Saviynt

Enabling APRA CPS 234 Compliance with Saviynt Identity Cloud

Achieve continuous APRA CPS 234 compliance quickly with Saviynt's Cloud Identity Governance (IGA) and Privileged Access Management (PAM) platform.

New edition updated for 2024

Contents

Contents

On February 22, 2024, the Office of the Australian Information Commissioner reported[1] that between July 1, 2023, and December 31, 2024, organisations had sent 483 notifications under the Notifiable Data Breaches scheme, up 19%. The report attributed 30% of the breaches to human error, 67% to malicious or criminal attacks, and 3% to system faults. Minimising the likelihood and impact of such information security incidents on the confidentiality, integrity, or availability of information assets, including those managed by related parties or third parties, is a key objective of the Australian Prudential Regulation Authority's (APRA) Australian Prudential Standard CPS 234. Failure to conduct a reasonable and expeditious assessment of a breach, or failure to notify the OAIC as soon as practicable, can result in civil penalties of up to $2,220,000 for each contravention.

This white paper will detail the requirements set out in CPS 234 and how Saviynt can help organisations achieve continuous compliance quickly and easily through our best-in-class cloud identity and governance platform and access management platform — Identity Cloud.

What is the Australian Prudential Standard CPS 234?

CPS 234 sets out a series of measures that regulated entities can use to establish best practices for maintaining cyber resiliency. CPS requires APRA-regulated entities to:

- Clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies, and individuals
- Maintain an information security capability commensurate with the size and extent of threats to their information assets, and which enables the continued sound operation of the entity
- Implement controls to protect information assets commensurate with the criticality and sensitivity of those assets, and undertake systematic testing and assurance regarding the effectiveness of those controls
- Notify APRA of material information security incidents

Who must comply with CPS 234?

CPS 234 applies to all APRA-regulated entities including:

- Authorised deposit-taking institutions (ADIs), including foreign ADIs, and non-operating holding companies authorised under the Banking Act (authorised banking NOHCs)
- General insurers and other organisations authorised under the Insurance Act (authorised insurance NOHCs)

[1] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2023

- Life insurance companies, including friendly societies, eligible foreign life insurance companies (EFLICs) and non-operating holding companies registered under the Life Insurance Act (registered life NOHCs)
- Private health insurers registered under the PHIPS Act
- RSE licensees under the SIS Act in respect of their business operations

APRA industry research highlights compliance gaps

In July 2023, APRA published the first round of findings from its expansive study[2] on cyber resilience in financial services as part of its 2020–2024 Cyber Security Strategy. By 2024 more than 300 banks, insurers and superannuation trustees will have participated in an independent cyber assessment – the largest study of its kind to be conducted by APRA.

The first round of findings showed around a quarter of APRA's regulated entities (24%) were assessed in the first tranche of CPS 234 assessments and results from this first tranche of assessments highlight "several concerning gaps" across the industry.

The most common control gaps identified were:

- Incomplete identification and classification for critical and sensitive information assets;
- Limited assessment of third-party information security capability;
- Inadequate definition and execution of control testing programs;
- Incident response plans not regularly reviewed or tested;
- Limited internal audit review of information security controls; and
- Inconsistent reporting of material incidents and control weaknesses to APRA in a timely manner.

