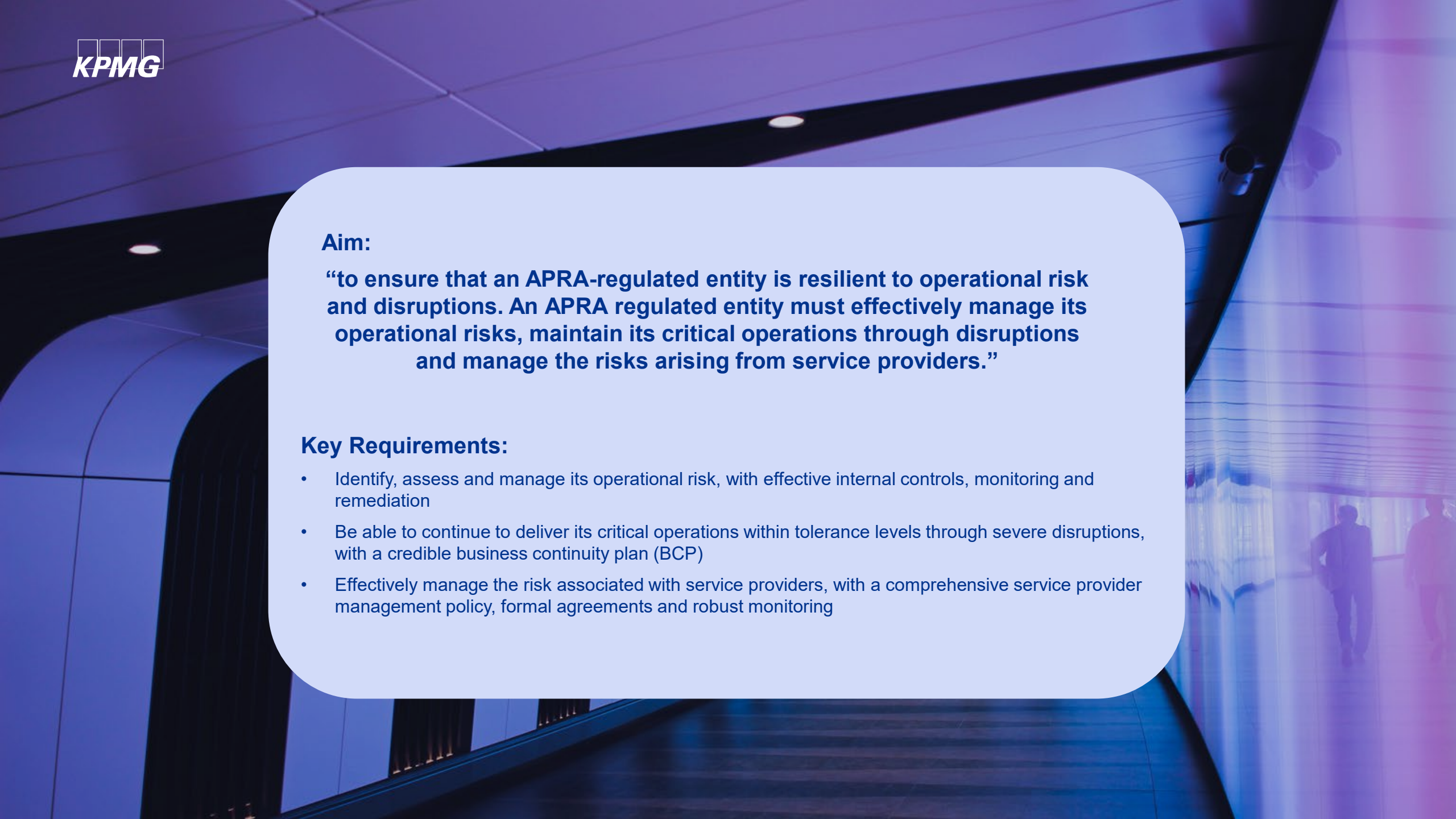
KPMG

APRA Prudential Standard CPS 230: Operational Risk

InsureTech Member Education Session

March 2023



Aim:

"to ensure that an APRA-regulated entity is resilient to operational risk and disruptions. An APRA regulated entity must effectively manage its operational risks, maintain its critical operations through disruptions and manage the risks arising from service providers."

