TATA CONSULTANCY SERVICES

TATA

CPS 230 Operational Resilience

Preface

The Australian Prudential Regulation Authority (APRA) has released their Prudential Standard CPS 230 Operational Risk Management, which has been designed to strengthen the management of operational risk by all APRA-regulated entities.

The standard underpins CPS 220 Risk Management and replaces several existing standards including CPS/SPS 232 Business Continuity management and CPS/SPS 231 Outsourcing. It sets out revised operational risk controls and monitoring, business continuity and the management of service providers expectations. The key elements highlight a continued focus on operational resilience across the Australian financial services sector.

Key requirements of CPS230

- Identify, assess and manage its operational risks, with effective internal controls, monitoring and remediation;

- be able to continue to deliver its critical operations within tolerance levels through severe disruptions, with a credible business continuity plan (BCP); and

- effectively manage the risks associated with service providers, with a comprehensive service provider management policy, formal agreements and robust monitoring

This e-book outlines TCS’s operational resilience framework and our technology capabilities to support our client's path to CPS230 compliance.

Operational Resilience Framework

Operational Resilience Framework

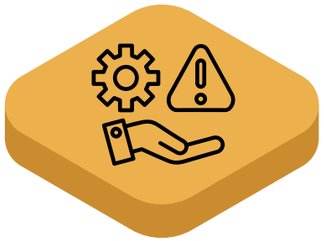
In today's rapidly evolving business environment, operational resilience has become a buzzword synonymous with sustainability and success. This concept, far from being a mere corporate jargon, is a critical strategy for businesses aiming to thrive amidst the uncertainties of the 21st century.

Events such as the COVID-19 crisis, the Suez Canal blockage, the war in Ukraine, and the recent Houthi attacks have disrupted global supply chains, putting operational resilience firmly in the spotlight. Consequently, fortifying operational resilience through an overarching framework is fast becoming a regulatory mandate in most regions across the globe.
In our view,

Australian BFSI organisations must not look at the current crop of regulations such as the CPS230, Security of Critical Infrastructures Act, and the Data Privacy Act through the myopic lens of just compliance. In a VUCA world, the risk landscape will only become more complex as new uncertainties arise.

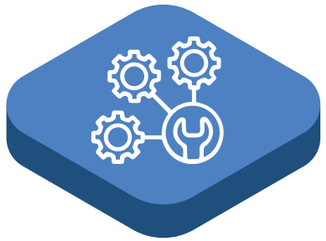
Recognising these challenges, TCS' Operational Resilience Framework demystifies the concept of operational resilience by focusing on its five key pillars. By understanding and implementing these pillars, businesses can navigate the complexities of the modern world with agility and confidence, ensuring not just survival but also long-term prosperity.

5 Pillars of Operational Resilience



Risk Management

Identify, assess and manage operational risks, with effective internal controls, monitoring and remediation



Service Mapping

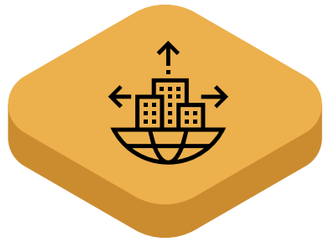
Clear understanding and mapping of critical operational services, services levels, and improvement roadmap

Incident Management

Have a defined and tested incident management plan that focuses on the recovery of critical customer focused services.

Business Continuity

Deliver critical operations within tolerance levels through severe disruptions, with a credible business continuity plan (BCP) and disaster recover capability.



Outsourcing Management

Effectively manage the risks associated with service providers, with a comprehensive service provider management policy, formal agreements and robust monitoring

Risk Management

Pillar 1

Integration of Resilience Culture within Business Practices

Resilience Culture Embedded

- Resilience integrated in the culture of an organisation
- Resilience Domain Silo's exist & Roadmap in place to align
- Service Taxonomy in place but no Tolerances defined
- Starting journey to implement Operational Resilience

Operational Resilience Embedded

- Resilience embedded within NFR / GRC Practices & Firmwide
- Governance Practices refreshed to embed tolerances
- Critical Services mapped End to End & Stress Tested against multiple types of scenarios
- Communication Practices aligned to services
- Supply Chain Dependencies integrated within Critical Services to ensure oversight & management of risk

