must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions.[3]** **[3] For the purposes of this Prudential Standard, governing bodies and individuals includes committees, working groups and forums.**
How Rapid7 helps	Our partners can assist you in the establishment and documentation of internal processes and procedures, enabling you to understand and deliver against this component.

Information security capability:

Includes the totality of your resources, skills and controls

15	**An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.**
How Rapid7 helps	The process of managing risks associated with the use of information technology involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets. Ultimately, treat risks in accordance with your organisation's overall risk tolerance. Our **Insight cloud platform** helps you understand what risk is present within your estate; as well as how your own people and potential threat actors may create and / or leverage any exposure available to them. • **InsightVM** is a vulnerability risk solution that helps you to find and fix vulnerabilities, misconfigurations, and exposures from the endpoint to the cloud. • **InsightIDR** is a cloud SIEM powered by user behavior analytics. It contains both pre-built compliance dashboards and detections across the entire attack chain. • **InsightAppsec** is an application security solution that dynamically assesses web, mobile, and cloud applications for vulnerabilities across all modern technologies. From a continuous operation of the function, both our partners and Rapid7's **Managed Detection & Response** Services can help you move forward.
16	**Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.**[1] **[1] For the avoidance of doubt, paragraph 16 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under Prudential Standard CPS 231 Outsourcing or Prudential Standard SPS 231 Outsourcing.**
	N/A

17	**An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.**
How Rapid7 helps	**FROM THE RISK PERSPECTIVE :** **InsightVM** not only provides visibility into your environment's vulnerabilities—including local, remote, cloud, containerized, and virtual infrastructure—but also, clarity into how those vulnerabilities translate into business risk, and which attackers are most likely to target. **Attack Surface Monitoring with Project Sonar** identifies rogue external assets on your attack surface. Then, our threat feeds tap into **Project Heisenberg**'s network of honeypots and findings from our Detection and Response team's active threat hunting, helping you understand what threat actors are actively doing in the wild. Live Dashboards in **InsightVM** update as soon as there's new data; letting you track your attack surface and risk as it changes. The views are also customisable for different technical teams or stakeholders. **FROM THE THREAT PERSPECTIVE:** We investigate a constant stream of attacker behavior. As part of the investigative process, our analysts directly contribute Attacker Behavior Analytics (ABA) detections into **InsightIDR**, paired with recommendations and adversary context. These detections leverage the real-time user and endpoint data collected by InsightIDR. As a result, every alert in **InsightIDR** automatically surfaces important user and asset behavior; along with context around any malicious behavior. This means you can easily pivot from a visual timeline to log search, on-demand endpoint interrogation, or user profiles to scope the incident and take informed action.

Policy framework:

Must be proportionate to their exposure to threats

18	**An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.**
How Rapid7 helps	Many policy frameworks exist today. Our **Insight cloud platform** provides you with the assurance you have implemented and importantly, are maintaining standards against your chosen framework. **InsightVM** audits against a number of common frameworks such as: • Center for Internet Security (CIS) benchmarks • Payment Card Industry Data Security Standard (PCI-DSS) • United States Government Configuration Baseline (USGCB) policies • Federal Desktop Core Configuration (FDCC). You can test assets for compliance with customised policies derived from these standards. Our Managed Services provides you with an expert team to run this function on your behalf.

19	**An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.[1]** **[1] For the purpose of paragraph 19 of this Prudential Standard, parties include governing bodies and individuals with responsibilities referred to in paragraph 14, as well as all other staff, contractors, consultants, related parties, third parties and customers.**
How Rapid7 helps	Our partners can help your team document roles, responsibilities and procedures concerning your information assets. This information is extremely helpful in any incident or crisis. As we move into the technology layer, our **Insight cloud platform** provides numerous functions to assist with this requirement. For example, with **InsightVM**, vulnerability management can be expanded to express assets to business processes and functions, including the asset owners. User Behaviour Analytics in **InsightIDR** track users and the assets they leverage to perform their roles. This observes malicious actions taking place within your environment, assisting you in establishing who to contact, as well as next steps to take. If you can authenticate the person, or service, we can help you understand the actions taking place.