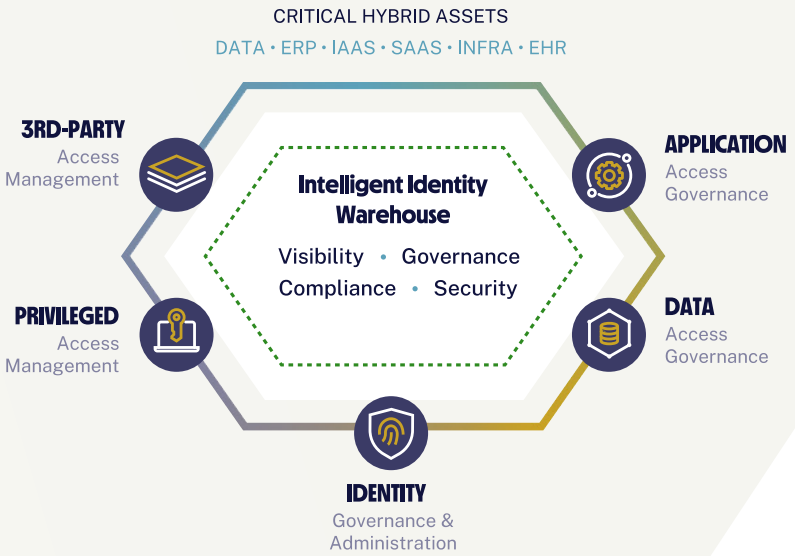
The study also highlighted the need for improved security controls to protect critical and sensitive data from unauthorised access or disclosure.

[2] https://www.apra.gov.au/news-and-publications/cyber-security-stocktake-exposes-gaps

Achieving Continuous APRA CPS 234 Compliance with Saviynt

Saviynt Identity Cloud combines multiple identity management capabilities. By providing unified controls and risk management for every identity, app, and cloud across the enterprise, the platform allows users to onboard people, apps, and machines in minutes and selectively turn on access and governance functionality.

The Identity Cloud
The leading cloud identity & governance platform built for simplicity and scale



Saviynt | Identity Cloud

CPS 234 Calls for Confidentiality

According to APRA, a key objective of Prudential Standard CPS 234 is to minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties.

In this context, confidentiality refers to “access being restricted only to those authorised”; which is the core capability of Saviynt Identity Cloud.

Generally, CPS 234 refers to information security as the preservation of an information asset’s confidentiality, integrity and availability. In addition, sensitivity means the potential impact of a loss of confidentiality or integrity.

Without proper protection and management of confidentiality, organisations cannot comply with CPS 234.

Designed for Rapid Deployment

- Configure without code and use our industry integrations, templates, and control libraries to deploy Saviynt in weeks.

Built on Zero Trust

- Automate dynamic access management and introduce just-in-time privilege elevation & time-bound access for any human or machine identity.

Continuous Compliance Ready

- Simplify audits with an assured compliance framework, reduce fraud with cross-application SoD management, & automated controls monitoring.

Trusted & Secure

- Meet evolving security & industry regulations with a SOC, ISO, and FedRAMP Moderate certified identity platform.

Saviynt Identity Governance and Administration (IGA)

As part of Saviynt Identity Cloud, Saviynt Identity Governance and Administration (IGA) increases organisational agility through automation and intuitive workflows. Saviynt IGA ensures users have seamless app and infrastructure access — without compromising compliance.

It enables APRA-regulated organisations to set risk-based access controls. Leveraging our identity warehouse, organisations can consolidate user account permission across on-premises, hybrid, and cloud-based ecosystems to create standardized role definitions and manage the complete identity lifecycle.

CPS 234 outlines the steps that APRA-regulated organisations need to take to prove governance over their data security controls. As part of the CPS 234 “defence in depth” process, organisations need to establish controls to protect from external risks as well as internal risks. Thus, to fully comply with CPS 234, regulated organisations need to ensure that they can govern and document identity lifecycle management.

This white paper will detail how Saviynt enables compliance, in part or in whole, with the following CPS 234 requirements:

- Roles and responsibilities
- Information security capability
- Policy framework
- Information asset identification and classification
- Implementation of controls
- Incident management
- Testing control effectiveness
- Internal audit
- Attachment A: Security Principles
- Attachment B: Training and Awareness
- Attachment C: Identity and Access
- Attachment H: Reporting

How Saviynt Enables Compliance

APRA's CPS 234 Prudential Practice Guide consists of more than 90 compliance recommendations across 18 sections, each covering important information security practice areas.

The significant focus areas of the recommendations are:

1. **Information security is board-level:** Organisations can no longer view information security as an "IT problem". APRA clearly states the board of an APRA-regulated entity is ultimately responsible for the information security of the entity. In practice this means organisations must have the right technology in place to inform the board of information security capability and a report on any incidents.