Resilience Operating Silo's

- Resilience not integrated with Operational Risk / Non Financial Risk
- Three Lines of Defence model requires development
- Resilience operating in Silo / Limited Governance
- Board level Roles & Responsibilities required
- Transformation journey, roadmap & Investment required to develop a firmwide Operational Resilience framework

Regulatory Alignment & Transformation

- Critical Services identified & Tolerances defined
- Roles & Responsibilities across Three Lines of Defence in place and Board are aware of roles & responsibilities
- Journey to mapping & stress testing commenced
- Operational Resilience a core pillar of NFR & GRC Practices, Governance needs to be further defined
- Steps mapped to fully embed firmwide Operational Resilience

Transformation of Resilience Frameworks & Practices

Outsourcing Management

Pillar 2

Business Continuity

Pillar 3

Understand the Business Context

- Discuss and Understand Nature of Business
- Identify Scope
- Conduct BIA and RA
- Identify requirements and dependencies

Build Business Continuity Strategyt

- Develop and Implement recovery strategies for people, process, technology, facilities and suppliers

Develop & Implement BCM Response

- Develop and Implement recovery strategies for people, process, technology, facilities and suppliers

Embed BCM Culture

- Conduct Training and Awareness on BCM
- Build Competency on BCM

Exercise, Maintain & Review

- Conduct BCP Exercises
- Monitor & Maintain BCM Process
- Review End-to-End BCM Process

Incident Management

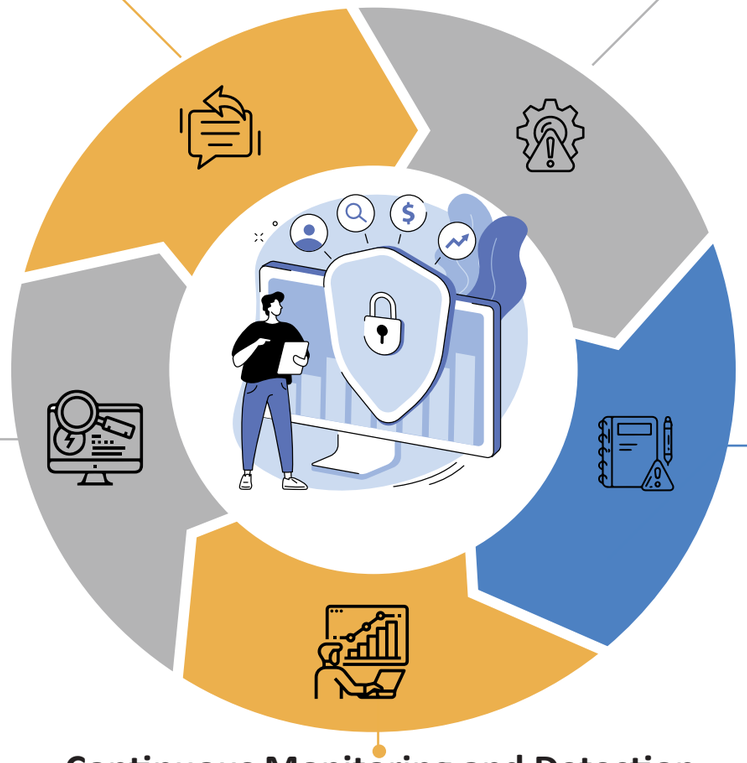
Pillar 4

Response and Recovery Execution

When incidents occur, swift and effective response and recovery execution are essential to minimize the impact on operations. Incident management processes should enable rapid response actions, such as containment, eradication, and recovery, to restore normal business operations as quickly as possible.

Risk Identification and Assessment

Operational resilience requires a thorough understanding of potential risks across various aspects of the business, including technology, supply chain, personnel, and regulatory compliance. Incident management processes should be designed to identify and assess these risks proactively, considering their potential impact on the organization's ability to maintain critical operations.



Post-Incident Analysis and Learning

Thorough post-incident analysis to identify root causes, lessons learned, and areas for improvement. This analysis should inform updates to incident management processes and operational resilience strategies, enhancing the organization's ability to prevent similar incidents in the future and strengthen overall resilience.

Response Planning and Preparedness

Effective incident management requires well-defined response plans and preparedness measures. These plans should outline clear roles and responsibilities, escalation procedures, communication protocols, and resource allocation strategies.