Information asset identification and classification:

With reference to their criticality and sensitivity

20	**An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or non financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.**
How Rapid7 helps	The ability to identify assets across your environment is a critical capability in an asset classification process. You can't classify what you don't know. Our **InsightVM** solution provides expert identification and fingerprinting technology. It accelerates your identification, and subsequent classification process. The bi-directional integration with ServiceNow CMDB also enables you to augment some of your existing classification systems and processes. Using the assigned classification, **InsightVM** contextualises our **Real Risk** Scoring based on the asset criticality rating. This enables you to focus your remediation efforts on the assets posing the greatest risk to your organisation. We calculate risk scores for every asset and vulnerability discovered. The scores indicate the potential danger the vulnerability poses to network and business security, based on impact and likelihood of exploitation. Vulnerability impact is a measure of what can be compromised on an asset when attacking it through the vulnerability, and the degree of that compromise. Impact is comprised of several factors including: • Confidentiality impact indicates the disclosure of data to unauthorized individuals or systems. • Integrity impact indicates unauthorised data modification. • Availability impact indicates loss of access to an assets data. • Access vector indicates how close an attacker needs to be to an asset in order to exploit the vulnerability. If the attacker must have local access, the risk level is low. Lesser required proximity maps to higher risk.

User case

You have a server with sensitive financial data and a number of workstations in your back office located in Adelaide, South Australia.

The back office department recently added three new staff members. Their workstations have just come online and will require a number of security patches immediately.

You want to assign the security-related maintenance of these accounting assets to different IT administrators: A SQL and Linux expert is responsible for the server; a Windows administrator handles the workstations. You want to make these administrators aware these assets have high priority.

These assets are of significant importance to your organisation. If they were attacked, your business operations could be disrupted or even halted. The loss or corruption of their data could be catastrophic.

Using a function called **RealContext**, you can apply tags to these assets to do exactly that. You can tag all back office assets with an Adelaide location and a 'Very High' criticality level. You can tag your accounting servers with a label, e.g. 'Policy Holder', mapping your assets against the potential impact of data that may be compromised from that location. You can then assign it an owner named Chris, a Linux administrator with SQL expertise.

You can assign your Windows workstations to Brett, the Windows administrator owner; tagging the new workstations with the label 'First-quarter hires'. Then, you can create dynamic asset groups based on these tags, sending reports on the tagged assets to Chris and Brett. They now understand the workstation assets should be prioritised for remediation.

Furthermore, our **Risk Score Adjustment** allows you to customise your assets' risk score calculations according to the business context of the asset. For example, if you have set the 'Very High' criticality level for assets belonging to your organization's senior executives, you can configure the risk score adjustment so that those assets will have higher risk scores than they would have otherwise.

Information asset identification and classification:

With reference to their criticality and sensitivity

21	**An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with:** **a. vulnerabilities and threats to the information assets;** **b. the criticality and sensitivity of the information assets;** **c. the stage at which the information assets are within their life-cycle;[1]** **d. the potential consequences of an information security incident** **[1] The use of the term 'life-cycle' in this context refers to the process from planning and design through to decommissioning and disposal of an information asset**
How Rapid7 helps (a)	We provide a fully available, scalable, and efficient way to collect your vulnerability, user and asset threat data. We turn it into answers, minimising your risk. Our **Insight cloud platform** provides analytics and technology to discover vulnerabilities, threats to people and assets and in real-time. It pinpoints their location, prioritises them for your business, all while facilitating collaboration with other teams. Finally, it provides the integrations required to confirm your exposure has been reduced in an automated way; thus delivering greater operation efficiencies, when you need it, and with minimal time required.
How Rapid7 helps (b)	We calculate risk scores for every asset and vulnerability discovered. The scores indicate the potential danger the vulnerability poses to network and business security, based on impact and likelihood of exploitation. Vulnerability impact is a measure of what can be compromised on an asset when attacking it through the vulnerability, and the degree of that compromise. Our **Real Risk** Score setting allows you to customise your assets' risk score calculations according to the business context of the asset. For example, setting the 'Very High' criticality level for assets belonging to your organisation's senior executives, means you can configure the risk score adjustment so those assets have higher risk scores than they would have otherwise. You can specify modifiers for your user-applied criticality levels that will affect the asset risk score calculations for assets with those levels set. Using asset criticality within **InsightIDR** enables you to mark 'Restricted Assets'. This increased scrutiny will be applied against interactions with the restricted assets. Should an alert or incident occur within your environment, you can use the Orchestration and Automation function to accelerate your investigations and quarantine actions.
How Rapid7 helps (c)	Our **InsightVM** solution provides operating 'End of life' tracking for major operating systems such as Microsoft Windows