2. **Identity and role-based controls:** APRA is aware a siloed approach to information security roles and responsibilities can result in a lack of ownership, unclear accountabilities, ineffective oversight and fragmentation. Having a modern identity and access management solution is no longer a nice-to-have, it is imperative for regulatory compliance.

3. **Implementation of controls:** From change management to monitoring and reporting, APRA regulated organisations must have information security controls implemented at all stages of their operations. This calls for more structure with how information security policies and processes are managed within the organisation.

A more detailed correlation between the requirements and how Saviynt enables compliance is included in the following table.

Roles and Responsibilities

CPS 234 Requirement	Compliance with Saviynt
The Board 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.	Saviynt's platform enables organizations to create business-process workflows focused on risk to alleviate the "rubber-stamping" often involved in periodic access reviews and certification campaigns. Intelligent analytics compare risk-based criteria to user requests, streamlining low-risk access and escalating higher-risk requests to resource owners. Saviynt's data analysis capabilities include pattern matching and natural language processing capabilities, to classify data as PII, PCI, PHI or Intellectual Property. Saviynt's Data Access Governance (DAG) solution allows the creation of risk-based policies to manage data access and automate user requests to data.
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.	Organizations can assign ownership and succession policies over human and machine identities, including third parties, to clearly define roles and responsibilities for identity and access governance. Through Saviynt's intelligent analytics and peer analysis, managers and IT administrators involved in the access review and certification campaign process gain visibility directly into the riskiest access. Approvers can use Saviynt's intelligent analytics to apply proper scrutiny to requests and relieve them of the burden of reviewing low risk and common access requests.

Information Security Capability

CPS 234 Requirement	Compliance with Saviynt
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.	Saviynt's role-engineering capabilities help secure data and mitigate threat risks by creating a single user identity. This user identity encompasses entitlements across all accounts to standardize role definitions that limit access according to the principle of least privilege. Saviynt's solution employs both bottom-up and top-down role analysis, as well as usage-log analysis, to provide visibility into access granted but not being used, mitigating excess access risk. Saviynt analyzes structured and unstructured data in the cloud and on-premises enabling organizations to set and enforce risk-based access control policies.
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.	Saviynt enables organizations to set ownership/sponsorship over third parties, including human and machine identities. This capability ensures that the organization limits third-party access to systems, software, and networks according to the principle of least privilege, incorporates third-party access risk into the access review process, and documents its continuous monitoring.
	Our fine-grained entitlements provide organizations a way to grant the most precise access necessary for a person to execute their job, ensuring the principle of least privilege is applied across the entire ecosystem. With Saviynt Third-Party Access Governance (TPAG), organizations can set time-bound rules that automatically revoke third-party access at the end of a contract. The check-in/check-out processes for human and machine identities mitigate excess access risk and credential theft risk by applying timebound rules for access to critical data and resources. Saviynt DAG integrates traditional data classification with identity and risk intelligence, identifying sensitive data such as PII, trade secrets, or corporate financial information. The platform enables organizations to set data access policies that drill down to file-level, fine-grained entitlements by combining access and usage information, data classification rules, and risk ranking of users to define preventive and detective data access rules.

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.	Saviynt Identity Cloud integrates with enterprise SIEMs to provide holistic access visibility. Saviynt's platform continuously monitors access privileges for control violations, such as those granted as part of emergency elevation or through a backdoor. When the platform detects potential violations, it sends alerts and suggests remediation actions, such as exception documentation, setting time limits, or rejections. Saviynt also provides preventative controls for structured and unstructured data. The platform reviews a document's risk level to trigger access approvals and reviews, and can quarantine sensitive documents in real-time to prevent business or compliance violations.

Policy Framework

CPS 234 Requirement	Compliance with Saviynt
An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.	Saviynt Risk Exchange accelerates compliance program maturity with its out-of-the-box control repository and a Unified Controls Framework cross-mapped across business-critical regulations, industry standards, platforms, and control types.
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.	Saviynt Identity Cloud enables organizations to set ownership and succession policies to ensure continuity over responsible parties.

