

CPS 230: Operational Risk Management

Strengthening the resiliency of the financial services ecosystem

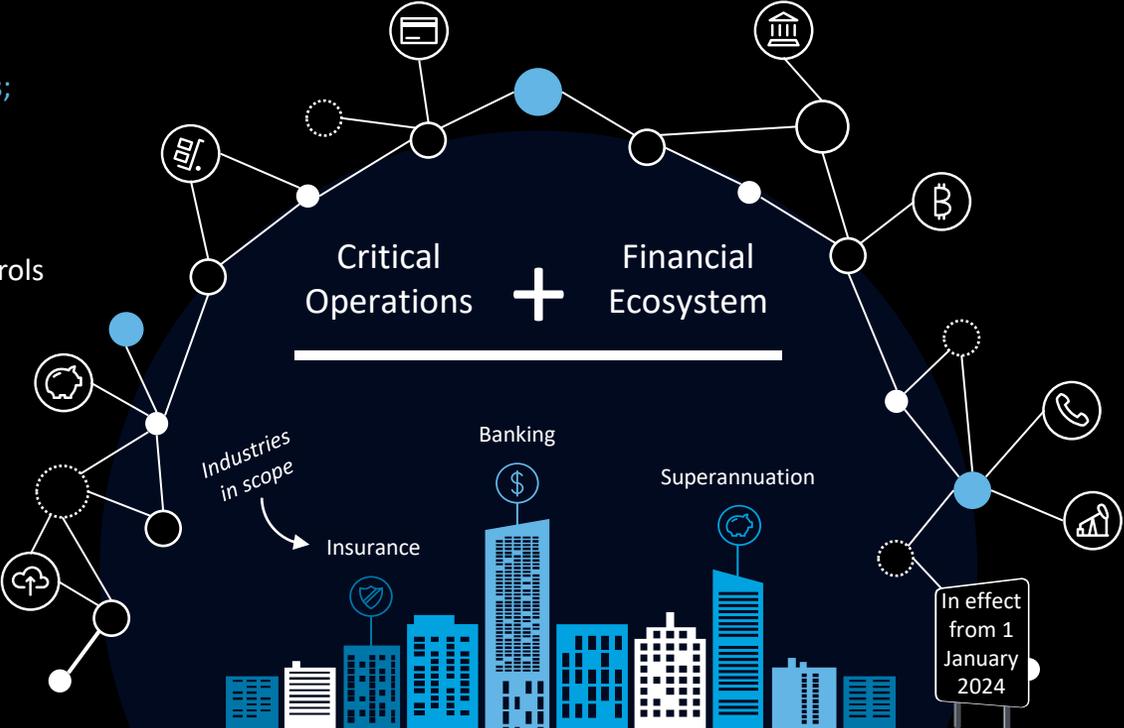
October 2022

CPS 230 Operational Risk

CPS 230 introduces new and enhanced requirements that will better align the industry with global standards and industry leading practices, and strengthen the overall resiliency of the Financial Services ecosystem.

Key Drivers

- **Low tolerance for disruptions;** increasing expectation (and need) to always be 'on', particularly given significance of the financial services being provided
- **Increasing reliance on service providers;** resulting in a more interconnected and complex financial ecosystem
- **Control failures;** issues and incidents continue to arise due to ineffective controls



Key Objectives

- **Strengthen operational resilience** and reduce the impact of disruptions on customers, market participants and the financial system
- **Ensure critical operations are maintained through severe business disruptions** and risks arising from the use of service providers, including fourth parties, are considered and managed effectively
- **Consolidate and streamline existing prudential standards**

Key Changes and Implications

Today

Critical Business Operations

Critical business operations are typically identified from the perspective of the entity by assessing the impact on the entity should critical business operations be unavailable.

Recovery Timeframes

AS part of conventional business continuity planning, entities have identified Maximum Allowable Outages (MAOs) (or Maximum Tolerable Periods of Disruptions (MTPD)), and Recovery Time Objectives (RTO).

Management of Material Outsourced Providers

Existing policies are typically focused on the management of third-party service providers performing material business activities that would otherwise be performed 'in-house', with monitoring activities usually limited to a review of their performance against agreed service levels. Additionally, entities largely rely on contractual agreements with third parties to mitigate risks associated with fourth-parties..

Testing and Review against BCM Objectives

Scenarios used for testing are often limited in scope (e.g. only testing a sub-set of critical operations) and/or based on generic unavailability scenarios that are '*contained and plausible*' (e.g., unavailability of technology or an office location).

Board Responsibility

Operational risk responsibilities have been steadily shifting towards Line 1 Management, there is still a heavy reliance on risk management functions to maintain end-to-end oversight, and no enforced linkage between Board and Senior Management decision making and the impact of these decisions on the resilience of critical operations.

Broad Focus on Material Risks

Entities are only required to maintain a risk management framework which addresses material risks – broadly defined as those with a financial or non-financial 'material' impact on the institution, its depositors and/or policyholders.

January 2024

Critical Operations

Take an 'outside-in' view and shift the focus from what is critical to the organisation to what is critical to customers, market participants and the financial system more broadly.

Tolerance Levels

Define not just how long a critical operation can be disrupted for, but *how much and for how long* before the impact is intolerable. In addition to setting recovery timeframes, identify Maximum Data Losses and Minimum Recovery Objectives or Service Levels.

Management of Material Service Providers, incl. Fourth Parties

Expand the scope beyond outsourced service providers and identify material service providers (incl. third and fourth parties, partners, suppliers and affiliates) that enable critical operations or expose the organisation to material operational risks. Additionally, ensure risks presented by third and fourth parties are managed proactively and comprehensively on an ongoing basis.

Testing and Review Against Tolerance Levels

Establish a more robust testing and review program which includes all critical operations and material risks, and assesses the entity's ability to maintain business operations within tolerance levels through '*severe but plausible*' disruptions.

Board Accountability

Place *accountability*, not just *responsibility*, on the Board and senior management to oversee and manage operational risk, end-to-end. Risk reporting should be clear on the impacts to the resilience of critical operations.

Clear Linkage to Operational Resilience

Review and update the entity's operational risk profile to ensure it comprehensively considers critical operations, approved tolerance levels and interdependencies with third and fourth parties. Risk profiling activities should also consider operational risk incidents and near misses.

Key Contacts



Caroline Brell

Partner, Financial Industry
Risk & Regulatory Services
cbrell@deloitte.com.au



Sean Moore

Partner, Financial Industry
Risk & Regulatory Services
semoore@deloitte.com.au



Erik Kronborg

Partner, Digital & Technology Risk
ekronborg@deloitte.com.au



Ally MacLeod

Partner, Digital & Technology Risk
amacleod@deloitte.com.au



Tommy Viljoen

Partner, Cyber Risk
tfviljoen@deloitte.com.au



Kreeban Govender

Director, Financial Industry
Risk & Regulatory Services
kregovender@deloitte.com.au



Kerri Hie

Director, Financial Industry
Risk & Regulatory Services
khie@deloitte.com.au



Jaramie Nejal

Director, Financial Industry
Risk & Regulatory Services
jnejal@deloitte.com.au



Tarah Unn

Senior Manager, Financial Industry
Risk & Regulatory Services
tunn@deloitte.com.au



This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the “Deloitte Network”) is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

About Deloitte

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 286,000 people make an impact that matters at www.deloitte.com.

About Deloitte Asia Pacific

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People’s Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

About Deloitte Australia

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia’s leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www.deloitte.com.au
Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

© 2022 Deloitte Touche Tohmatsu.

Designed by CoRe Creative Services. RITM1206245