Key Requirements:

- Identify, assess and manage its operational risk, 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)
- Effectively manage the risk associated with service providers, with a comprehensive service provider management policy, formal agreements and robust monitoring

CPS 230 (draft) is designed to strengthen the management of operational risk and focuses on critical operations

Purpose

APRA proposes to introduce a **new cross industry Prudential Standard** CPS 230 Operational Risk Management (CPS 230), designed to **strengthen operational risk management** in banking, insurance and superannuation industries.

"Ensure that an APRA-regulated entity is resilient to operational risk and disruptions." *(Draft CPS 230 Standard)*

Approach

The regulator is looking to **simplify** its regulatory architecture by the proposed **integration of existing standards** for outsourcing and business continuity into a single, **principle-based** standard which will **strengthen operational resilience** across the industry.

Outcomes

The consultation paper sets out requirements for regulated entities to:

- **maintain effective internal controls** for operational risk, commensurate with the size, business mix and complexity of the activities they undertake;
- be **prepared and ready** to ensure **continued delivery of critical operations** during periods of disruption; and
- effectively manage the risks associated with the use of service providers.

Timeline

July 2022
New Consultation Paper CPS230

October 2022
Consultation response submissions due

Early 2023
Final CPS230 Standard expected for release

1 Jan 2024
New standard expected to come into force

Overview: Draft Prudential Standard CPS 230 – Operational Risk Management

On 28 July 2022 ARPA released a Draft CPS 230 – Operational Risk Management for consultation with responses due by 21 October 2022

See the Appendix for explanation of core concepts:

- **meaning of "critical operations"**
- **meaning of "service provider".**

Rationalisation of Standards

The proposed standard replaces and supersedes the existing standards CPS/SPS 232 – Business Continuity
&
CPS/SPS 231 – Outsourcing

PROPOSED FRAMEWORK

CPS 230 – Operational Risk Management

CPS/SPS 234 – Information Security

CPS/SPS 232 – Business Continuity Management

CPS/SPS 231 – Outsourcing

AIM OF STANDARD

Strengthen Operational Risk Management

Improve Business Continuity Planning

Enhance third-party risk management

Summary of Standard

Requirements for APRA-regulated entities

- Effectively manage its operational risks, & set & maintain appropriate standards for conduct & compliance
- Maintain its critical operations within tolerance levels through severe disruptions
- Manage the risks associated with the use of service providers

Risk Management Framework

- The requirements of CPS 220 – Risk Management are not superseded by CPS 230
- Operational Risk Management (ORM) must be integrated to the overall Risk Management Framework
- The required Risk Management Framework reviews must now incorporate ORM
- Entities with weaknesses in ORM may have additional requirements imposed by APRA

Role of the Board

- Must oversee ORM & effectiveness of key internal controls to maintain risk profile within risk appetite
- Must approve BCP, including tolerance levels for disruptions to critical operations
- Must approve service provider management policy & review risk & performance of material service providers
- Senior management must provide clear & comprehensive information to the Board

Operational Risk Management

- Entities must consider their operational risk profile and maintain a comprehensive assessment that considers systems to monitor, analyse & report operational risk, identify processes and resources needed to operate and undertake scenario analysis to identify and assess the impact of severe risk events
- The assessment must consider the impact of business and strategic decisions as part of its planning process