Information Asset Identification and Classification

CPS 234 Requirement	Compliance with Saviynt
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.	Saviynt DAG scans all locations where data resides, including applications, email, file systems, documents, databases, and collaborative tools, and identifies structured and unstructured data across the organization's on-premises, hybrid, or cloud-based IT ecosystems for full visibility into location, ownership, and access.

Implementation of Controls

CPS 234 Requirement	Compliance with Saviynt
An APRA-regulated entity must implement security controls and ensure that related parties and third-parties also implement controls commensurate with vulnerabilities and threats to information assets.	Saviynt Risk Exchange accelerates compliance program maturity with its out-of-the-box control repository and a Unified Controls Framework cross-mapped across business-critical regulations, industry standards, platforms, and control types. The control library enables rapid, risk-aware access policy establishment for digital transformation. The library contains more than 250 controls that are aligned with regulations, industry standards, and cloud services providers/applications for seamless access risk mitigation across on-premises, hybrid, cloud, and multi-cloud ecosystems. Organizations can also create and apply data access policies to structured and unstructured data across on-premises, hybrid, and cloud resources. The policies can drill down to file-level, fine-grained entitlements by combining access and usage information, data classification rules, and risk ranking of users to define preventive and detective data access rules. Saviynt enables organizations to set ownership/sponsorship over third parties, including human and machine identities. This capability ensures that the organization limits third-party access to systems, software, and networks according to the principle of least privilege, incorporates third-party access risk into the access review process, and documents its continuous monitoring.

An APRA-regulated entity must implement security controls and ensure related parties and third parties also implement controls commensurate with criticality of information assets.	See above
An APRA-regulated entity must implement security controls and ensure related parties and third parties also implement controls commensurate with the state at which information assets are in their lifecycle.	See above
An APRA-regulated entity must implement security controls and ensure related parties and third parties also implement controls commensurate with potential consequences of an information security incident.	See above

Incident Management

CPS 234 Requirement	Compliance with Saviynt
An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.	Saviynt's platform continuously monitors for new risks so that organizations can prove continuous control effectiveness. The Intelligent Request process uses analytics to compare risk-based criteria to user requests streamlining low-risk access and escalating higher-risk requests to resource owners. Approvers are then able to apply proper scrutiny to requests as they are relieved of the burden of reviewing low-risk and common access requests. Saviynt's platform continuously monitors access privileges for control violations, such as those granted as part of emergency elevation or through a backdoor. When the platform detects potential violations, it sends alerts and suggests remediation actions, such as exception documentation, setting time limits, or rejecting access.

An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.	Saviynt's analytics can detect high-risk activity based on various data risk scoring parameters including volume spike, ingress/egress traffic, event rarity, outlier access, policy/control violations, threat intelligence, etc. Saviynt enables enterprises to perform signature-less analysis for rapid detection, effective investigation, and closed-loop security response. Leveraging techniques such as quarantine, access lockdown, or security team alerts to address suspicious activity, Saviynt's platform automatically prevents insecure data sharing. Saviynt Identity Cloud integrates with cloud platform notification services, so as soon as a workload is created, we bootstrap SSH keys and credentials and automatically register the workload in our Privileged Access Management (PAM) solution for ready access. Saviynt de-registers workloads when they are destroyed.
An APRA-regulated entity must have mechanisms for managing all relevant stages of an incident, from detection to post-incident review.	Saviynt's continuous documentation capabilities include exception documentation, dashboard visualizations, and logs required to detect, review, and mitigate identity and access incidents.
An APRA-regulated entity must have mechanisms for 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.	Saviynt's automation escalates risky access requests and risky access entitlements to appropriate responsible parties as part of the detection process. Saviynt's Risk Exchange integrates with key monitoring solutions, including SIEM and UEBA platforms, so organizations can centralize identity risk visibility as part of the holistic risk analysis.