22	**Where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party's information security controls that protects the information assets of the APRA-regulated entity.**[2] **[1] The use of the term 'life-cycle' in this context refers to the process from planning and design through to decommissioning and disposal of an information asset.** **[2] For the avoidance of doubt, paragraph 22 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under Prudential Standard CPS 231 Outsourcing or Prudential Standard SPS 231 Outsourcing**
How Rapid7 helps	A *Cybersecurity Maturity Assessment* performed by Rapid7 or one of our partners focuses on specific controls that protect critical assets, infrastructure, applications, and data by assessing your organisation's defensive posture. The assessment also emphasises operational best practices for each control area, as well as the organisational effectiveness and maturity of internal policies and procedures. You can leverage such a service, or the output of it to assess the effectiveness and preparedness of third party services providers.
How Rapid7 helps [1]	Development and maintenance of Information Security Policies, is an integral part of any Information Security Program. Security policies set the standard for the implementation of all controls associated with managing the risk associated with an organisation's Information Security Plan. Our policy development services help you rapidly create and deploy comprehensive security policies, standards, and guidelines. We offer a full range of information security policies that better align with business objectives, best practices, and address the risk and compliance requirements of your organisation's chosen security framework. A sample of policies includes: • Configuration and Maintenance Policies • Data Protection Policies and Procedures • Data Classification Guide and Policy • Personnel Policies and Procedures • Audit Policy These and many more can be delivered either by our partners or Rapid7.
How Rapid7 helps [2]	Rows 25 & 27

Incident management:

Mechanisms in place to detect and respond to threats in a timely manner, as well as specific response plans

23	**An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.**
How Rapid7 helps	Incident investigations aren't easy. Especially when you're faced with a huge volume of alerts with log data and spreadsheets. Every alert in **InsightIDR** automatically surfaces important user and asset behavior, along with context around any malicious behavior. Easily manoeuvre from a visual timeline to log search, on-demand endpoint interrogation, or user profiles, to scope the incident and take informed action. Within **InsightIDR**, trigger workflows to automatically create service tickets to share context around investigations you're performing in **InsightIDR**. From the moment an alert is verified, set an entire workflow into motion to quickly enrich, triage, investigate, and even respond to an alert. With easy shifts to log search and endpoint interrogation from within InsightIDR, you can detect and respond to threats, without having to jump from tool to tool. By connecting the tools your teams already use, ensure everyone is working from the same data set regarding any incident or threat that arises. **InsightIDR** comes with a full *Investigations API*, giving you the flexibility to feed and manage alerts through your existing case management investments. Once your security ecosystem is automated to deliver alerts, investigation findings, and other data to the right team members, you can accelerate your mean time to response, maximising the strengths of your team. By using **InsightVM** and **InsightAppSec**, you can use the supplied vulnerability data as part of an investigation to establish potential root cause, for remediation.
24	**An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).**
How Rapid7 helps	Both our partners and Rapid7 can evaluate your environment from technology to assets to people, processes, and policy. This rates your capabilities and preparedness, while offering relevant, business-based recommendations to help you meet your Incident Response (IR) program goals. Starting from scratch? We, or our partners can help with that too. Our **IR Program Development** offering can be customised to build or improve your capability in any area of the Security Program Lifecycle. From a risk perspective, **InsightVM** and **InsightAppsec** provides visibility into the vulnerabilities in your modern IT environment—including local, remote, cloud, containerized, and virtual infrastructure. It also gives you clarity into how those vulnerabilities translate into business risk, and which attackers are most likely to target. Live Dashboards in **InsightVM** update as soon as there's new data, letting you track your attack surface and risk as it changes. The views can also be customised for different technical teams or stakeholders. As such, you can be confident in keeping your infrastructure secure as it expands into the cloud and beyond.