Business Continuity

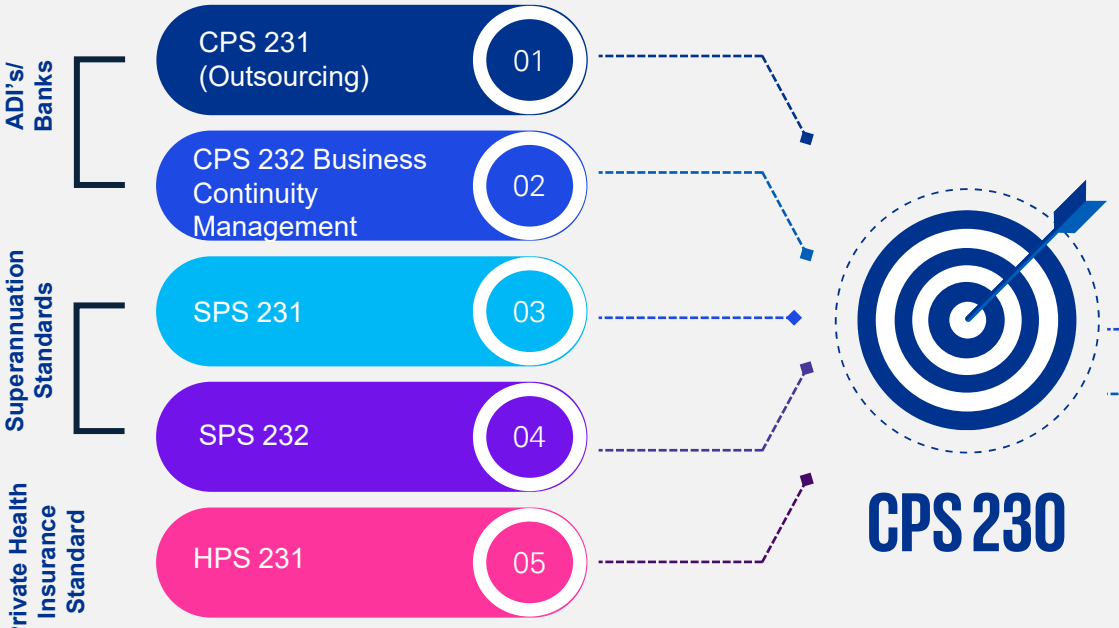
- A register of critical business processes must be maintained & reasonable steps taken to minimise disruptions
- A credible BCP must be maintained & enacted in the event of a disruption of critical business processes
- Board approved tolerance levels must be established
- A systematic testing program for BCP must be implemented

Management of Service Provider Arrangements

- A comprehensive Service Provider Management Policy must be maintained
- Material Service Providers (and relevant 4th parties) must be identified and risks arising from their use managed appropriately
- Appropriate Due Diligence, Risk Assessments & consideration of systemic importance is required before entering into or renewing a material service provider arrangement
- Formal legally binding service agreements must be maintained that include the prescribed matters

KPMG Thematic Observations: Draft CPS 230

Five standards will be replaced by the new CPS 230 as APRA move towards modernising and simplifying its regulatory architecture:



KPMG Thematic Observations:

1. Accountability & Responsibility

- Proposed standard suggests the Board is 'ultimately accountable for the oversight of an entity's operational risk management, including business continuity and the management of service provider arrangements' – this is consistent with overall CPS 220.
- The proposed standard outlines that senior management 'must provide clear and comprehensive information to the Board on the expected impacts on the entity's critical operations.
- Further detail will be required on the level of detail provided to the Board to ensure the capacity to effectively review and challenge this information, amongst other responsibilities.
- Additionally, increased Board oversight required may limit autonomy to discharge operational responsibilities effectively.

2. Timeline for effective implementation

- Proposed effective date of 1 January 2024 of < 1y following the publication of the final standard is exceptionally challenging for entities to meet all requirements.
- May result in tactical or ill-considered approaches that do not allow the standard to be fully embedded
- Risk of stand-alone centralised processes being constructed to meet compliance dates rather than sustainable change.
- Other overseas jurisdictions that implemented similar regimes allowed several years for full implementations – allowing more time to carefully design, review, implement and embed.

3. Operational approach to service provider management

- The impact on the requirements related to service provider management under the proposed standards is very high.
- Expanded definition of 'material service provider' may capture a significantly increased number of regulated entities in scope and translate to additional compliance costs.
- Significant need for investment in technology and internal capability required. This may prove challenging, and cost-prohibitive for smaller entities.
- CPS 230 and CPS 511 require organisations to review and update contracts. The need to continually revisit and renegotiate contracts with service providers mid-way poses significant operational challenges and increased costs.