Continuous Monitoring and Detection

Continuous monitoring and detection capabilities to identify potential threats and vulnerabilities in real-time. This includes the use of monitoring tools, threat intelligence sources, and risk assessment frameworks to detect anomalies and security incidents promptly. By monitoring for emerging risks, organizations can proactively mitigate threats before they escalate into operational disruptions.

Service Mapping

Pillar 5

Identification of Critical Services

Clearly define what constitutes a critical service within your organization. This includes services that are essential for the institution to meet its financial, legal, regulatory, and reputational obligations. Identification should consider the impact of service disruption on the institution's operations and its customers.

Service Dependencies

Map out and document the internal and external dependencies that each critical service relies upon. This includes understanding the upstream suppliers and downstream users of the service, as well as the technological, human, and physical resource dependencies.

Risk Assessment

Perform a comprehensive risk assessment for each critical service to identify vulnerabilities and potential points of failure. This should include risks stemming from third-party vendors, IT security risks, and risks related to physical infrastructure. The assessment should consider both the likelihood and the impact of these risks.

Impact Analysis

Conduct an impact analysis to determine the consequences of disruptions to each critical service. This involves understanding the financial impact, the effect on customer service and satisfaction, legal or regulatory repercussions, and the timeline for service degradation and recovery.

Mitigation Strategies and Recovery Plans

Develop mitigation strategies to reduce the identified risks and establish recovery plans for restoring services in the event of disruption. This includes setting up alternative processes, engaging backup suppliers, or having redundant systems in place. Recovery plans should be specific, with clear roles and responsibilities, and they should be tested regularly to ensure effectiveness.

Tools and Technology

Automated Regulatory Compliance

Streamlining the regulatory compliance process

Banks need to comply with a plethora of obligations which could often result in a higher inherent risk of non-compliance, affecting the agility and customer experience of the enterprise. TCS **Automated Regulatory Compliance** is an integrated RegTech solution that drives intelligent interventions and automation in the core compliance value chain. It helps banks and financial institutions:

- Enable obligation processing with NLP and AI-based components
- Facilitate regulatory knowledge modeling and lineage analytics with NLP and ontology-based design
- Manage obligations and risk taxonomy by leveraging machine learning-based services
- Enable cognitive intelligence with automated compliance and control assurance enabled by NLP, ML, and metadata-based smart data solutions
- Leverage SBVRL framework for obligation codification and breach monitoring/reporting

Key benefits of using this platform include:

- Improved accuracy in identifying obligations by 70-80%
- Reduced compliance and residual risk exposure
- Improved agility in driving compliance readiness by 50-75%
- Improved delivery of frictionless compliance through automation>
- Reduced cost of compliance with increased automation in control assurance

TCS Operational Resilience Hub

Driving effective resiliency risk management

The TCS Operational Resilience Hub is a one-stop digital solution for operational resiliency management. It provides digital service footprint and dependency analyser, impact tolerance manager, scenario onboarding and what if analysis workbench and intuitive resiliency dashboard.

Furthermore, it unifies integrated data fabric to uild master service directory and provides BIA framework to assess business impact across people, process, technology and third-party dimensions.

It leverages machine learning based models to recommend impact tolerance levels and scenario recommendations and is flexible to integrate with existing operational risk and decision management systems of the bank. It's customisable and comprehensive reporting capabilities cater to regulatory and internal reporting.

By using this platform, banks can

- Increase automation by reducing over 60% manual effort in creating master directory
- Efficiency gain of over 70% through end-to-end visibility of IBS
- Resilient reporting to support regulatory and internal governance

TCS Supplier Risk Analytics Solution

Data and Analytics driven automated service components to drive effective supply risk management

In today's expanding marketplace the competition is fierce, and it's ever more important to ensure banks are maintaining the right supplier relationships. Unfortunately, only 6% of banks report full visibility of their supply chain.

As disruptions increase, organisations need to modernise the assessment and monitoring of suppliers and the supply chain. Leveraging the right technology to instantly assess multiple types of risk within your supplier network can help improve the effectiveness of onboarding new suppliers, while simultaneously flagging changes in the risk profile of existing suppliers.

