semperis

WHITE PAPER

APRA Cross-Industry Prudential Standard for Operational Risk Management

CPS 230 and Your Identity Infrastructure

TABLE OF Contents

semperis

Introduction

The economist and financial historian Peter L. Bernstein noted that uncertainty makes us free; venturing into the unknown means our future is not predetermined. Banking regulators don't always see things quite as philosophically. Uncertainty, when it relates to our banking and financial services sector, is not welcome.

Our global society depends on robust financial services. The sector's viability and our mechanisms for financial exchange are based on trust in both the financial instruments we use and the operational capability of the systems that support them.

In other words, we rely on the operational resilience of our critical financial sectors.

For this reason, most developed countries have comprehensive operational risk frameworks for financial services organisations. The Australian Prudential Regulation Authority (APRA) is the latest to release such a standard: the Cross-Industry Prudential Standards (CPS) 230 Operational Risk Management.[1]

1 CPS 230 Operational Risk Management | Prudential Handbook

What is the CPS 230 prudential standard?

The CPS 230 requires banks, insurers, private health insurers, and superannuation entity licencees to identify, assess, and manage their operational risks.

The standard requires effective internal controls, monitoring, and remediation. In addition, financial organisations must be able to ensure continuous delivery of their services, even during "severe disruptions." And the requirements for resilience also cover key service providers that financial organisations rely on for their operations.

The current CPS 230 standard is effective as of July 1, 2025, and—as with all CPS standards—is part of the comprehensive prudential regulation work of APRA.

Why is identity security critical in CPS 230?

The days of protecting your financial services "castle" with a moat and a wall are long gone. Attackers now circumvent firewall perimeters through phishing, exploiting vulnerabilities, or using other identity compromise techniques.

The reality of this shift was revealed in 2024, when superannuation funds across Australia were exposed to identity-based attacks. Organised attackers targeted specific high-value customers of the funds, stealing significant amounts from some customers' pensions. Meanwhile, other funds saw persistent credential stuffing—attacks that use password and username combinations stolen or captured in data breaches and then sold. This information is used to gain unauthorised access, resulting in compromise.[2,3]

Extensive digitisation and automation mean that credential vulnerability and weakness exist in every level of our organisations. Interconnected systems enable a destructive event in one area to propagate and drive catastrophe across a much broader domain.

The implications for organisational resilience are significant. As the cornerstone of operational access, your identity system enables you to manage access to the data and services that users trust and rely on.

Thus, when your aim is to build resilience at every level and into every component of business, identity is the new perimeter—the "wall and moat" that contains the keys to your castle. Effective identity and access management prevents bad actions. Protecting the availability and integrity of the identity system is vital.

2 https://www.news.com.au/national/aussie-superannuation-funds-hit-in-major-cyberattack/news-story/a39634e07fe0c8b9458d472888311abd

3 https://www.abc.net.au/news/superannuation-cyber-attack-rest-afsa/105137820

Unfortunately for financial services organisations and regulators craving resilience, most rely on identity systems such as Active Directory (AD), which has become the new battleground for defenders and attackers. Microsoft sees 600 million attacks a day against the Entra ID identity infrastructure, and they suspended nearly 64 million abusive administrative accounts in 2023.[4] Meanwhile, IBM reported in 2024 that 74% of data breaches start with privileged credential abuse.[5]

One of the highest profile attack types, ransomware, causes significant destruction while exposing sensitive personal and business data, enabling the extortion of millions of dollars—often multiple times.[6]

In addition to being responsible for a significant volume of identity-based attacks, the most prolific ransomware actors are highly sophisticated and organised. Ransomware-as-a-service groups such as RansomHub, ALPHV Blackcat, and PlayCrypt all leverage AD account discovery and AD account creation and re-enablement to establish persistence in targets, move laterally, and escalate privileges for further impacts.[7,8,9]

With the volume of change in a typical large enterprise AD, the complexities arising from hybrid on-premises and cloud identity environments, and the ageing technologies in play, we must devote focused attention to identity system security as we work to establish resilient—and compliant—enterprises.

Key areas of operational resilience in CPS 230

The CPS 230 standard covers a wide variety of risk measures. Two key control areas demand particular focus on your identity infrastructure:

- **Managing operational risk:** A regulated institution needs to control their capabilities and assets to manage and reduce risk.
- **Ensuring business continuity:** The organisation needs processes and capabilities that ensure business continuity and underlying controls to support the resilience of critical operations.