CPS 230 – Interplay with existing landscape

CPS 230 is a combination of existing standards (CPS/SPS 231 Outsourcing and CPS/SPS 232 Business Continuity Management). Apart from these, the draft CPS 230 intersects with many other existing standards from both within APRA and other regulators and industry bodies. Entities need to examine and consider these intersections should the standard be implemented in its current form, so they succeed in meeting other obligations.

Financial Accountability Regime (FAR)

Those holding accountable positions under FAR, will need to consider how CPS 230's lens on Board accountability for oversight of operational risk management impacts them.

Risk Management

In line with CPS/SPS 220's required reviews, CPS 230 further details out the aspects to be covered under operational risk management review.

Information Security

CPS/SPS 234 and CPS 230 outline the same requirement to report an incident within 72 hours. These requirements overlap with notification requirements to regulators such as OAIC, ASX, AFP, ASIC which will need consideration.

Resolution Planning

CPS/SPS 900 links closely with CPS 230 around critical processes. CPS/SPS 900 critical functions though distinct from CPS 230 critical operations, do have elements that overlap. A broader linkage of CPS/SPS 190 with ICAAP/ ILAAP also needs consideration.

Critical Infrastructure Act

Cross over of the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) with CPS 230 relates to incident reporting, registration of critical infrastructure assets and the requirement to have a risk management program.

CPS 230 is designed to strengthen the management of Operational Risk and focuses on critical operations

CPS 230 will set out minimum standards for managing operational risk, including business continuity and service provider management. It will incorporate updated requirements for service providers and business continuity management, replacing CPS/SPS 231 and CPS/SPS 232.

For many organisations, the incoming Operational Risk Management regulations set out a new way of looking at how their business operates and interacts with the broader financial services ecosystem. As organisations engage with the new regime, we see several common challenges and pitfalls emerging.

The top 5 challenges for regulated entities

The top 5 challenges we see globally in the market concern both short- and medium-term implementation along with internal and external components.

01 Defining and modelling critical operations

- **What is a critical operation and how are they identified**
- What level of process modelling is required
- Driving end-to-end accountability across business units and entities

02 Understanding the risk, key data and controls

- **Mapping risk, control and obligations to the processes**
- Providing the board with a view of the critical business process risk and control environment, risk appetite, key indicators

03 Measuring resilience and disruption

- Defining metrics, testing, data quality, MI dashboards and tooling
- Defining the maximum period of disruption, incorporating the voice of the customer

04 Material Service Providers

- **Identifying material service providers for critical business processes.**
- **End-to-end resilience with ecosystem partners, influence over other parties, large service provider dependencies e.g. Technology and Cloud**

05 Embedding into BAU

- Investment prioritisation
- People Engagement
- True Board ownership
- Service ownerships
- Embedding Operational Risk into the DNA of all staff

CPS 230 key considerations

CPS 230 emphasises the integration of operational risk, business continuity management and service provider management. End-to-end oversight and accountability must be supported by the appropriate people, governance structures, technology, and service providers.

Frameworks & Policies

- Frameworks and Policies updated / aligned to CPS 230
- Creation of Integrated Resilience (Crisis Management, Incident Management, BCP and DRP)
- Development of operational frameworks and policies, and identification of critical operations
- Consideration towards overlapping standards including linkage to key prudential standards, policies and frameworks (e.g. SPS 515, CPS 231, SPS 220, SPS 250 and SPS 530)
- Change Management to manage changes in products (including investments and insurance), operations and services

Governance & Reporting

- Increased Board responsibilities to be incorporated into role accountabilities
- Enhanced decision making processes around service providers
- Ensuring that CPS 230 requirements are applied appropriately throughout the group (including connected entities that are not APRA regulated)
- Enhanced Board reporting, requiring supporting data & metrics from service providers (including administrators, insurers, financial advice providers, custodians and investment managers)
- Consideration of Member Outcomes, Business & Strategic Planning and Members' Best Financial Interests obligations in decision making

Operational Risk

- Mapping of operational risks, controls, issues and incidents
- Strengthening process for managing risk and controls across operating model
- Articulating difference between Risk Appetite and Disruption Tolerances where they diverge
- Comprehensive risk assessment for critical processes (including scenario analysis to assess impact of severe risk events)
- Prioritisation of residual risk for critical processes
- Ensuring Data Governance is fit for purpose for critical operations
- Tooling to monitor and report operational risk against risk appetite metrics and tolerances to the Board

