BeyondTrust

This paper will explore CPS 234 in greater depth and discuss how BeyondTrust and its solutions can support financial services organisations.

How Privileged Access Management Supports Alignment to APRA CPS 234

TABLE OF CONTENTS

APRA is Prioritising Cyber Resilience

Introduction to CPS 234

CPS 234 Capabilities & BeyondTrust

Attachment A: Security Principles

Attachment B: Training and Awareness

Attachment C: Identity and Access

Attachment H: Reporting

The BeyondTrust Privileged Access Management Platform

APRA is Prioritising Cyber Resilience

As cyber threats increase around the world, organisations in certain industries are frequently in attackers' crosshairs. Financial services organisations are highly valued targets given the sensitive information they hold and implied value of successful attacks.

In its information paper on Supervision Priorities, dated February 2023, the Australian Prudential Regulation Authority (APRA) highlighted improving the cyber resilience of organisations that fall under its purview amongst its top priorities. A core component of this priority will be the independent reviews of financial services organisations and their compliance with CPS 234.

APRA has made clear that this heightened supervision will result in greater enforcement of security standards and breaches of conduct. This plan also includes comprehensive remediation plans and deep-dive reviews of organisation cyber weaknesses.

This paper will explore CPS 234 in greater depth and discuss how BeyondTrust and its solutions can support financial services organisations as they comply with the new requirements of the standard.

Introduction to CPS 234

The Australian Prudential Standard CPS 234 Information Security was introduced by APRA to make Australian financial services organisations more resilient against cybersecurity attacks. It first came into force on July 1, 2019 for all APRA-regulated entities.

CPS 234 is a direct response to the ever-evolving cyber security landscape financial services organisations face. As the Prudential Standard document points out, a "key objective 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."

To assist organisations in meeting the standard, APRA has published an associated guide to the standard: the Prudential Practice Guide (PPG) CPG 234 Information Security. The information contained in the PPG, APRA notes, provides guidance on best practices for cyber resilience and cyber defence. Though while educational, the guides themselves do not create enforceable requirements.

Many aspects of this guidance do align to information security best practices, referencing cornerstone cybersecurity concepts like zero trust, least privilege, and defence in-depth.

Similar to the **Essential Eight**, CPS 234 calls out the need for APRA-regulated entities to maintain "an information security capability commensurate with information security vulnerabilities and threats."

But unlike the Essential Eight – which has a number of maturity levels for organisations to align to, based on the complexity and nature of threats – CPS 234 and CPG 234 do not explicitly define what capabilities should be implemented. Instead, as CPG 234 highlights, "APRA expects that regulated entities will implement appropriate information security controls informed by contemporary sound industry practices, including in areas not explicitly addressed by this PPG."

The Prudential Practice Guide explicitly states that the controls and practices it provides are not to be considered as exhaustive checklists. Instead, they are illustrative of the types of controls that could be implemented to address the security principles referenced.

While the following pages will discuss various cybersecurity capabilities highlighted by the guide – with a distinct focus on identity and access management – APRA-regulated entities are expected to look beyond the CPS 234 standard and PPG when formulating a cybersecurity strategy. Organisations should look to implement the best practices most appropriate to combat the threats most relevant to their business.

CPS 234 Capabilities & BeyondTrust

CPS 234 calls for the implementation of a wide range of controls, spanning a variety of information security disciplines – including risk mitigation, protection, vulnerability detection, and several others.

This document will go into more detail on several of the highlighted controls in the following pages. However, it is worth recognising that in the era of supply chain attacks, the need to address service provider management controls in conjunction with access management controls is vitally important.

With the **Privileged Remote Access solution,** BeyondTrust customers can provide secure access to the vendors connecting to their critical systems, both IT and operational technology (OT), with granular controls over what third-parties can do and access. In addition, full audit trails and session forensics are collected from each access session.

Another area highlighted is end-of-life and out-of-support issues, a common source of vulnerabilities. BeyondTrust supports risk mitigation in out-of-support software by providing the ability to block the execution of particular versions of applications; or, from particular applications outright.