Testing Control Effectiveness

CPS 234 Requirement	Compliance with Saviynt
(c) the consequences of an information security incident; (d) the risks associated with exposure to environments where the APRA regulated entity is unable to enforce its information security policies; and (e) the materiality and frequency of change to information assets.	Saviynt Identity Cloud continuously monitors access privileges for control violations, such as those granted as part of emergency elevation or through a backdoor. When the platform detects potential violations, it sends alerts and suggests remediation actions, such as exception documentation, setting time limits, or rejecting access. Saviynt Identity Cloud integrates with cloud platform notification services, so as soon as a workload is created, we bootstrap SSH keys and credentials and automatically register the workload in PAM for ready access. Saviynt de-registers workloads when they are destroyed, providing the agility essential in an ephemeral environment. Our risk-aware certifications and intelligent access request automation surface risky access requiring exception documentation. Microcertifications triggered by the organization's HR system give reviewers a way to make and document their access decisions in real-time. Additionally, our platform quarantines information when users attempt to share sensitive data, requiring approval before releasing it.
An APRA-regulated entity must escalate and report to the Board or senior management any identified control deficiencies.	Saviynt's dashboards offer easy-to-read visualizations that can be used to present high-level control and risk data to the Board or senior management. Organizations can also download complete audit trail logging information such as keystroke logs for more detailed information about controls' weaknesses.
An APRA-regulated entity must review testing annually or when the organization makes a material change to information assets or business environment	Saviynt Identity Cloud enables continuous monitoring, remediation, and documentation to provide continuous assurance for a continuous testing cycle that includes all changes, regardless of materiality.

Internal Audit

CPS 234 Requirement	Compliance with Saviynt
An APRA-regulated entity's internal audit 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).	Saviynt Identity Cloud provides a single source of information for assessing risk, managing the identity lifecycle, and automating continuous assurance activities. Saviynt's Risk Exchange accelerates compliance program maturity with its out-of-the-box control repository and a Unified Controls Framework cross-mapped across business-critical regulations, industry standards, platforms, and control types Saviynt's audit documentation capabilities include keylogging, record retention, query-based real-time dashboard screenshots, actionable reports, and drop-down, easy-to-use menus that enable real-time documentation of risk-based access decisions.
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.	See above

Attachment A: Security Principles

CPS 234 Requirement	Compliance with Saviynt
An APRA-regulated entity must ensure: b) access to, and configuration of, information assets is restricted to the minimum required to achieve business objectives. This is typically referred to as the principle of 'least privilege' and aims to reduce the number of attack vectors that can be used to compromise information security;	Saviynt's role-engineering capabilities help secure data and mitigate threat risks by creating a single user identity that encompasses entitlements across all accounts to standardize role definitions that limit access according to the principle of least privilege. Saviynt's solution employs both bottom-up and top-down role analysis, as well as usage-log analysis, providing visibility into access granted but not being used, mitigating excess access risk. Saviynt DAG analyzes data repositories across on-premises and cloud-based storage locations to identify sensitive information. Saviynt mitigates data access risk by monitoring data sharing repositories and emails, quarantining sensitive information, and requiring authorization before releasing the information to the intended recipient.
c) timely detection of information security incidents. This minimises the impact of an information security compromise;	Saviynt continuously monitors access requests, surfaces high-risk requests for additional approvals, enables enforcement of the principle of least privilege, and suggests remediation activities so that organizations can document exceptions.
e) use of, and access to, information assets is attributable to an individual, hardware or software, and activity logged and monitored;	Saviynt's role-engineering capabilities enable organizations to standardize user roles across on-premises, hybrid, and cloud-based resources to prevent SOD violations and ensure continued compliance with the principle of least privilege. Our role-engineering capabilities include both top-down and bottom-up analysis so that organizations can establish a single authoritative identity source across complex ecosystems to ensure continuous compliance, logging, and monitoring.
f) error handling is designed such that errors do not allow unauthorised access to information assets or other information security compromises;	Saviynt suggests risk remediation activities when it locates a potential access control violation. Organizations can set time-bound access termination and document policy exceptions to prevent errors that can compromise data security.

