Managing CPS 230 Requirements

A Guide for APRA-Regulated Entities and Financial Institutions

Camms.

Software to Change Tomorrow.

What is CPS 230?

CPS 230 is a Prudential Standard for Operational Risk Management introduced by the Australian Prudential Regulation Authority (APRA). It is due to become mandatory for all APRA-regulated entities on 1 July 2025 - affecting the banking, insurance, and superannuation industries. This new standard is designed to empower organisations to effectively manage operational risks and ensure business operations can continue during a crisis.

CPS 230 will act as a roadmap for best-practice risk management and long-term operational resilience. It sets out clear guidelines for companies to identify, assess, and manage operational risk, effectively manage the risks associated with suppliers & service providers, and be able to continue its critical operations throughout a disruption with effective business continuity plans.

The APRA CPS 230 standard sets out a clear framework for companies to effectively identify, assess, and manage operational risks. By proactively addressing these risks, companies can minimise disruptions, safeguard their financial well-being, and ultimately, ensure continued service delivery to their customers.

CPS 230 is all about building a fortress against disruption. It will empower companies to anticipate potential threats, develop effective mitigation strategies, and bounce back quickly from unexpected events. This translates to a more stable and reliable organisation, fostering trust with stakeholders and regulators alike. CPS 230 represents a proactive approach to risk management, it recognises and elevates operational resilience as a critical pillar of stability within Australia's financial services sector.

Why was CPS 230 introduced?

The financial services sector is vital to critical infrastructure and any instability can severely impact the finances of individuals, companies, and the entire economy. New technologies, cyber threats, system downtime, economic fluctuations, and even natural disasters can all pose a significant operational risk to companies and must be carefully managed to ensure the sector remains operational. Prior to CPS 230, regulations surrounding operational risk management were fragmented and varied across different industries. This created a landscape where potential vulnerabilities could go unnoticed, potentially leading to avoidable disruptions and financial losses.

Recognising this gap, APRA saw the need for a more comprehensive approach to operational risk management; following which, CPS 230 was introduced. Here are some of the key reasons APRA introduced CPS 230:

1 To strengthen operational risk management

CPS 230 establishes a comprehensive and standardised approach to managing operational risk, as it takes a broader view ensuring all APRA-regulated entities have a robust framework in place to identify, assess and mitigate potential risks. This holistic approach aims to build stronger organisational resilience, allowing companies to not only recover from disruptions, but also prevent them in the first place through proactive risk management.

2 To enhance business continuity

To comply with CPS 230 requirements organisations must be able to continue their operations during a crisis or unexpected event with credible business continuity plans. This translates to minimal service interruptions for customers and protects the overall health of the organisation.

3 To increase oversight and transparency

CPS 230 provides APRA with greater visibility into the operational risk management practices of regulated entities. This allows for more consistent processes and informed oversight - ensuring companies are taking the necessary steps to safeguard their operations to protect critical infrastructure.

4 To promote a culture of risk awareness

The implementation of CPS 230 fosters a culture of risk awareness within organisations, as it encourages employees at all levels to be vigilant and proactive in identifying and mitigating potential operational risks.

5 To reduce third party risk

Most organisations rely heavily on a network of third-party service providers which can pose additional risk to an organisation. CPS 230 introduces stricter requirements for managing these relationships and the associated risks. Companies will need to conduct thorough due diligence on service providers to manage vendor risk and monitor vendor performance using relevant policies, procedure documents, and robust monitoring.

6 To future-proof the industry

CPS 230 aims to equip institutions with a flexible framework that can manage the operational risks associated with new technologies and emerging threats. By fostering a culture of risk awareness and continuous improvement, companies can ensure they remain prepared for whatever the future holds.

Who needs to comply with CPS 230?