Within the Prudential Practice Guide are several attachments that provide additional detailed guidance on the principles highlighted in this document. Again, it is important to note that this guidance is not to be interpreted as the legal regulations by which an organisation should measure themselves. Instead, this guidance is designed to point towards best practices to be carefully considered to increase cyber resiliency.

CPG 234 contains eight attachments covering a wide array of topics, including general information security principles, employee training, identity and access management, software security, cryptographic techniques, customer security, testing, and reporting. This paper only looks at the attachments where BeyondTrust provides solutions that support the cybersecurity categories mentioned in the attachment. Readers are recommended to review the CPS 234 practice guide for a more complete understanding of the APRA guidance.

Attachment A: Security Principles

The first attachment of CPG 234 examines common information security principles, highlighting the benefits organisations stand to gain by adopting them. There are a number of principles where Privileged Access Management (PAM) can be used to meet APRA expectations. These include:

Layered Defence Measures:

An example of this expectation would be an endpoint detection and response (EDR) or other email filtering solution in place to defend against emails with links to malware (or a malware laced attachment). If this first layer of defence fails to identify the threat, BeyondTrust's Trusted Application Protection – a feature of the **Privilege Management for Windows/Mac** solution – can protect the integrity of running processes and guard against malware.

The Trusted Application Protection capability is part of the Application Control feature, which uses pre-built templates to stop attacks involving trusted apps that may be added to a whitelist, catching bad scripts and neutralising infected email attachments immediately. It can be used to protect trusted applications such as Word, PowerPoint, Excel, Adobe Reader, common web browsers, and more by controlling their child processes and DLLs.

Least Privilege:

BeyondTrust **Privilege Management for Windows/Mac** and **Privilege Management for Unix/Linux** combine least privilege management and application control to minimise the endpoint attack surface and eliminate unwanted lateral movement by removing excessive privileges from local administrator or root accounts. This can be done across Windows, Mac, Unix, Linux systems, network devices, IoT, ICS systems, and virtual machines.

Timely Detection of Incidents:

Leveraging **Identity Security Insights**, BeyondTrust's centralised threat reporting and analytics platform, IT and business leaders have visibility into the privilege-related risks facing their organisations.

Security and IT teams can quickly analyse privileged password, user, and account activity alongside asset characteristics to correlate application, service, and process data against a continuously updated malware database. BeyondTrust connects the dots and flags the events you need to focus on, allowing you to act decisively and effectively prioritise risk mitigation. Integrating BeyondTrust solutions with your existing SIEM or XDR solution can provide additional data points to identify anomalous behaviour, including unusual login attempts to privileged accounts.

Access is Logged & Monitored:

Password Safe from BeyondTrust gives security and audit teams a secure audit trail, detailed session reporting, and deep credential analytics across all privileged credentials, DevOps secrets, and accounts.

Never Trust, Always Identify:

BeyondTrust solutions allow organisations to enforce continuous authentication, grant time-limited access based on context, administer least privilege, and layer on continuous monitoring and session management.

Enforced Segregation of Duties:

Segregation of duties requires defining and delineating employee, application, and system roles and tasks, ensuring access is only granted to specific, discrete parts of systems or data as necessary.

While not an identity governance and administration (IGA) solution, BeyondTrust **Password Safe** is built to apply unique, separate credentials for every account type. BeyondTrust's Password Safe solution helps prohibit unsanctioned password and account sharing, while also enforcing unique passwords for users, applications, and other system components.

Attachment B: Training and Awareness

The guidance provided in the CPG attachment on training and awareness highlights key themes commonly found in employee security and awareness programs. This includes email and internet usage, common attack vectors such as social engineering, the handling and securing of sensitive data, and standards relating to passwords along with a host of other authentication requirements.

It is important that employees are given the tools to support the best practices endorsed during training; even the most diligent employees can make mistakes. BeyondTrust's **Password Safe** solution supports the onboarding and training experience in several ways. Long, strong passwords can be automatically rotated on an appropriate schedule, while credentials can be masked from the employee. This makes it significantly more difficult for an attacker to execute a successful phish attack. Password Safe can also be integrated with multiple MFA solutions to enable step-up authentication and increase the resiliency of authentication protocols.