	Organizations can create fine-grained controls that limit access to information based on the principle of least privilege to mitigate the risks associated with excess access that lead to unintentional unauthorized access within the organization. Organizations apply their risk tolerance as part of generating the workflows that drive Saviynt's automation. The Intelligent Access Request capability continuously monitors access requests, applying the risk-based workflows to the requests. It then automates low-risk request approvals while surfacing high-risk requests for additional review, suggesting remediation actions. With Saviynt's fine-grained access controls and data scanning capabilities, organizations can create detailed data access controls that limit access to cloud-based resources. Organizations can apply their IGA controls to data access policies so that only users who should be receiving information via email or links are allowed to view it.
i) design controls that enforce compliance with the information security policy framework, thereby reducing reliance on individuals.	Saviynt's intelligent analytics enable organizations to automate risk monitoring, reducing the reliance on manual processes and human error risk.

Attachment B: Training Awareness

CPS 234 Requirement	Compliance with Saviynt
2. An APRA-regulated entity would regularly educate users, including both internal and third party staff, as to their responsibilities regarding securing information assets. Common areas covered would typically include: c) physical protection, remote computing and usage of mobile devices; e) access controls, including standards relating to passwords and other authentication requirements;	Saviynt's user-friendly interface and self-service capabilities reinforce the organization's employee training to create a culture of security. Saviynt's Intelligent Access Request process provides end-users with a color-coded likelihood of approval. When an approval is not likely, the system then informs the user of the reason the request will likely be denied. When users understand the reason for request denial, they are less likely to request more access than necessary, thus reinforcing the organization's security training and the principle of least privilege simultaneously.

f) responsibilities with respect to any end-user developed/configured software (including spreadsheets, databases and office automation); h) handling of sensitive data.	

Attachment C: Identity and Access

CPS 234 Requirement	Compliance with Saviynt
1. Identity and access management controls would ideally ensure access to information assets is only granted where a valid business need exists, and only for as long as access is required. Access is typically granted to users, special purpose system accounts, and information assets such as services and other software.	Organizations can create fine-grained controls that limit access to information based on the principle of least privilege to mitigate the risks associated with excess access that lead to unintentional unauthorized access within the organization. Organizations can set access controls across applications, even in a hybrid ecosystem, to mitigate SOD risks that can also lead to excess access and potential privilege misuse. With Saviynt's fine-grained access controls and data scanning capabilities, organizations can create detailed data access controls that limit access to cloud-based resources. Organizations can establish fine-grained entitlements for vendors, time-bound access requirements, and continuously monitor for potentially risky access requests.
2. Factors to consider when authorising access to information assets include: business role, physical location, remote access, time and duration of access, patch and antimalware status, software, operating system, device and method of connectivity.	Saviynt enables organizations to set attribute-based access controls that incorporate multiple factors including but not limited to business role, geographic location, and timebound access termination.

3. The provision of access involves the following process stages: c) authorisation — assessment of whether access is allowed to an information asset by the requestor based on the needs of the business and the level of information security (trust) required.	Saviynt applies the organization's risk tolerance to the workflows that drive the Intelligent Access Request process, ensuring continued enforcement of the organization's principle of least privilege controls. Saviynt's peer-and usage-based analytics surface high-risk access requests, escalating them for additional review and suggesting actionable risk-mitigation activities, such as exception documentation or additional review.
4. Regulated entities would typically put in place processes to ensure that identities and credentials are issued, managed, verified, revoked and audited for authorised devices, users and software/processes.	Saviynt's role-engineering capability decreases the time it takes organizations to complete onboarding and birthright provisioning activities. Additionally, Saviynt's certification processes leverage our intelligent analytics to surface high-risk access entitlements, reducing reviewer fatigue by highlighting the riskiest access that requires additional review, such as access to sensitive data locations and potential SOD violations.
6. The following are examples where increased authentication strength is typically required, given the impact should an identity be falsified: a) administration or other privileged access to sensitive or critical information assets; b) remote access (i.e. via public networks) to sensitive or critical information assets; and c) high-risk activities (e.g. third-party fund transfers, creation of new payees).	Saviynt's peer-and usage-based analytics detect anomalous access requests which can help identify falsified accounts. Our platform provides check-in/check-out capabilities that enable organizations to manage access to sensitive and/or critical information assets. Combined with our fine-grained entitlements, Saviynt's platform continuously protects organizations from excess access risk and enforces the principle of least privilege across complex ecosystems. Saviynt mitigates third-party access risk by assigning an internal user who owns the vendor relationship. Organizations can also set succession policies to prevent compliance gaps if the original owner leaves their role. By assigning ownership and succession policies, organizations extend governance to their vendor relationships in the same way that they monitor their internal users' access. Saviynt also natively connects with UEBA, GRC, and SIEM solutions to detect anomalous behaviors.