In this paper, we discuss the required controls in these areas and how they relate to and depend on your identity infrastructure. And we explore how your organisation can strengthen your capability for CPS 230 compliance by addressing identity security.

4 Microsoft Digital Defense Report 2024
5 https://www.ibm.com/reports/data-breach
6 Ransomware Risk Report - Semperis
7 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
8 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
9 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

Manage your operational risk

In his 1996 book *Against the Gods: The Remarkable Story of Risk*, Peter Bernstein described risk management as an opportunity "...to put the future in the service of the present." In financial theory, this idea points to the ability to make money by understanding and managing risks of business activities such as lending and insurance.

In operational risk-reduction, the focus is on ensuring the availability and integrity of your services.

CPS 230 Requirement

Paragraph 26

"An APRA-regulated entity must assess the impact of its business and strategic decisions on its operational risk profile and operational resilience, as part of its business and strategic planning processes."

Assessing overall operational risk

First, you must understand your assets, the business services they support, the technology and platforms that support them, and the risk that you face if those assets and systems are compromised or eliminated.

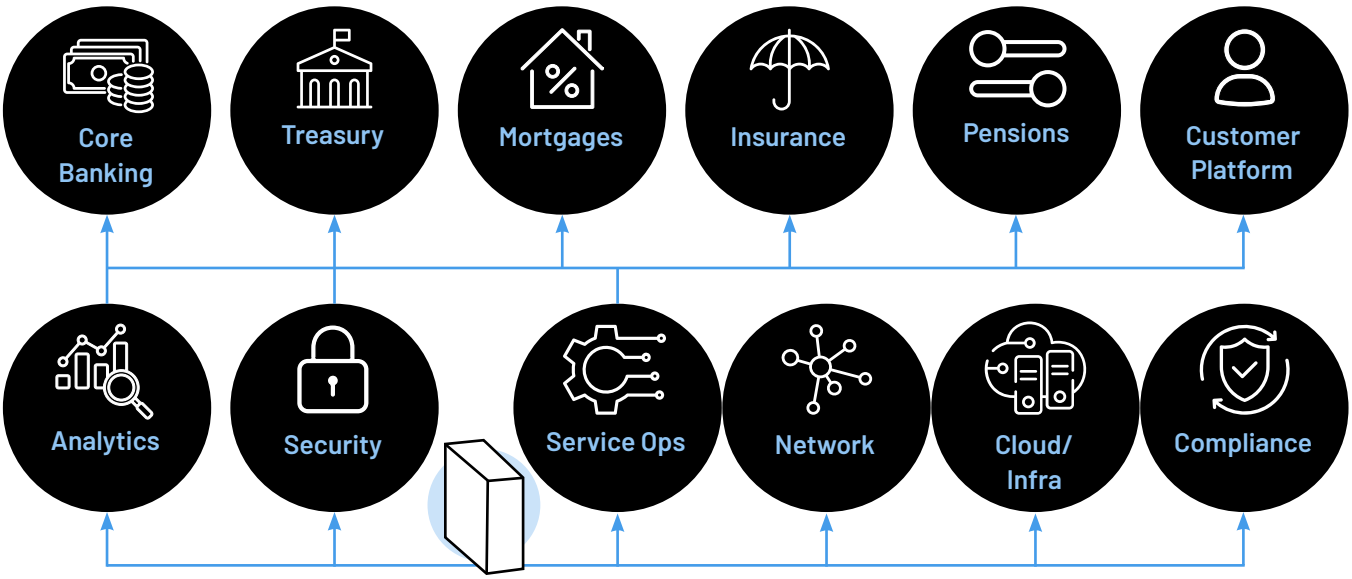
Once critical systems are defined, you must identify critical dependencies on platforms and technologies, as *Figure 1* shows.

CPS 230 Requirement

Paragraph 16b

"An APRA-regulated entity must develop and maintain an assessment of its operational risk profile, with a defined risk appetite supported by indicators, limits, and tolerance levels."

Figure 1. Defining operational risk in financial services



Your business operations depend on multiple capabilities running on underlying systems and platforms. This is where the complexity of operational risk becomes apparent.

