SAI360
RISK FROM EVERY ANGLE

Your introduction to APRA CPS230

Table of Contents

Our unified approach to risk sets us apart

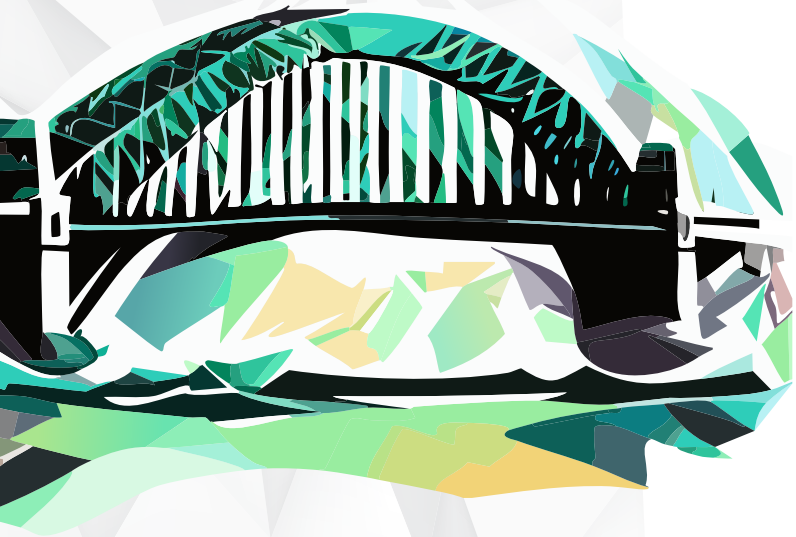
Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk and compliance spectrum.

Risk Management Solutions

- Risk & Compliance Management Solutions
- Enterprise & Operational Risk Management
- Regulatory Compliance
- Policy Management
- Third-Party / Vendor Risk Management
- Internal Controls
- Internal Audit
- Incident Management
- Conflicts of Interest (COI)
- Gifts and Hospitality
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Exports, Imports & Trade Compliance
- Harassment & Discrimination



Operational resilience in the financial sector

In today's interconnected and rapidly evolving world, businesses face a multitude of risks which may disrupt operations and threaten their ability to deliver critical services. The concept of operational resilience has emerged as a crucial framework for managing these risks and ensuring business continuity in the face of adversity. Operational resilience itself refers to the ability of an organization to withstand and adapt to operational disruptions, both expected and unexpected, whilst maintaining critical functions. These "operational disruptions" are, unsurprisingly, very broad in nature and encapsulate a range of incidents such as cyberattacks, system failures, human error, natural disasters and third-party disruptions.

The financial sector, in particular, relies on a complex web of technological systems to facilitate transactions and deliver services to customers. As a result, operational failures can have severe and long-lasting consequences on individuals and broader financial stability. Australian institutions have encountered several notable system failures in recent years, and such cases provide all-too-real examples of the need for operational resilience:

- In October 2022, Medibank suffered a massive security breach, exposing the personal data of each and every one of its 3.9 million customers. As part of their efforts to improve security and recover from the breach, Medibank took all of its IT systems offline and closed its branches over a weekend in December 2022. Medibank is expected to take a half-year hit of $26 million as a result, with this expected to climb to ~$40 million over the full year.
- In March 2023, Latitude Financial Services suffered a cybersecurity breach in which attackers stole personal data of nearly 14 million customers. Much like the Medibank case, Latitude's response included shutting down customer-facing systems to contain the attack whilst investigations to reveal the full scope of the impact continued.

In response to a historical track record of similar incidents, Australian regulators have taken steps to enhance operational resilience across the financial sector, and in July, 2022, the Australian Prudential Regulation Authority (APRA) released their own draft prudential standard on operational risk management (CPS 230)[2].

1. Medibank reveals attack vector and cost of 2022 security breach - Security - iTnews
2. https://www.apra.gov.au/sites/default/files/2022-07/Draft%20Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management.pdf

APRA Prudential Standards

CPS 230 sets out a comprehensive framework for APRA-regulated entities to identify, assess, manage and report on operational risks in a systematic and effective way. It emphasizes the importance of proactive risk identification, robust controls, and transparent reporting and disclosure.