25	**An APRA-regulated entity's information security response plans must include the mechanisms in place for:** **a. managing all relevant stages of an incident, from detection to post-incident review; and** **b. escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate.**
How Rapid7 helps	Rows 33 & 34
How Rapid7 helps (a)	Standing up an effective detection and response program isn't as simple as buying and implementing the latest security products. It requires a dedicated Security Operations Centre (SOC), staffed with highly skilled and specialised security experts; as well as 24/7 vigilance using the best technology to ensure stealthy attackers have nowhere to hide. This needs to be combined with a defined Incident Response playbook, with defined roles and responsibilities. Our **Managed Detection and Response (MDR)** helps security teams of all sizes and experiences strengthen their security posture, find attackers, and keep ahead of emerging threats. Our **MDR** service uses a combination of security expertise and technology to detect dynamic threats quickly across your entire ecosystem. It provides the hands-on, 24/7/365 monitoring, threat hunting, response support, and security guidance you need, stopping nefarious activity and accelerates your security maturity. Along with your dedicated *Security Advisor*, our team handles the configuration, scanning, and reporting for you. This ensures you don't have to spend extra time getting trained or offloading other important initiatives. They act as an extension of your team, and your top priorities are theirs. All that's left for your team is to take care of is the execution of remediation. If you have the people in-house for example, we know incident investigations aren't easy when you're facing huge volumes of alerts with log data and spreadsheets. Every alert in **InsightIDR** automatically surfaces important user and asset behavior, along with context around any malicious behavior. Easily manoeuvre from a visual timeline to log search, on-demand endpoint interrogation, or user profiles to scope the incident and take informed action. And, with **InsightConnect** you will accelerate and streamline time-intensive processes—no code necessary. With over 280 plugins to connect your tools, and customisable workflow building blocks, you'll be free to tackle other challenges, while still leveraging their expertise when it's most critical. The **MDR** service also includes Incident *Response Escalations*, providing you with skilled resources to help you through major incidents. At the conclusion of the Incident Response, we provide you with a *Remote Incident Response Report*. This gives you an overview of the Incident and a retrospective to include an executive summary, findings details, analysis, root cause, and recommendation.
How Rapid7 helps (b)	For any type of alert created or managed by **InsightIDR**, you can automatically create a corresponding ticket or case in tools like Atlassian Jira and ServiceNow. Paired with our native case management features, this ensures that for any alert, the right team members are notified and empowered to take action. **InsightIDR** built-in dashboarding functions, powered by the **InsightIDR** Log Query Language, mean that data visualisations and reports are easy to generate and export. Security operations overview Dashboards provide executive level snapshots of the health of your **InsightIDR** security operations. **InsightVM** includes executive reporting, providing a high-level snapshot into the status of vulnerability related risks within the organisation. The information contained within vulnerability management reports are beneficial in escalations or reporting. Demonstration of the function *Vulnerability Management* program may also be desirable

26	**An APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.**
How Rapid7 helps	Many incident response engagements result in struggle, as security teams have never previously executed their proposed plans. We will walk you through real incident scenarios, identify evidence sources, perform mock communications, and make recommendations for cleanup and recovery. In the event of a true incident, all hands are on deck. We tabletop exercises by going beyond just technical analysis and response, to extend to how business owners react, communicate, and manage the event. To ensure you are armed with a well-rounded approach to incident response, we also involve stakeholders across your organisation, including but not limited to: • *Technical teams:* Assess how well your technical teams identify, respond to and contain potential incidents. • *Legal representation:* Through our understanding of regulatory and fiduciary responsibilities, we provide guidance and legal disclosure to the necessary parties. • *Marketing teams:* Brand equity is paramount. We will analyze crisis communication content, cadence, and approach. Additionally, we provide guidance for crisis communications, including internal communications, social media messaging, and public/investor disclosures. • *Executive teams:* A security event is a business event; review your organisation's relationship with the executive team, and how underlying support structures identify and communicate critical information to the business owner. In the event you have already deployed **InsightIDR**, the testing of these response plans provides you with the required visibility to further tune your platform, increasing your detection and response maturity.

