gieom

Risk Central
Operational Risk & Resilience

Navigating APRA CPS 230 with Risk Central

www.gieom.com

APRA CPS 230 is a new prudential standard designed to strengthen operational risk management and resilience for APRA-regulated entities in the banking, insurance and superannuation fund areas.

Implementation Timeline

Key Principles

1 Operational Risk Management

Effectively manage its operational risks, set and maintain appropriate standards for conduct and compliance

2 Critical Operations

Maintain its critical operations within tolerance levels through severe disruptions

3 Service Providers

Manage the risks associated with the use of service providers

Guide to Implement an Operational Resilience Program

1 Register of Critical Operations

Understand & maintain critical operations

2 Resource Mapping

Mapping and visualization tool, help giving dependency visibility

3 Set Tolerance & Scenario Testing

Set Customer and outcome focused

4 Risk Management

Improve operational risk profile

5 Business Continuity Management

Focus on prevention and to demonstrate response to disruptions

6 Service Provider Management

Robust monitoring of material service providers

You might also like

Blog : 6 Simple Steps for Implementing an Operational Resilience Framework

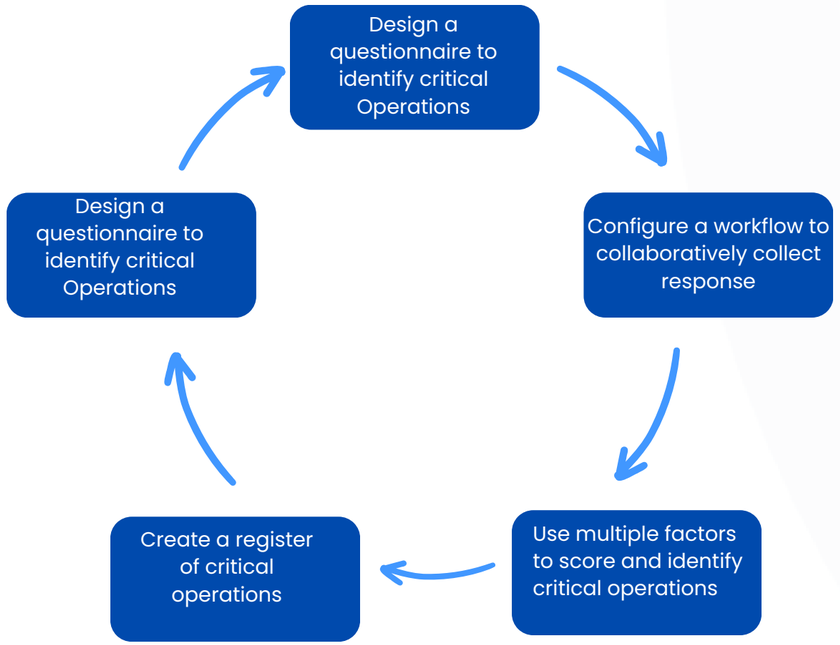
Blog : Overview of the Australian Operational Resilience Regulatory Guidelines

1 Register of Critical Operations

Expectations

Must include

- Payments, deposit-taking and management, custody, settlements and clearing
- claims processing
- investment management and fund administration
- customer enquiries
- Additions based on nature of business



How

Our operational resilience platform features a low-code, drag-and-drop interface with configurable workflows and reporting components. Users can easily customize forms, workflows, and scoring rules. This centralized system streamlines documentation, enhances risk assessment, and enables effective monitoring, ensuring that all critical operations are clearly defined and managed within the organization's resilience framework.

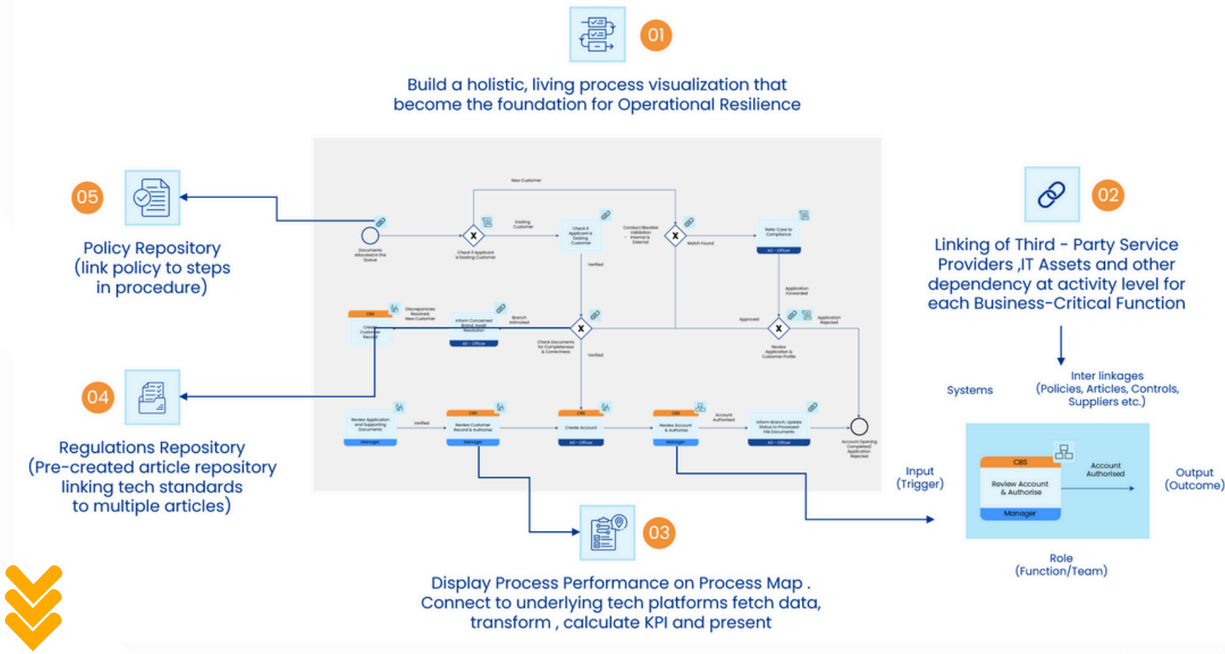
2 Resource Mapping

Expectations

Identify and document the processes and resources needed to deliver critical operations, including people, technology, information, facilities and service providers, the interdependencies across them, and the associated risks, obligations, key data and controls .