June 2022	Oct. 2022	H1 2023	01 Jan. 2024
Prudential Standard CPS 230 Consultation opens	Consultation closed	CPS 230 rules finalized	Final implementation date

Scope

The draft standards cover a range of operational risks, including internal and external fraud, cybersecurity, business disruptions, and regulatory non-compliance. The proposed rules will apply to all APRA-regulated entities, described within the standards as the following:

- Authorized deposit-taking institutions (ADIs), including foreign ADIs, and non-operating holding companies authorized under the Banking Act (authorized banking NOHCs)
- General insurers, including Category C insurers, non-operating holding companies authorized under the Insurance Act (authorized insurance NOHCs), and parent entities of Level 2 insurance groups
- Life 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
- Registrable superannuation entity licensees (RSE licensees) under the SIS Act in respect of their business operations

Importantly, if the Head of the Group is an APRA-regulated entity, then the obligations are to be applied appropriately throughout the group, irrespective of whether or not they themselves are APRA-regulated. Firms with a global presence will therefore need to implement controls which account for the interplay between CPS 230 obligations and other jurisdictions with similar standards. In particular, its important for businesses to understand whether the APRA obligations are equivalent to, or lesser or greater than those set out by the other regulators and draft their resolution plans accordingly.

The risk management framework

Under the requirements, institutions must establish and maintain a comprehensive operational risk management framework consisting of policies, procedures and controls for identifying, assessing, and mitigating operational risks. Such risks are explicitly highlighted within CPS 230 and include the following[3]:

- Legal risk
- Regulatory and compliance risk
- Conduct risk
- Technology risk[4]
- Data risk
- Reputational risk
- Change management risk

Senior manager accountability is a pertinent theme throughout the draft standards, and APRA makes it clear that the board and senior management of in-scope firms are responsible for overseeing the effectiveness of the framework, ensuring it remains in line with the organization's overall risk appetite.

Operational risk profile

A robust operational risk framework is underpinned by a thorough, data-driven risk assessment. Institutions are expected to take a multi-stage approach to ensure each critical service line and associated risks are covered. The first, and arguably most important aspect involves mapping all processes and resources required to deliver critical operations.[5] These include, but are not limited to, people, technology, information, facilities and third-party service providers, as well as the interdependencies between them.

Once these processes are mapped, institutions must employ a variety of methods such as scenario analyses and impact assessments to identify the potential impacts of each operational risk typology. The primary aim here is to expose any deficiencies in existing controls and address any needs for new or improved mitigation processes. CPS 230 makes it clear that APRA-regulated entities must also conduct a similar risk assessment before engaging with third-party service providers to another party to ensure that such agreements do not jeopardize the institution's ability to meet prudential obligations in future.

Operational risk mitigation

Once critical business processes have been mapped and risk assessed, in-scope firms must design, implement and embed internal controls to mitigate the risks in line with their broader risk appetite. These controls must be tested, reviewed and, if necessary, revised at regular intervals to ensure their operating effectiveness. According to APRA, the frequency of review must be "commensurate with the materiality of the risks being controlled", any deficiencies in the control environment must be reported to senior management and rectified in a timely manner.

As is the case throughout the draft Prudential Standards, remedial measures must be attributable to individuals to promote accountability and encourage proactive intervention.

3. Despite being listed as such, these risks are not mutually exclusive and institutions must consider if and how they interact with and amplify one another.
4. Technology risk is particularly crucial as it spans multiple APRA regulations. Prudential Standard CPS 234, for example, requires institutions to monitor the age and health of its IT systems to meet stringent requirements for information security.
5. Critical operations are processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system.

Management of service provider arrangements

A growing number of institutions across Australia and the rest of the world are outsourcing non-core functions such as IT services, payment processing and customer support to third-party providers who may be able to offer services more efficiently and effectively. However, this growing interdependence means organization's often lack direct control over certain operations, making it challenging to monitor security and compliance.

CPS 230 therefore requires entities to perform appropriate due diligence when entering into, renewing or modifying arrangements with material service providers.[6] This includes assessing all financial and non-financial risks associated with reliance on particular providers and maintaining formal legally binding agreements - including Service Level Agreements (SLAs) - with minimum provisions related to service coverage. Entities must also implement SLA review policies and procedures that enable ongoing and effective management and oversight.

Entities must also identify and manage risks that could affect the ability of the supplier to provide ongoing services and ensure they are able to promptly exit the relationship if necessary. APRA-regulated entities are required to monitor and report on their service provider arrangements, notify APRA of any critical service provider agreements, and have their internal audit function review any proposed outsourcing arrangements prior to formal engagement.

Business continuity

Despite institutions best efforts, operational disruptions can, and do occur. By having a plan in place to respond and recover from these events, firms can minimize the impact and ensure continuity of critical services. With that in mind, CPS 230 is not just about encouraging firms to prevent disruptions, but also making sure they are prepared to respond in an agile manner.

APRA requires in-scope firms to prepare a full Business Continuity Plan (BCP), containing a register of all critical operations and risk tolerance levels, triggers to activate the plan, and subsequent key internal workflows and external dependencies required to maintain critical operations in the event of a disruption.

Institutions must also notify APRA within 24 hours of activating the BCP, covering the nature of the disruption, the action being taken, the likely impact on business operations, and the timeframe for returning to normal operations.