Attachment C: Identity and Access

BeyondTrust can assist organisations in gaining significant coverage across the identity and access security capabilities outlined in Attachment C of CPG 234. In many cases, BeyondTrust solutions provide the exact controls described in the attachment with regard to privileged accounts and access. In other cases, BeyondTrust's capabilities work hand-in-hand with other technology choices to provide desired outcomes.

As outlined in Attachment C, capabilities include:

Enforcing Limited Access:

"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." – Attachment C, CPG 234.

Granting access to information assets only "where a valid business need exists and only for as long as is required" can be encompassed using several approaches. Firstly, BeyondTrust Password Safe enforces access to specific systems via approval workflows, which allow an organisation to control who (or what) can access information assets, from where and at what time.

Additionally, BeyondTrust Privilege Management for Windows/Mac elevates privileges to applications for standard users on Windows or Mac through fine-grained policy-based controls, providing just enough access to complete a task. Similar benefits can also be gained for Unix and Linux environments via Privilege Management for Unix/Linux.

Contextual Authorisation Protocols:

"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." – Attachment C, CPG 234.

Authorising access based on factors including physical location, remote access, time and method of connectivity can be done via BeyondTrust's Password Safe solution. Access is determined based on Role-Based Access Controls (RBAC) with Active Directory and LDAP integration. Additional considerations can also be enforced including the day, date, time and location when a user accesses resources to determine their ability to access the systems. Password Safe can also accommodate "break-glass" requests, where needed, for after-hours access in emergency situations.

Access Provisioning Controls:

"The provision of access involves the process of identification, authentication and authorisation." – Attachment C, CPG 234.

In addition to the RBAC integration previously mentioned, BeyondTrust solutions support authentication and authorisations to be sourced from Active Directory or Azure, as well as enhanced security through multi-factor authentication (MFA), smart card authentication, or SSO.

All enhanced security standards are based on allowing both the best of breed industry solutions to be used, and for customers to use their existing technology investments. This allows IGA tools to perform provisioning of access or use a single identity source (AD) for consistency.

Identity & Credential Lifecycle Management Processes:

Thanks to the interoperability between BeyondTrust **Privileged Access Management** and identity governance solutions like SailPoint, organisations can gain a comprehensive approach when managing the entire lifecycle of privileged accounts. This includes automated privileged access and centralised management of each identity's access across all standard and privileged, shared and system accounts.

In addition, BeyondTrust **Password Safe** offers advanced credential lifecycle abilities including:

a. **Automated Discovery and Onboarding:** The ability to scan, identify and profile systems and applications with auto-onboarding of privileged, shared, and service accounts.
b. **Secrets Management:** Secure and control access to secrets used in DevOps tools, workflows and CI/CD processes.
c. **Credential and Password Management:** Secure and control access to privileged credentials (privileged passwords, SSH keys, secrets) with automated password rotation.
d. **Application Password Management:** Control scripts, files, code, and embedded keys by eliminating hard-coded credentials. In addition, a REST based API is available for programmatic access.

Strong Identity & Authentication:

"Identification and authentication is commensurate with the impact should an identity be falsified." – Attachment C, CPG 234.

While BeyondTrust does not have a native multi-factor authentication offering, Password Safe and Privilege Management for Windows/Mac or Unix/Linux solutions readily integrate with the most popular MFA solutions, allowing customers to enforce step-up authentication as required.

Examples where increased authentication strength is typically required:

1. **Admin or other privileged access:** As mentioned above, such access would be typically handled by integrating Password Safe with MFA.

2. **Remote access:** Leveraging BeyondTrust's Privileged Remote Access solution allows organisations to use strict access controls for both remote employee and third-party access sessions. These can be made as granular as needed, for example allowing for a single task to be undertaken, such as updating software on a server or even restarting a specific service on that system. With Privileged Remote Access, customers can leverage either the native multifactor authentication or the MFA solution of your choice.