A variety of global standards provide guiding frameworks for risk management, including:

- **COSO 2017**[10] and **ISO31000:2018,**[11] which support enterprise and operational risk management
- **ISO/IEC 27031**,[12] which concerns business continuity management
- **ISO/IEC 27001**,[13] which provides guidance on information security

Reflecting these standards, APRA requires regulated institutions to align and comply with the Prudential Practice Guide SPG 220 Risk Management.[14] Both APRA and industry standards follow a similar logic:

- Identify and understand your assets.
- Map threats and vulnerabilities to assets.
- Understand how adverse events are mitigated.
- Establish a view of the likelihood of an adverse event.
- Define and map event risk to your enterprise risk framework.
- Manage remediation.
- Monitor ongoing and emerging risk.
- Continuously improve your processes for responding to and recovering from adverse events.

Understanding identity system risk

In defining operational risk, you'll quickly discover that identity is a critical system in itself—and it's also a dependency for other critical operational capabilities throughout the business. Risk in your identity system takes two forms:

1. When identity system security is compromised, the availability, confidentiality, and integrity of your overall services are negatively affected.
2. When the identity system is hit by an outage, the outage cascades to identity-dependent services.

10 Enterprise Risk Management | COSO
11 ISO 31000:2018 - Risk management — Guidelines
12 ISO/IEC 27031:2025 - Cybersecurity — Information and communication technology readiness for business continuity
13 ISO/IEC 27001:2022 - Information security management systems
14 prudential-practice-guide-spg-220-risk-management-july-2013.pdf

Without a resilient identity system, you won't be able to deliver many of your organisation's other capabilities and thus meet your legislative requirements. This means you need awareness of risks stemming from your identity systems and the ability to:

- **Identify** any malicious states
- **Respond** to adverse events
- **Recover** to a secure state when an outage happens

Essential actions

Identity is at the core of risk management.

- Understand the role of your identity system and identity security in your organisation's overall risk posture.
- Integrate identity security objectives into your strategic roadmap.
- Define ownership of the capabilities related to the identity system.
- Understand what other critical services depend on your AD and Entra ID systems.
- Define assurance activities to ensure close monitoring and management of your identity security posture.

Ensure business continuity

The requirements of CPS 230 help financial organisations to implement relevant and comprehensive security controls that enable the organisation to be resilient in the face of increasing cyber threats.

In 2023, the APRA did a stocktake survey to identify the state of resilience in the industry. The resulting report outlined challenges in multiple controls, including user access reviews, role definitions for incident response, and third-party risk management.[15]

CPS 230 Requirement

Paragraph 16c

"... an APRA-regulated entity must develop and maintain ... internal controls that are designed and operating effectively for the management of operational risks."

With those results in mind, the CPS 230 standard requires regulated entities to manage a set of controls that help prevent disruption of critical financial services. These controls should align with industry standards and cover both operational resilience and security.

Because operational systems rely on user and service accounts managed by the identity system, identity plays an important role in the overall resilience of the organisation. Thus, when building a business continuity plan, a strong focus on your identity infrastructure is advised.

15 Cyber security stocktake exposes gaps | APRA

Let's examine four essential areas for identity system resilience: vulnerability management, monitoring and detection, incident response, and recovery.

Vulnerability and exposure management

Misconfigurations and vulnerabilities can quickly undermine the cyber resilience of your identity system. Yet vulnerability management is one of the biggest challenges facing cybersecurity teams—not least because of the sheer volume of threats.

In 2024 NCC Group reported a record-breaking year for ransomware attacks, with attackers taking advantage of more than 40,000 identified vulnerabilities.[16] This was an increase of 28% over the preceding year, so organisations face an uphill battle.

CPS 230 Requirement

Paragraph 31

"An APRA-regulated entity must remediate material weaknesses in its operational risk management, including control gaps, weaknesses, and failures."

Attackers search for unpatched vulnerabilities in your internet-facing enterprise IT to get to critical enterprise assets and exploit vulnerabilities that can allow access to your operational environments. Those critical services are supported by your identity systems, so identity is most often the path threat actors take to move laterally and escalate privileges for maximum damage.

Rapid identification and mitigation of identity system vulnerabilities is essential. However, management of vulnerabilities in critical identity systems such as AD—with its layered legacy structure and complexity—can be a significant undertaking.

Essential actions

Establish a robust programme of identity and access management (IAM).