The TCS Supplier Risk Analytics Solution helps banks:

- Unify integrated data model focused on supplier risk management value chain
- Measure resiliency insights of suppliers against impact on related business services
- Seamlessly integrate analytics on supply chain risks to parent suppliers
- Leverage AI/NLP driven media analytics to generate early warning signs on supplier risks
- Easily integrate with existing GRC, procurement and risk systems to feed risk analytics
- Customise data-driven risk scoring framework to cover wide variety of risk categories

Success Stories

Third-party risk assessment for one of the largest banks in North America

Business requirement

One of North America's largest banks was working with multiple vendors and adhering to multiple vendor policies and processes for their information security controls. This limited the availability of skilled resources to conduct vendor security assessment and validate the efficacy of their control framework. The bank partnered with TCS to design and identify the operating effectiveness of Information Security controls.

How TCS helped?

TCS, leveraging its industry expertise and domain knowledge, conducted a risk and scope assessment based on the nature of services, duration of engagement with suppliers including the data shared with them. After conducting a detailed InfoSec Risk Assessment and a gap remediation, TCS developed a framework complying with ISO27001 and Standardised Information Gathering (SIG).

Key benefits

Having delivered a success pilot within 4 months, TCS developed & deployed an assessment structure; completing over 700 assessments.

TCS closed over 950 critical gaps and over 2300 low-critical gaps across supplies and conducted a remediation of identified gaps.

CRO transformation for operational resiliency for a UK financial service firm

Business requirement

The customer is a leading UK based financial service group, providing wide range of financial services focused on investment management, lifetime mortgages, pensions , annuities and life assurance.

Driven by the regulations and its organisational objective to enable business service centric framework to attain higher operational preparedness and resilience maturity, the bank had taken a work-stream based approach.

How TCS helped?

TCS conducted a holistic, end-to-end mapping of critical operations from a resilience perspective. TCS also defined the bank's Operational Resilience Maturity Assessment mode & template, its overall target framework, incidence response, and gap analysis.

Based on the above, TCS was able to redefine the BIA process and template to be resilient and cover scenarios that would result in identifying wider martial risks, gaps and business service requirements. TCS also collaborated with divisional business owners to assist in incorporating the new framework and standards as well as carryout assessments.

Key benefits

Having developed a growth roadmap, TC was able to enable an effective policy, standard, process, measurable metrics so as to enable orgaisational-wide operational resilience framework and ensure OR regulatory compliance.

Enabled a holistic, end-to-end mapping of critical operations thereby providing Resilient Business Services & Streamlined BAU operations.

Risk Assessment & Due Diligence for US Based Global Retail Bank

Business requirement

This client is a leading global retail bank headquartered in the US and works with over 7000 third-party vendors or suppliers. The bank wanted to conduct a third-party management (TPM) lifecycle assessment and due diligence. They also wanted to conduct an ongoing oversight review, review their information security process and consolidate their TPM processes to recalibrate business operations and future-proof the organisation.

How TCS helped?

Deploying its TCS SRM solution, an employee and customer-centric progressive, risk aware, operationally resilient business continuity solution that can reevaluate the business of any enterprise and help them in prolonged operations. Leveraging the insights from the tool, TCS then deployed a robust governance model for seamless delivery of the TLM process including:

- Developing risk mitigation workflows to address any delegated tasks based on regulations, standards and frameworks
- Using metrics as automation triggers, the solution automatically schedules reports to quickly generate and share key details with critical stakeholders to maintain compliance at a federal and regulatory level
- Facilitating better decisions on risk management and resilient actions for business continuity

Key benefits

Having developed a growth roadmap, TC was able to enable an effective policy, standard, process, measurable metrics so as to enable orgaisational-wide operational resilience framework and ensure OR regulatory compliance.
Enabled a holistic, end-to-end mapping of critical operations thereby providing Resilient Business Services & Streamlined BAU operations.

For more details, contact:

Ajya Atreya
Consulting Partner
Strategic Risk Initiatives
BFSI- A&NZ
Tata Consultancy Services
ajay.atreya@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over 56 years. Its consulting-led, cognitive powered, portfolio of business, technology and engineering services and solutions is delivered through its unique Location Independent Agile™ delivery model, recognized as a benchmark of excellence in software development.

A part of the Tata group, India's largest multinational business group, TCS has over 601,000 of the world's best-trained consultants in 55 countries. The company generated consolidated revenues of US $29 billion in the fiscal year ended March 31, 2024, and is listed on the BSE and the NSE in India. TCS' proactive stance on climate change and award-winning work with communities across the world have earned it a place in leading sustainability indices such as the MSCI Global Sustainability Index and the FTSE4Good Emerging Index.

For more information, Visit **www.tcs.com**