Service Providers

- Maintenance of a comprehensive service provider management policy (including DD, tender & selection process, appointment, management and termination of material service providers)
- Increased obligations for service providers requiring review and renegotiation of service agreements
- Best financial interests termination clause
- Consideration of material risks associated with outsourced arrangements and related party arrangements
- Development of appropriate metrics to monitor performance of service providers (including outsourced and related party arrangements)
- Internal audit to review proposed outsourcing arrangements with a material service provider and regularly report to the Board / Audit Committee on compliance with service provider management policy

Operations and Technology

- Alignment of BCPs and DRPs to Critical Operations, including tolerances, testing and triggers
- Importance of understanding critical internal processes
- Opportunities to integrate Value Chains and critical processes for efficiency
- Complexity of identifying components of technology supporting critical operations
- Integration of BCP and DRP processes and assessments with operational risk management practices
- Review of notification processes around critical incidents and risk events that have a material financial impact to the fund
- Commercial implications of incorrectly set tolerances

Related Entities & Other

- Application and oversight of CPS 230 requirements to all related entities and associates, including offshore operations
- Designing the optimum Operating Model and ensuring appropriate capability (outsourced vs insourced)
- Criticality of Value Chain / Business Stakeholder engagement early given likely investments required
- Strengthening processes around managing actual / perceived conflicts of interests

Material Service Providers

Material service providers are those on which the entity **relies to undertake a 'critical operation'** or that **expose it to material operational risk**. They include third parties and related parties deemed to be material because of one or a number of arrangements with the APRA-regulated entity.

"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. Material service providers also include providers that manage information assets classified as critical or sensitive under CPS 234"

Draft CPS230

Considerations for Service Providers

Procurement & Risk Activities

Before entering into any contract there is likely to be enhanced due diligence requirements which include a detailed assessment of both financial and non-financial risks (including risks associated with geographic location or concentration of the service provider or the partied the service provider relies upon to provide the service) and an assessment of whether the providers is systemically important in Australia.

Fourth Parties & Sub-Contractors

Currently this is addressed through the use of an outsourcing contract where any subcontracting is the responsibility of the third-party service provider.
CPS230 requires that service providers assume liability for failure of a sub-contractor.

Contracts & Agreements

All service providers must be appointed by a formal and legally binding agreement. These agreements must require notification by the service provider of its use of other material service providers (through sub-contracting or other arrangements), for the service provider to take responsibility for its sub-contractors, force majeure provisions and termination rights.