- Implement a least-privilege access model.
- Implement just-in-time and privileged access management principles to safeguard your most sensitive (Tier 0) assets, including AD.
- Review Entra ID Connect synchronisation rules to ensure proper segregation of access between AD and Entra ID; only the necessary principals are synchronised.
- Execute active penetration testing or red teaming and ensure the identity infrastructure is in scope.
- Invest in automation of threat monitoring, identification, and remediation for the identity system.

16 NCC Group releases Annual Cyber Threat Monitor Report 2024 | NCC Group

Monitor and detect

When healthcare provider Medibank was hacked in 2024,[17] multiple identity security failures quickly got the attention of the regulator and public.

The attacker was able to capture the privileged user credentials of a contractor—stored in a browser and the contractor was not enrolled with multifactor authentication (MFA)—enabling direct access to the enterprise environment. Sensitive personal data of 9.7 million Australians was lost, leading to a revamp of the regulatory environment for such data breaches.

CPS 230 Requirement

Paragraph 16d

"... an APRA-regulated entity must develop and maintain ... appropriate monitoring, analysis, and reporting of operational risks and escalation processes for operational incidents and events."

The breach in question could have been avoided had the organisation monitored and responded to identity-focused security alerts. Without capability and capacity to triage such alerts, troves of personal data can be lost; in the case of Medibank, a full 520 GB was stolen.

Here, too, cybersecurity teams face significant challenges. Even when you've hardened your identity security and mitigated AD vulnerabilities, you need to remember that AD is in a constant state of flux, tasked with meeting business and organisational requirements as they evolve. Inevitably, some configuration changes will introduce potential vulnerabilities that were previously remediated. Monitoring your identity system for indicators of exposure and compromise (IOEs and IOCs) is essential.

This is difficult in large enterprises, where AD systems sprawl in scale and complexity. It is not as simple as turning on logging. You need to define use cases and playbooks so teams can make sense of the many alerts they receive. In addition, the teams managing these services will invariably be under significant operational pressure to keep services running without creating blockers for users.

For these reasons, when managing complex, hybrid identity infrastructures, robust automation solutions are essential to identify IOEs and IOCs and speed corrective actions.

Essential actions

Build a path to effective identity risk detection.

- Configure and manage best-practice security measures on your identity infrastructure.
- Ensure logging is enabled and a trained team is monitoring to discover suspicious and potentially harmful events.
- Enable secured logs on your identity system.
- Consider identity-focused monitoring tools for a richer dataset and scalability through automation.

17 How Medibank allegedly ignored the warning signs in one of Australia's worst cybersecurity breaches - ABC News

Incident response

Threat actors have been advancing their capabilities at a significant pace. For defenders, this means that prevention alone is not a reliable option. You must be ready when a cyber incident occurs.

The art of containment and recovery after a breach is key to restoring critical services with minimal disruption. You need a robust crisis response plan, with defined processes for incident management.

CPS 230 Requirement

Paragraph 32

"An APRA-regulated entity must ensure that operational risk incidents and near misses are identified, escalated, recorded and addressed in a timely manner."

Within this plan, identity systems require numerous considerations. You need to know:

- **Whether** your logs are intact or have been tampered with
- **What changes** have been made by an attacker—and your own teams
- **How quickly** you can recover your identity system and restore operations

In addition to stressing response to incidents, the CPS 230 standard puts strong emphasis on *reporting* them within tight timelines, placing further demands on your team's ability to quickly identify root causes of outages and breaches.

Timeline	Section	Description
72 hours	33	An APRA-regulated entity must notify APRA as soon as possible, and not later than 72 hours, after becoming aware of an operational risk incident that it determines to be likely to have a material financial impact or a material impact on the ability of the entity to maintain its critical operations.
24 hours	42	An APRA-regulated entity must notify APRA as soon as possible, and not later than 24 hours after, if it has suffered a disruption to a critical operation outside tolerance. The notification must cover the nature of the disruption, the action taken, the likely impact on the entity's business operations and the timeframe for returning to normal operations.

Essential actions

Prepare, plan, and practice for an inevitable cyber crisis.

- Conduct a thorough security review, detailing shadow administrators, nested groups, and local administrative rights to understand your access risk profile.
- Map attack pathways leading to Tier 0 assets.
- Devise an incident response plan that includes clearly defined roles and responsibilities for each member of your team.
- Ensure the integrity of your identity system logs.
- Enable the ability to monitor changes to AD in real time.
- Establish the ability to collect forensically sound data in AD and perform a forensic investigation to determine the origin and methods of attack.
- Ensure your identity forensics capabilities are integrated and tested as part of your broader crisis response readiness.