7. A regulated entity would typically deploy the following access controls: a) undertake due diligence processes before granting access to personnel. The use of contractors and temporary staffing arrangements may elevate the risk for certain roles; b) implementation of role-based access profiles which are designed to ensure effective segregation of duties; e) timely removal of access rights whenever there is a change in role or responsibility and on cessation of employment; f) session timeouts; g) processes to notify appropriate personnel of user additions, deletions and role changes; h) audit logging and monitoring of access to information assets by all users; i) regular reviews of user access by information asset owners to ensure appropriate access is maintained.	Once organizations set their risk tolerance and use those to generate workflows that drive the automation, they ensure compliance by automating tasks such as birthright provisioning, contractor/temporary staffing arrangements, and joiner/mover/leaver access. Saviynt's platform natively connects with most-used Human Resources applications, such as Workday, to enable organizations to set HR as their authoritative identity source. Using the HR system, organizations can establish real-time access provisioning and termination to ensure compliance as users' roles change within the organization. Changes in a user's HR role trigger a microcertification, ensuring continuous governance over the identity and access lifecycle. Our certification and Intelligent Access Request capabilities automatically notify the appropriate personnel by surfacing risky access either during the request process or as part of regularly scheduled reviews. By surfacing the riskiest access, Saviynt reduces reviewer fatigue, ensuring purposeful review and reducing "rubber stamping." Saviynt enables organizations to document exceptions within the platform, which can be downloaded as part of the overarching audit package.
8. For accountability purposes, a regulated entity would typically ensure that users and information assets are uniquely identified and their actions are logged at a sufficient level of granularity to support information security monitoring processes.	Saviynt's fine-grained entitlement capabilities provide visibility into user access at a detailed level. Additionally, organizations can apply their identity governance controls to document data access monitoring for potential violations across on-premises, hybrid, and cloud-stored structured and unstructured data.

Attachment H: Reporting

CPS 234 Requirement	Compliance with Saviynt
Common Information for Boards and Management: Incidents • Incident trend analysis (internal and external) • Incident response test results (includes simulations)	Saviynt's intelligent analytics use peer-and usage-based data to detect access outliers. Additionally, organizations can run SOD simulations as part of the Intelligent Access Request process.
Pre-Compromise Events: • Applications going into production with code vulnerabilities	Saviynt's PAM continuously monitors cloud assets, such as instances and workloads, for misconfigurations that can lead to access risks. Saviynt notifies the organization of any potential risks in near real-time and either automatically terminates the process or suggests other remediation activities.
Pre-Compromise Events: • Systems protected by identity and access management systems (count) • User access review (by role, privilege, ageing, coverage %) • Information security configuration compliance (coverage %)	Saviynt's reporting and logging capabilities support both dashboard visualizations and detailed log reports documenting these activities. Saviynt's PAM detects and alerts organizations in near real-time to potential information security misconfigurations arising from workloads and instances.

Learn More

For more information about how Saviynt can enable your organisation's CPS 234 compliance, please review the following documentation available on our website:

- Saviynt's Identity Cloud
- Saviynt for Financial Services
- Saviynt PAM for Robust Cloud Security
- Future-Proofing Information Security for Investors Bank

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suit e D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com