3. **High-risk activities:** The examples provided in CPG 234 of third-party fund transfers or the creation of new payees would typically be managed within the application or system for that activity. However, other high-risk activities, such as running scripts or Macros or installing applications can be managed via BeyondTrust's Privilege Management solutions. Step-up authentication, including challenge-response scenarios can be put in place depending on the level of risk associated with the activity. This also assists in improving the user experience while reducing the burden on the support desk by not forcing every step-up to be managed through a support ticket.

Full Coverage Access Controls:

"A regulated entity would typically deploy the following access controls"
– Attachment C, CPG 234.

Attachment C of the CPG 234 articulates an in-depth list of access controls a fully regulated organisation should be utilising to prove compliance. BeyondTrust Privileged Access Management solutions meet several of these controls outright in the following ways.

Excerpts from Attachment C include:

1. **Due Diligence Before Granting Access to Personnel:**
   a. Privileged Remote Access substantially mitigates the risks of third-party, vendor, and contractor access. In addition to masking credentials, Privileged Remote Access can narrowly define appropriate access levels down to the individual process or application.

2. **Role-based Access Profiles:**
   a. As mentioned earlier, access can be determined based on RBAC within the solutions or with Active Directory and LDAP integration.

3. **Prohibiting Sharing of Accounts & Passwords:**
   a. In an ideal world, unique accounts would exist for every system in an organisation. However, there are some systems where shared accounts may exist, including corporate social media accounts or developer test environments. In these instances, BeyondTrust access tools such as Password Safe or Privileged Remote Access provide a secure way to share access to such systems in a fully auditable controlled environment.

4. **Changing Default Passwords & Usernames:**
   a. Many IT devices — including routers, firewalls, IoT, etc. — are frequently shipped with embedded and/or default credentials that need to be managed and regularly rotated. Otherwise, these offer attackers easy backdoor access into critical systems.

      BeyondTrust Password Safe ensures credentials are regularly rotated at intervals set by your policies, which will be influenced by credential type, security importance, and other attributes. Additionally, you can enable seamless synchronisation of password changes in the directory where the account resides to reflect the changes in the system/device/application/service where the password is used, thus avoiding any downtime.

5. **Timely Removal of Access Rights:**
   a. The integration of BeyondTrust Password Safe and Active Directory allows for prompt changes to account permissions and privileges and streamlines offboarding processes for user accounts.

   b. In some instances, Privileged Remote Access customers may also choose to connect to a third party's IdP to allow the smooth onboarding and offboarding of a supplier's employees. This has the potential to expedite the revoking of access to systems following their departure from the supplier.

6. **Session Timeouts:**
   a. Timeouts can be easily configured in Password Safe and Privileged Remote Access tools to ensure stale connections are not maintained.

7. **Audit Logging & Access Monitoring:**
   a. Privileged session monitoring and management can be gained via Password Safe. A variety of capabilities are provided, including the ability to use keystroke

indexing, access and watch sessions, real-time alerting based on user activity along with integration with native tools such as Microsoft Terminal Services Client and PuTTY.

8. **Regular Reviews of User Access:**
   a. BeyondTrust Password Safe provides a streamlined process for auditors, managers and system administrators to view user access permissions and privileges to sensitive, privileged or shared accounts that are managed. Reports can be configured to show new accounts, or accounts with particular privileges that exist on systems that can be scanned and automatically onboarded for management. These reports can be distributed for review externally to the Password Safe.

9. **Multi-Factor Authentication for Privileged & Remote Access:**
   a. BeyondTrust solutions can apply multi-factor authentication at several different levels. For Privileged Access or Remote Access, contextual access rules can be used with a combination of support for best-of-breed MFA via open standards-based integrations.

   In addition to performing MFA for account/system access, BeyondTrust Privilege Management solutions can apply MFA in conjunction to application control, or privileged escalation and delegation management once user sessions have begun.