Recovery

To achieve the required resilience of your services, you will need to make sure you can recover to a secure state in a timely manner in case of an outage or breach.

In 2020 and 2024, ASX had issues with its settlement system, causing outages for brokers. The 2020 issue pertained an incorrect order identification number causing market closures for a whole day.[18] In December 2024, an outage shut down trading on a Friday and took an entire weekend to resolve. The resulting extended investigation revealed a vulnerability that had been lurking in the systems for a decade.[19]

CPS 230 Requirement

Paragraph 34

"An APRA-regulated entity must ... maintain a credible BCP that sets out how it would maintain its critical operations within tolerance levels through disruptions, including disaster recovery planning for critical information assets."

The threat of destructive events has linked information security and operational resilience. In 2024 the NCC Group tracked 94 criminal groups leveraging destructive capabilities to hold organisations to ransom, or at best face a costly and time-consuming recovery or at worst a total rebuild from scratch of essential services.[20]

18 Nasdaq has 'full attention and resources' on ASX outage

19 ASX faces ASIC, Reserve Bank blowtorch over December settlement outage

20 NCC Group releases Annual Cyber Threat Monitor Report 2024 | NCC Group

Overcoming blocks to timely recovery

Your identity infrastructure is key for the availability of most, if not all, digitally enabled services. Without a disaster recovery plan for AD and Entra ID, you are unlikely to be able to restore your overall services from a major destructive event.

Identity infrastructure is highly complex and includes many interdependencies. Because is a core foundation of your technology-enabled services, restoring it after an incident is time consuming and high risk for complex and large organisations.

Legacy identity systems such as AD can be notoriously difficult to restore to a *known* secure state.[21] The official Microsoft guidance details the process to restore a single AD forest—requiring 28 steps covered in a 150-page document—and even a slight deviation will curtail a successful recovery.

For many organisations, recovery is further complicated because of other services (such as DHCP and DNS) running on AD, hybrid cloud and on-premises integrations, and the sheer number of changes that occur daily in a large AD forest.

Depending on backup frequency, AD backups may also be compromised. Thus, once an AD forest is recovered, it still cannot be trusted for use without extensive forensic analysis to remove persistence mechanisms that enable the attacker to retain a footprint.

A well-developed disaster recovery plan includes mechanisms for avoiding these onerous and devastating recovery delays, including:

- Frequent, immutable identity system backups
- Automated and timely AD forest recovery
- Thorough and rapid post-incident forensics

Recovery testing

For information security, APRA holds organisations to its **CPS 234 standard**.[22] In addition to robust security controls to support resilient services, the standard places emphasis on testing and providing evidence for control effectiveness.

CPS 230 Requirement

Paragraph 25

"In managing technology risks, an APRA-regulated entity must monitor the age and health of its information assets and meet the requirements for information security in Prudential Standard CPS 234 Information Security."

21 Top Manual AD Forest Recovery Pitfalls | Semperis Guides

22 CPS 234 Information Security | Prudential Handbook

Reiterating the testing requirements in CPS 234, CPS 230 section 30 requires the regulated entity to:

"... regularly monitor, review and test controls for design and operating effectiveness, the frequency of which must be commensurate with the materiality of the risks being controlled. The results of testing must be reported to senior management and any gaps or deficiencies in the control environment must be rectified in a timely manner."

Thus, you rely on a variety of controls—and the standard imposes requirements to prove that they do in fact work.

Tool Specialisation

CPS 230 requires strong controls around detection, protection, recovery, and response. When it comes to identity systems in large enterprises, these controls can be very difficult to execute effectively and efficiently.

In most organisations, teams rarely have the specialised AD skills or the capacity to manage the risk of compromise and destructive events, nor are they prepared to ensure recovery if the worst should happen.

The use of specialised toolsets designed to secure these systems will allow you and your organisation to shift focus from day-to-day security operations to a strategic focus, quickly and efficiently implementing policies and procedures to keep your identity systems secure.

Consider evaluating security solutions that are purpose built for identity security, such as those from Semperis. Semperis offers both community and paid tools that directly address the challenges of complying with CPS 230.

How can Semperis help?

Below is a table highlighting the specialised capabilities that Semperis offers to support CPS 230 and CPS 234 compliance. Semperis' products are enhanced by deep research from the identity security and AD-focused security research team.