Testing control effectiveness:

Carry out appropriate testing of the security controls protecting your data

27	**An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with:** **a. the rate at which the vulnerabilities and threats change;** **b. the criticality and sensitivity of the information asset;** **c. the consequences of an information security incident;** **d. the risks associated with exposure to environments where the APRAregulated entity is unable to enforce its information security policies;[1] and** **e. the materiality and frequency of change to information assets.** **[1] Also referred to as an 'untrusted' environment.**
How Rapid7 helps (a)	We believe security is the responsibility of all technology users, manufacturers, and intermediaries. Collaboration is the only way to achieve long-term change. That's why we're committed to openly sharing security information, helping our peers to learn, grow, and develop new capabilities. As well as supporting each other in raising and addressing issues affecting the cybersecurity community. We help your team meet this requirement in several ways, for example: • Threat feeds informed by *Project Heisenberg* honeypots in **InsightVM** • *Attacker Based Analytics* sourced from Projects Sonar and Heisenberg and threat intelligence in **InsightIDR** • Accelerated discovery and coverage of zero-days and other low-notice exploits in **InsightVM** and **Metasploit**. • Discovery of internet-facing assets in **InsightVM** using integration with *Project Sonar* • Identification of weak or distrusted certs using research on SSL certificate ecosystem

How Rapid7 helps (b)	We calculate risk scores for every asset and vulnerability discovered. The scores indicate the potential danger the vulnerability poses to network and business security, based on impact and likelihood of exploitation. Vulnerability impact is a measure of what can be compromised on an asset when attacking it through the vulnerability, and the degree of that compromise. Our **Real Risk** Score setting allows you to customise your assets' risk score calculations according to the business context of the asset. For example, setting the 'Very High' criticality level for assets belonging to your organisation's senior executives, means you can configure the risk score adjustment so those assets have higher risk scores than they would have otherwise. You can specify modifiers for your user-applied criticality levels that will affect the asset risk score calculations for assets with those levels set.
How Rapid7 helps (c)	The **Insight cloud platform**'s *RealContext* function helps assess this situation in a more human way. Imagine you are close to a data and asset classification model, and have applied tags to assets, including their location, the asset owners, the business processes they support. With this information available, when **InsightIDR** identifies a potential compromise, all the contextual information is at hand to communicate a timeline of events and actions. For greater fidelity, adjustment of our *Risk Score* function allows you to customise your assets' risk score calculations according to the business context of the asset. For example, if you have set the 'Very High Criticality' level for assets belonging to your organization's senior executives.
How Rapid7 helps (d)	
How Rapid7 helps (e)	*Asset Discovery* takes place via various functions including discovery scans and network topography mapping. Our *User Behavior Analytics (UBA)* uncovers those patterns and insights to identify evidence of intruder compromise, insider threats, and risky behavior on your network. And, since it focuses on behaviour, not static indicators of threat, UBA can find attacks that bypass threat intelligence, and alert on malicious behavior earlier in the attack. This gives security teams the time and context they need to quickly respond. The scope of detection includes attacks not using malware at all, such as phishing, compromised credentials, and lateral movement. This is critical, especially considering that in today's environments, users move seamlessly between IPs, assets, cloud services, and mobile devices. **InsightAppSec** can be integrated into the DevSecOps lifecycle to enforce compliance checking prior to build processes completing. This prevents potentially vulnerable systems being promoted into production. Likewise, **InsightVM** can be used to assess containers to prevent high risk issues being used within production, in potentially rapidly changing environments. **InsightVM** can also integrate with back of house systems such as DHCP, vSphere, Amazon Web Services, and Microsoft Azure to import assets into the vulnerability management tools to ensure visibility. Automated or manual actions can then be taken against these assets.

28	**Where an APRA-regulated entity's information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, the APRA-regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs 27(a) to 27(e) of this Prudential Standard.[2]** **[2] For the avoidance of doubt, paragraph 28 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under Prudential Standard CPS 231 Outsourcing or Prudential Standard SPS 231 Outsourcing.**
How Rapid7 helps	There are two potential options. First, asking for your third parties equivalent of a *Cybersecurity Maturity Assessment*, detailing the specific controls that protect critical assets, infrastructure, applications, and data used and generated on your behalf. Second, you may also look to a more active assessment in the form of a *Red Team Attack Simulation*. This is an exercise focused on an organisation's defense, detection, and response capabilities. We work with you to tailor the service to properly emulate the specific threats your organisation faces. Our *Red Team* operators carry out real-world adversarial behaviour and commonly used tactics, techniques, and procedures (TTPs). You can then measure your program's effectiveness and team's responsiveness in the context of an attempted breach. This allows you to pinpoint potential risks, including technical and organisational gaps in the third parties defenses. Requesting permission to perform this style of engagement with your partners is advised.
29	**An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner.**
How Rapid7 helps	If you have purchased and run our **Managed Detection and Response (MDR)** service, you are assigned a Customer Advisor (CA). This is deemed a critical role in the success of the **MDR** service, fronted by an experienced Cyber Security individual. During the course of the **MDR** service, your team will engage with their assigned CA. This resource is available to you to answer any questions about the **MDR** service, and offer security advisorship as you improve your security maturity. This advice extends to identified incidents, and associated remediation recommendations. The CA works with you to present the finding, recommendations and issues to the Board or senior management.