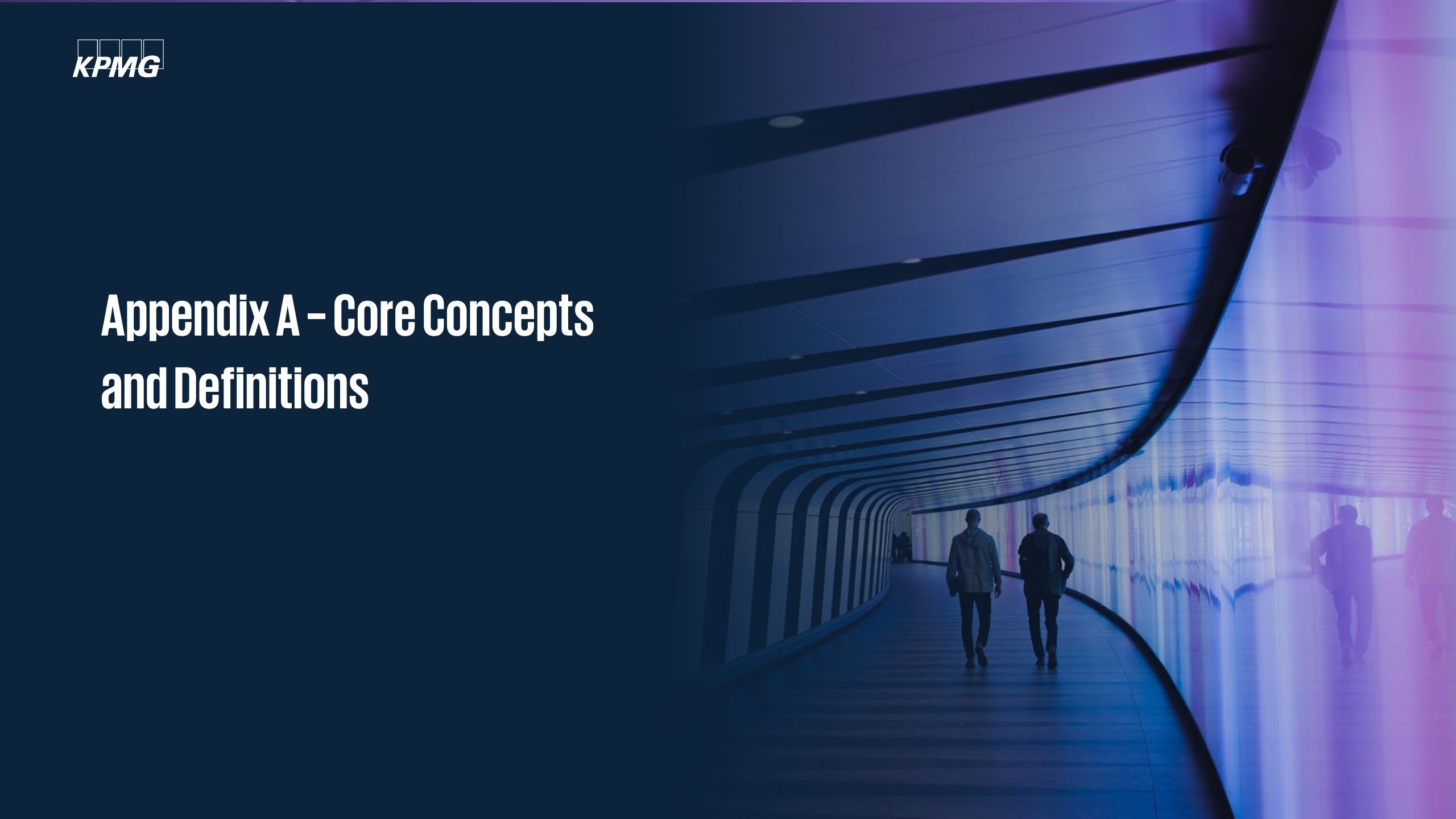
Ongoing Oversight

The implication of the changes proposed by CPS230 will most likely result in a combination of reporting obligations, the inclusion and exercise of rights to audit and test service provider systems, inclusion of service providers in simulations/tabletop exercises, and the continued requirement that third parties remain liable for any acts or omissions of their subcontractors.

Questions / Comments

KPMG

Appendix A – Core Concepts and Definitions



Draft CPS 230 - Key concepts and definitions

Core concept	Definition / explanation
Operational Risk (Draft CPS 230 @ para 23)	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, reputational risk and change management risk.
Critical Operations (Draft CPS 230 @ paras 34-36)	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. For the purposes of this Prudential Standard, critical operations include, but are not limited to: • payments • deposit-taking and management • custody • settlements • clearing • claims processing • investment management • fund administration • customer enquiries, and • the systems and infrastructure needed to support these operations. APRA may require an APRA-regulated entity, or a class of APRA-regulated entities, to classify a business operation as a critical operation.
Material Service Provider (noting that the definition is different and broader than SPS 231) (Draft CPS 230 @ paras 49-50)	Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. 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 Material service providers also include providers that manage information assets classified as critical or sensitive under CPS 234.

Contacts

Gavin Rosettenstein
Partner, Operational Risk & Service Provider Risk Management

T: +61 413 956 179
E: gavin1@kpmg.com.au

Kat Conner
Partner, Insurance Risk & Regulation

T: +61 438 057 483
E: katconner@kpmg.com.au

Campbell Logie-Smith
Director, Business Continuity & Resilience

T: +61 422 050 021
E: clogiesmith@kpmg.com.au

kpmg.com/socialmedia