Challenge	How Semperis can help	Solution
Risk management Knowing your assets and their risks, vulnerabilities, and possible exposures is key to achieving a truly resilient enterprise.	• Confirm the accountable officer responsible for identity security. • Map threat and vulnerability indicators in AD and Entra ID. • Provide visibility into identity security posture. • Deliver semi-automated, research-led view of software vulnerabilities and misconfigurations. • Provide ongoing risk identification and management.	• Purple Knight provides point-in-time security assessment of AD that empowers you to understand vulnerabilities and delivers remediation guidance to help you reduce risks in your identity system. • Directory Services Protector (DSP) provides continuous threat and vulnerability detection, capturing every change made in AD, helping identify malicious changes, and automatically rolling back risky changes. • DSP provides comprehensive logging and highly specialised AD and Entra ID threat analysis, enabling up-to-date and industry leading insights and enrichment of SOC visibility through SIEM integration.
Protection Establishing strong controls helps you ensure robust identity and technology resilience.	• Provide privileged access management and identity and access management for all users. • Enhance protections for identity security capabilities, including attack prevention and post-attack recovery.	• DSP enables continuous monitoring of AD and Entra ID security posture, ensuring the underlying identity systems are secure and trustworthy. • Active Directory Forest Recovery (ADFR) reduces the time for a full AD forest restore by 90% compared to manual recovery.

Challenge	How Semperis can help	Solution
Monitoring and detection Your identity infrastructure is a rich source of vulnerabilities and misconfiguration, requiring skill and dedication for meaningful detection	• Provide AD and Entra ID monitoring to detect attacks and enable accurate incident reporting. • Comprehensively control the constantly changing AD environment with its rich attack surface. • Provide visibility into AD-focused attacks and changing vulnerabilities.	• DSP provides continuous threat and vulnerability detection, capturing every change made in AD, helping identify malicious changes, and automatically rolling back risky changes. • Forest Druid (community tool) discovers attack paths to Tier 0 assets and helps identify excessive privileges that attackers can exploit.
Respond Increasingly, large enterprises are required to be able to manage and report on incidents in short time periods.	• Secure your logs for forensic analysis. • Enhance ability to detect actions of a malicious actor and rapidly report incidents and attacks impacting AD and Entra ID.	• DSP provides comprehensive logging and highly specialised AD and Entra ID threat analysis, enabling up-to-date and industry-leading insights and enrichment of SOC visibility through SIEM integration. • Identity Runtime Protection uses machine learning to perform attack pattern detection by capturing, analysing, and correlating AD user activities with Semperis' identity threat intelligence to signal malicious behaviour.
Recover You need to be able to restore your identity system capabilities rapidly, to a known clean state—and have testing that proves you can.	• Enable early detection or avoidance of a security breach of your identity system and dependent technology-enabled services. • Provide proven, clean-state restore with validated recovery objectives. • Operationalise proven crisis and incident response frameworks, enhanced with expert playbooks—from preparation to after-action review.	• ADFR can automate forest recovery, restoring AD quickly and safely without reintroducing malware. • ADFR automates the complicated recovery process and reduces AD recovery time by up to 90%. • ADFR also allows for post-breach forensics to identify persistence and recover AD to a trusted state. • Disaster Recovery for Entra Tenant (DRET) recovers Entra ID objects. • Ready1 centralises crisis response, enabling teams to develop, test, remediate, and continuously improve incident response planning.

Conclusion

If your organisation is found to have material weaknesses, the APRA can impose remediating actions, fines, or restrictions on your licence to operate. To comply with CPS 230, we recommend you implement seven major initiatives for the resilience of your AD and Entra ID services:

1. Establish governance and risk management for your identity system.
2. Enable visibility into risks and dependencies.
3. Establish comprehensive and automated exposure, threat, and vulnerability monitoring and integrate this capability with your security operations centre.
4. Reduce your identity system vulnerabilities through scanning and testing to reduce the attack surface.
5. Build robust crisis response capabilities for your identity system to enable rapid incident response, reporting, and forensic capabilities.
6. Have an automated and tested identity system recovery process to enable rapid restoration in case of a destructive incident.
7. Establish a programme of continuous improvement, including best practices from identity experts and leaders in the cyber security industry.

In our experience, achieving these capabilities is challenging, and sustaining them over time is not possible without significant automation. Semperis' market-leading products and services can provide you with this threat-led, automated capability.