30	**An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists.**
How Rapid7 helps	In regards to *Penetration Testing* and *Red/Purple Teaming* engagements; to stay perpetually one step ahead of attackers—and help others do the same—our testers devote 25 percent of their time to conducting research. They contribute to the security community, publish articles, present at conferences, develop and release open source testing tools, and write popular Metasploit modules. *(Since we own Metasploit, our pen testers get unparalleled access to the most widely used penetration testing tool in the world.)* Our **Managed Vulnerability Management (Managed VM)** service takes all the power of **InsightVM**—including comprehensive asset discovery, cloud configuration, container assessment, reporting, and more—and layers on the expertise of our professionals. Our experts' tailored recommendations help you manage, execute, and optimise your vulnerability management program. Not only does this allow you to offload day-to-day operations, but also lets you allocate people, time, and resources to other areas of security. This allows you to focus more on your risk exposure and strengthen your overall security posture. Our experts' tailored recommendations help you manage, execute, and optimise your vulnerability management program. Not only does this allow you to offload day-to-day operations, but also lets you allocate people, time, and resources to other areas of security. This allows you to focus more on your risk exposure and strengthen your overall security posture. Our **Managed Application Security (Managed AppSec)** services allow you to offload your application security program – from scan management and vulnerability validation to pen testing – onto our experts, guaranteeing a consistent application assessment process. This helps you to minimise your workload, maximise your productivity, and free you up for other, more strategic tasks. Along with your dedicated *Security Advisor*, our team handles the configuration, scanning, and reporting for you. This means your team doesn't have to spend extra time getting trained or offloading other important initiatives. They act as an extension of your team, and your top priorities are theirs. Your team is simply left to take care of the execution of remediation.
31	**An APRA-regulated entity must review the sufficiency of the testing program at least annually or when there is a material change to information assets or the business environment**
How Rapid7 helps	**InsightVM** analyses your asset and vulnerability data to identify the singular actions you can take to have the largest impact on risk reduction. In short, no more thousand-page lists of individual patches to apply; just informed decisions on how you can make the most progress. We've helped organisations with one of the leading vulnerability management solutions for over a decade. We also recognise that for some teams, powerful technology alone doesn't guarantee success. Developing a true vulnerability management program requires time and resources. You have to prioritise what's most critical in the context of your business, remediate vulnerabilities, and establish sustainable processes for working within and across teams. The *Live Dashboards* in **InsightVM** update as soon as there's new data, letting you track your attack surface and risk as it changes. The views can also be customised for different technical teams or stakeholders. The aim is to understand and reduce your attack surface as quickly as possible, 24x7x365. Our Partners and our Consulting Services can assist you to run table top exercises, develop and measure security strategy, and much more.

Internal audit:

Review the effectiveness and the design of all information security controls

32	**An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance).**
How Rapid7 helps	A *Cybersecurity Maturity Assessment* performed by Rapid7 or one of our partners focuses on specific controls protecting your critical assets, infrastructure, applications, and data by assessing your organisation's defensive posture. The assessment emphasises operational best practices for each control area, as well as the organisational effectiveness and maturity of internal policies and procedures. *Internal Audit Teams* can leverage such a service, or the output of it, to assess the effectiveness and preparedness of third party services providers. In relation to our **Managed Services**; we have successfully completed a SOC 2 Type II Assessment on the operating effectiveness of security controls for the **Insight cloud platform**. The SOC 2 Type II report is a representation of Rapid7's overall security posture and controls.
33	**An APRA-regulated entity must ensure that the information security control assurance is provided by personnel appropriately skilled in providing such assurance.**
How Rapid7 helps	In relation to our **Managed Services**; our SOC 2 Type II Assessment has been performed by an accredited testing authority.
34	**An APRA-regulated entity's internal audit function must assess the information security control assurance provided by a related party or third party where:** **a. an information security incident affecting the information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; and** **b. internal audit intends to rely on the information security control assurance provided by the related party or third party.[1]** **[1] For the avoidance of doubt, paragraph 34 of this Prudential Standard applies to all information assets managed by related parties and third parties, not only those captured under agreements with service**
How Rapid7 helps	We have successfully completed a SOC 2 Type II Assessment on the operating effectiveness of security controls for the Insight cloud platform. The SOC 2 Type II report is a representation of Rapid7's overall security posture and controls. Our Legal team would be happy to provide a copy of this report with the corresponding Non-Disclosure Agreements in place.