Risk reporting and disclosures

CPS 230 asks firms to report their operational risks to the board and senior management, as well as to APRA, on a regular basis. The reports should include information on the nature, scale, and significance of the risks, as well as the effectiveness of the controls in place. This information must also be disclosed in annual reports and financial statements. Failure to comply may result in APRA taking corrective actions such as independent reviews, full remediation program development, imposition of conditions on the entity's license, and other supervisory actions.

[6] Material service providers include, but are not limited to, those that provide the following services to an APRA-regulated entity: risk management, core technology services, internal audit, credit assessment, funding and liquidity management, mortgage brokerage, underwriting, claims management, insurance brokerage, reinsurance, fund administration, custodial services, investment management and arrangements with promoters and financial planners.

This goes beyond compliance

Aside from regulatory sanctions, operational failures expose firms to a range of risks, of which the effects can be extremely damaging:

- **Financial losses:** Operational failures can lead to financial losses for banks in the form of lost revenue or compensation payments to customers.
- **Reputational damage:** Operational failures can result in disruptions to key banking services, such as online banking, ATM withdrawals, and card payments. This can leave customers unable to access their funds, make payments, or conduct other important financial transactions. Such issues can severely impact a bank's reputation, eroding customer trust and confidence in the institution.

Financial institutions themselves are critical to the functioning of national economies, and their failure can have catastrophic ripple effects, both domestically and internationally. Disruptions to critical financial market infrastructure, such as payment and settlement systems, can also have significant spillover effects on other industries and markets, potentially causing systemic risk. By focusing on building operational resilience, financial institutions of the future will be better equipped to provide essential services to customers and counterparties even in the event of significant disruption.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R2088

The role of technology

APRA recognizes the challenge firms face in monitoring and maintaining all critical services, and they themselves advocate for the use of technology in adopting a data-driven approach to risk management:

"Entities must maintain appropriate and effective information systems to monitor operational risk, compile and analyze operational risk data and facilitate reporting to the Board and senior management."

Identify and quantify risk

Operational risk management software such as SAI360 can help firms identify and assess their key operational risks. Such solutions enable leaders to conduct comprehensive risk assessments that take into account huge volumes of internal and external data and overlay advanced analytics to extract quantifiable insights. By analyzing data on risks, compliance, and performance, both across the organization and its third and fourth parties, SAI360 can help businesses make data-driven decisions that improve their operations and enhance their competitive advantage.

Improved incident management

SAI360's operational risk module can be used to enhance business continuity planning by providing a framework for developing and testing effective responses. By using SAI360, firms can quickly identify critical business processes and develop strategies to operations in the event of a disruption, such as a natural disaster, cyber-attack, or system failure.

In the event that a disruption does occur, operational risk management software offers a centralized platform with a complete view for managing incidents and tracking their resolution. SAI360's solution can therefore be used to monitor incidents in real-time, assign tasks to relevant teams, and ensure that incidents are resolved quickly and efficiently.

Bullet-proof compliance

The Board of an APRA-regulated entity is ultimately accountable for the oversight of an entity's operational risk management, including business continuity and the management of service provider arrangements. Senior management must therefore provide clear and comprehensive information to the Board when they are making decisions that could impact the resilience of critical operations.

SAI360 can improve compliance management by providing real-time status updates of your risk program with configurable dashboards and visualization options. Such software offers a framework for tracking and reporting on operational risk exposure, enabling board members to act confidently and demonstrate decision making to authorities.

Rise above the competition

The average cost of downtime is significant. Research from the Ponemon Institute estimates the downtime cost per hour to be around $500,000, and recent findings from Uptime Institute's 2022 Outage Analysis Report found that over 15 percent of outages cost firms more than $1 million. It's clear then, that minimizing the impacts of system outages is critical to maintaining long-term profitability. What's more, customers value reliability, and they want to be confident that their bank will continue to meet their needs regardless of external factors, so it's important that institutions demonstrate an ability to manage risks and maintain stability during times of crisis and disruption.

Operational resilience is therefore not only important from a risk mitigation perspective, but it should also be considered an opportunity to distinguish your business from competitors. SAI360's software provides an integrated approach to risk management by collecting and aggregating risk data across the entire organization and its network of third parties. This allows firms to have a complete view of their operational resilience program and to proactively manage and mitigate risks. This resilience enables businesses to recover more quickly from disruptions and minimize the severity and duration of system outages, offering profound benefits to both the top and bottom line.

See what SAI360 has to offer

SAI360 is a leading cloud-based solution provider for operational resilience and more. Our modular approach allows you to take advantage of configurable solutions and quickly shape them to help you thrive in the evolving Governance, Risk and Compliance landscape. To learn more about the SAI360 platform and how we can advance your GRC goals, contact us online to set up a call with one of our representatives.

151227 0324