10. **Password & PIN Generation:**
    a. Password Safe can auto rotate and generate passwords on a frequency chosen by the system administrators, including after every login. This removes the need for users to create long, strong, and unique passwords that risk growing stale or being compromised.

Attachment H: Reporting

Attachment H of the CPG 234 outlines examples of information that APRA-regulated entities should collect in their reporting mechanisms, including incident reporting, testing activities, and more.

BeyondTrust provides reporting capabilities within the individual solutions, including full audit trails of who accessed what and when. In addition, BeyondTrust Identity Security Insights helps security teams visualise all identities across the organisation in a single place. This helps to uncover hidden privileges and attack vectors, detect identity-based threats, and take proactive measures.

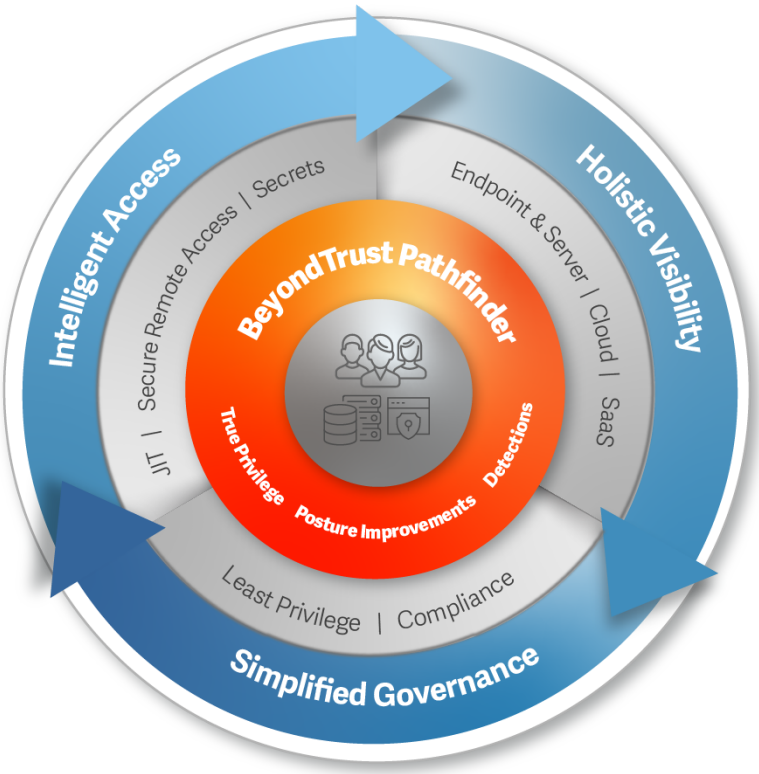
The reports support various aspects mentioned in the reporting attachment, including the measurement of internal audit activities against common controls, vulnerability, and threat assessments. More specifically, BeyondTrust can provide the needed information for a user access review, including information on user roles, privileges, aging, and coverage percentage.

The BeyondTrust Pathfinder Platform

BeyondTrust Pathfinder provides a complete Privileged Access Management platform that helps implement the secure foundation organisations need to enable remote work and digital transformation, while remaining resilient, adaptive, and protected.

Why should you partner with BeyondTrust?

- BeyondTrust is the only product vendor to address all Privileged Access Management use cases. Our comprehensive solution includes substantive capabilities no other vendor delivers.
- Our next-generation capabilities extend your line-of-sight to privileged threat pathways and identity-based attack chains, beyond what other solutions can provide.
- The breadth of our solutions and the flexibility of our offerings enable you to handle today's threat scenarios and prepare for tomorrow's possibilities.
- You can choose from the deployment model that best suits your needs – including cloud, virtual, or on-premises appliances. No other PAM vendor provides more choices.



The BeyondTrust Pathfinder platform includes:

- Password Safe
- Privileged Remote Access
- Identity Security Insights
- Privilege Management for Windows/Mac
- Privilege Management for Unix/Linux
- Active Directory Bridge
- Entitle

About BeyondTrust

BeyondTrust is the global cybersecurity leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at www.beyondtrust.com.