APRA notification:

Must be notified no later than 72 hours after an entity becomes aware of an information security incident

35	**An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that:** **a. materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or** **b. has been notified to other regulators, either in Australia or other jurisdictions.[1]** **[1] For the avoidance of doubt, paragraph 35 of this Prudential Standard applies to notifications of information security incidents not already captured as notifications under Prudential Standard CPS 231 Outsourcing, Prudential Standard SPS 231 Outsourcing, Prudential Standard CPS 232 Business Continuity Management or Prudential Standard SPS 232 Business Continuity Management. Other regulators include domestic government agencies and international regulators.**
How Rapid7 helps	If you're like the 62 percent of organisations that report getting more alerts than they can investigate, you're likely all too familiar with piecing together user activity, gathering endpoint data, and validating known good behavior just to uncover yet another false positive. **InsightIDR** unites log search, user behavior, and endpoint data in a single timeline to help you make smarter, faster decisions. Customers report accelerating their investigations by as much as 20 times quicker than previous efforts. Threats can be used to track indicators of compromise, and with **InsightIDR**, you can create your own threats, use Rapid7 threats, or other community threats to add to your defenses. When **InsightIDR** detects an IoC tracked within a threat, an alert is automatically triggered. **InsightIDR** correlates the millions of daily events in your environment directly to the users and assets behind them. This highlights risk across your organisation and prioritises where to search. Attackers rarely pick one spot. **InsightIDR's** advanced search enables security analysts to pivot from validating an incident, to quickly determining its scope, so they are poised to contain it quickly. You can be confident **InsightIDR** reduces the amount of time it takes to investigate and scope the impact of the breach; and to identify a complete containment strategy. With all your data correlated by user, asset, and activity, it's easy to expand, pivot, and focus investigations to make communication internally and externally to regulators clear and consistent. If you have an **MDR** service, any detected incidents will be notified to you, with critical incidents communicated through your assigned Customer Advisor. You receive a findings report which provides written analysis ("attack storyboard"), criticality, raw details, remediation and mitigation recommendations, and suggested containment actions at the conclusion of each validated incident investigation. We notify you of any malicious activity ("incident") discovered. This will assist with defining the potential scope of the issue to be reported. Should an incident escalation be required, our incident responders can assist.

36	**An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.**
How Rapid7 helps	**InsightIDR** reduces the amount of time it takes to investigate and scope the impact of the breach, and to identify a complete containment strategy. With all your data correlated by user, asset, and activity, it's easy to expand, pivot, and focus investigations to make communication internally and externally to regulators clear and consistent. **InsightVM** not only provides visibility into the vulnerabilities in your modern IT environment—including local, remote, cloud, containerized, and virtual infrastructure—but also clarity into how those vulnerabilities translate into business risk. And, which are most likely to be targeted by attackers. In addressing this requirement **InsightVM** analyses your asset and vulnerability data to identify the singular actions you can take to have the largest impact on risk reduction. In other words, no more thousand-page lists of individual patches to apply—just informed decisions on how you can make the most progress. Our **Managed Vulnerability Management (Managed VM)** service takes all the power of **InsightVM**—including comprehensive asset discovery, cloud configuration, container assessment, reporting, and more—and layers on the expertise of our professionals. Our experts' tailored recommendations help you manage, execute, and optimise your vulnerability management program. Not only does this allow you to offload day-to-day operations, but lets you allocate people, time, and resources to other areas of security. This ensures you can focus on your risk exposure and strengthen your overall security posture. Along with your dedicated *Security Advisor*, our team handle the reporting for you so that you don't have to spend extra time offloading other important initiatives. They act as an extension of your team, and your top priorities are theirs. All that's left is for your team to take care of the execution of remediation. **InsightConnect** can help automate this too.