How

Map your critical processes visually and link all the dependencies at the granular activity level. Integrate regulations, checklists, and third- and fourth-party processes to create an end to end map. The platform offers tools to aid impact analysis for quick change management assessments, a collaborative workflow to support the creation and updating of processes. This ensures stakeholder alignment and effective integration of changes across the organization.



3 Set Tolerance & Scenario Testing

Impact Tolerance

Expectations

For each critical operation, an APRA-regulated entity must establish tolerance levels for:

- The maximum period-of-time the entity would tolerate a disruption to the operation
- the maximum extent of data loss the entity would accept as a result of a disruption
- minimum service levels the entity would maintain while operating under alternative arrangements during a disruption

Actionable

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.

How

Using the rule engine, multiple thresholds can be established with corresponding notification rules. In incident reporting, users can map tolerance breaches, and all such incidents can be reported to the regulator through a standardized reporting functionality.

Scenario Analysis

Expectations

Undertake scenario analysis to identify and assess the potential impact of severe operational risk events, test its operational resilience and identify the need for new or amended controls and other mitigation strategies

How

The scenario analysis functionality allows users to simulate various risk scenarios and assess their potential impact on operations, helping to identify vulnerabilities and prepare effective response strategies. This feature enables organizations to proactively manage risk by testing different outcomes and understanding how changes in one area could affect overall performance and resilience.

4 Risk Management

Expectations

An APRA-regulated entity must manage its full range of operational risks, including but not limited to legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk and change management risk. Senior management are responsible for operational risk management across the end-to-end process for all business operations.

An APRA-regulated entity must maintain appropriate and sound information and information technology (IT) capability to meet its current and projected business requirements and to support its critical operations and risk management. 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 (CPS 234).

How

Provides an integrated platform to identify, assess, and mitigate risks across various operations, ensuring comprehensive oversight and control. By leveraging advanced analytics and customizable risk thresholds, the software allows organizations to respond proactively to emerging threats, enhancing overall resilience and compliance with regulatory standards.

5 Incident & Business Continuity Management

Expectations

Incident Management

- Record Incident & near miss
- RCA
- 24-72 hours regulatory reporting
- Mitigation
- Changes and improvements

Business continuity Management

- Business Impact Analysis
- Business Continuity Plan
- Business Continuity Testing
- Action Plan
- Changes & Improvements

How

Gen AI-enabled incident management enhances the description and recording of incidents, providing clearer insights for users to improve response times and minimize the impact of disruptions. Additionally it provides features for creating and maintaining recovery plans, ensuring that all critical functions and processes are well-documented and ready for immediate activation in the event of a disruption

6 Third Party Service Provider

Expectation

Policy Management

- Maintain a comprehensive service provider management policy
- Should include monitoring, substituting , exiting agreement with MSP
- Approach to MSP`s risk and risk associated with fourth parties

Material Service Provider

- Register of MSP and classify type of MSP
- Classify following service providers as MSP – mortgage brokerage, credit assessment, underwriter, claims management et.

Due Diligence & Assessment

- selection, assessment process and due diligence
- Assess financial and non financial risks , including- location, concentration, fourth parties
- Regular performance assessment
- Control effectiveness and compliance

Contractual Agreement

- Mandatory contractual clauses
- Contract clauses providing APRA access

APRA Reporting

- Register of MSP on Annual basis
- Within 20 days of any material change in agreement of MSP
- Prior to entering into any material off shoring arrangement

How

Gen AI-enabled contract vetting offers advanced capabilities to automatically review and analyze contracts for compliance and risks, while digital impact analysis assesses the potential effects of changes in real-time.

The solution also includes unique features for vendor scoring and assessment, evaluating security and compliance checks based on multiple criteria, and conducting ESG analysis to ensure alignment with sustainability goals.

Additionally, robust API integration allows seamless connectivity with various platforms and systems, enhancing overall functionality and data sharing capabilities

You might also like

Video - Gieom's operational resilience platform

Case Study : UK Financial Services Supervisory Authority Appoints Gieom as Sole Provider for Integrated Risk and Resilience Platform

Consider Gieom's Operational Resilience Solution

At Gieom, we specialise in financial services operational resilience and risk management. Since 2012 we have partnered with more than 120 global financial services organisations to help manage their operational resilience, risk management and compliance faster, smarter and more cost-effectively. Underpinned by Gieom's award-winning Operational Risk & Resilience

We have customers and strategic partnerships across 3 continents, with proven implementation, stand-out technology, unrivalled functionality and robust support services.

Get in touch

Sales contact : Nishant Betgeri

nishant.betgeri@gieom.com

9916444644

Follow me on LinkedIn

For all other queries contact marketing@gieom.com

www.gieom.com

© 2024 Gieom Business Solutions Pvt. Ltd. All rights reserved.