Rapid7 Solutions Glossary

Rapid7 InsightVM is a vulnerability risk management solution that helps organizations to find and fix vulnerabilities, misconfigurations, and exposures from the endpoint to the cloud.

Outcomes

- *Gain Clarity Into Risk:* Better understand the risk in your modern environment so you can work in lockstep with technical teams.
- *Extend Security's Influence:* Align traditionally siloed teams and drive impact with the shared view and common language of InsightVM.
- *See Shared Progress:* Take a proactive approach to security with tracking and metrics that create accountability and recognize progress.

Rapid7 InsightIDR is a SaaS SIEM powered by user behavior analytics, complete with both pre-built compliance dashboards and detections across the entire attack chain.

Outcomes

- *Unify Your Security Data:* Easy cloud-based log and event management to meet compliance. No data expertise, hardware, or ongoing maintenance required.
- *Detect Behavior Behind Breaches:* Attackers favor stolen credentials, malware, and phishing. Detect and contain these threats before things get critical.
- *Respond With Confidence:* Accelerate investigations 20x with visual timelines. Contain attacks across your users and assets from within InsightIDR.

Rapid7 InsightAppSec is an Extensive dynamic application security testing for seeing more and remediating faster

Outcomes

- *Secure the Modern Web:* Automatically assess modern web apps and APIs with fewer false positives and missed vulnerabilities.
- *Collaborate with Speed:* Fast-track fixes with rich reporting and integrations, and inform compliance and development stakeholders.
- *Scale with Ease:* Effectively manage the security assessment of your application portfolio, regardless of its size.

Rapid7 InsightOps is an IT Operations solution that automatically combines live log and asset data from across your infrastructure into one central and searchable location, so you can easily access the insight you need, when you need it.

Outcomes

- *Centralise:* Collect data from any source, in any format. Search and analyze logs using simple keywords or analytic functions to find answers.
- *Monitor:* Track metrics like CPU, memory, and disk usage. Receive real-time alerts. Review live dashboards and scheduled reports.
- *Troubleshoot:* Quickly identify and resolve errors, reliability problems, and security issues across your infrastructure and software stack. Automate and remediate issues using the RESTful API.

Managed Detection and Response Services use a combination of security expertise and technology to detect dynamic threats quickly across your entire ecosystem, providing the hands-on, 24/7/365 monitoring, threat hunting, response support, and security guidance needed to stop nefarious activity and help you accelerate your security maturity.

Outcomes

- *Detect advanced threats:* Multiple advanced detection methods including behavioral analytics and human threat hunts find evil in your environment.
- *Stop attackers in their tracks:* Instantly contain, remediate, and mitigate risks with detailed reporting and guidance tailored to your business.
- *Accelerate your security program:* Leverage a team of experts - from your security advisor to the SOC - to mature your program and strengthen your posture.

Managed Vulnerability Management (Managed VM) takes all the power of InsightVM—including comprehensive asset discovery, cloud configuration, container assessment, reporting, and more—and layers on the expertise of Rapid7 professionals. Our experts' tailored recommendations help you manage, execute, and optimize your vulnerability management program.

Outcomes

- *Reduce risk and save time:* Ideal for lean security teams, Managed VM provides superior coverage and risk reduction, freeing your team up for more priority security initiatives.
- *Implement a successful program:* Develop, tune, and optimize a holistic vulnerability management program that's tailored to your unique business and risk tolerance.
- *Accelerate progress toward your goals:* Our mission is to accelerate your vulnerability management program—no matter your current level. Consider us an extension of your team.

Managed Application Security (AppSec) allows you to offload your application security program – from scan management and vulnerability validation to pen testing – onto our experts, guaranteeing a consistent application assessment process to help you to minimize your workload, maximize your productivity, and free you up for other tasks.

InsightConnect helps you accelerate and streamline time-intensive processes—no code necessary. With 280+ plugins to connect your tools, and customizable workflow building blocks, you'll free up your team to tackle other challenges, while still leveraging their expertise when it's most critical.

Outcomes

- *Orchestrate:* Connect your teams and tools for clear communication and complete integration across your tech stack.
- *Automate:* Streamline your manual, repetitive tasks with connect-and-go workflows—no code necessary.
- *Accelerate:* Supercharge your operations with automation that creates efficiency without sacrificing control.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. To learn more about Rapid7 or get involved in our threat research, www.rapid7.com.