CPS 230 applies to a wide range of organisations operating within the Australian financial landscape. If you're operating in the Australian financial services sector and fall under the purview of the Australian Prudential Regulation Authority (APRA), then compliance with CPS 230 is mandatory from 1 July 2025. CPS 230 is relevant to a broad spectrum of entities within the Australian financial services sector including but not limited to:

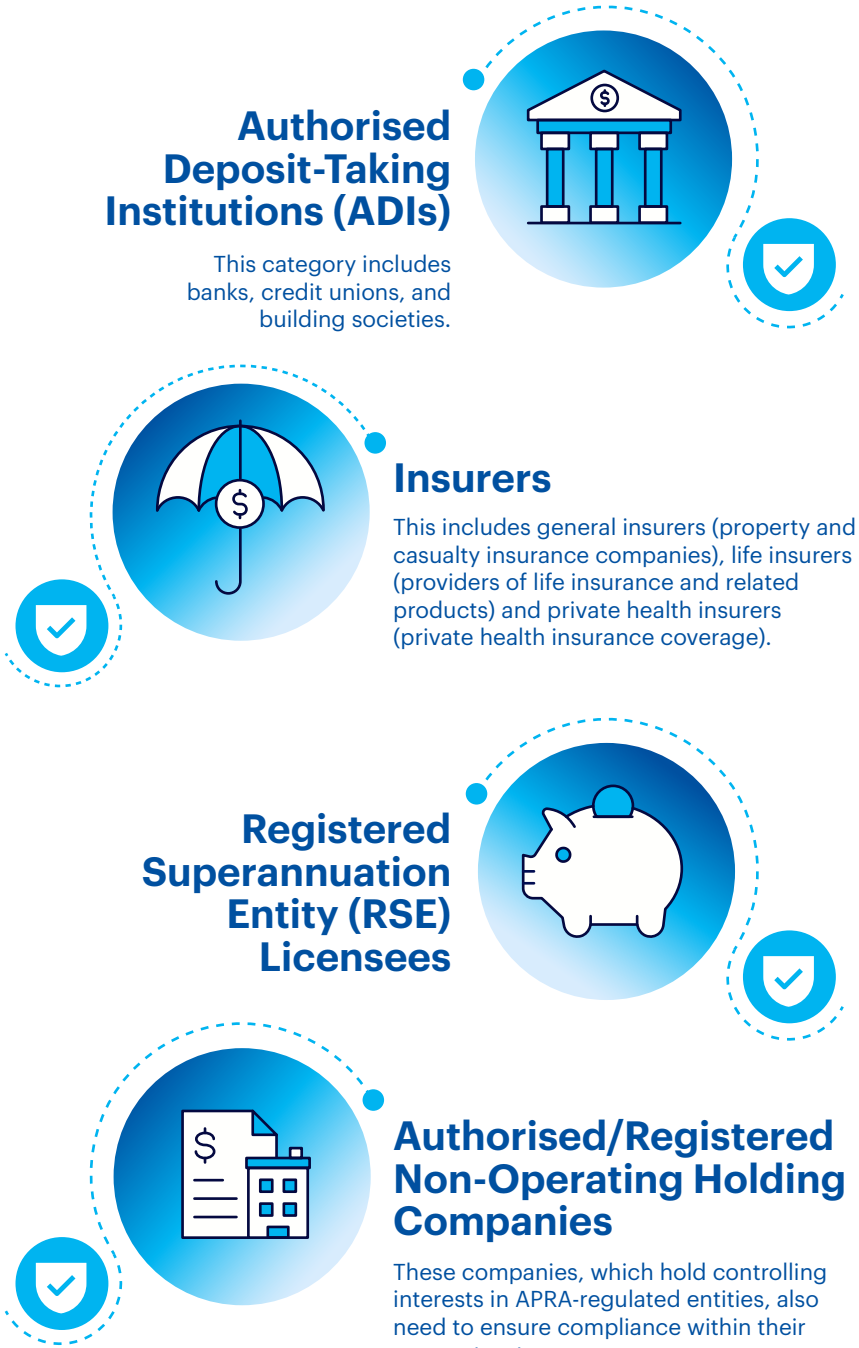
1. **Authorised Deposit-Taking Institutions (ADIs):**
   This category includes banks, credit unions, and building societies.

2. **Insurers:**
   This includes general insurers (property and casualty insurance companies), life insurers (providers of life insurance and related products) and private health insurers (private health insurance coverage).

3. **Registered Superannuation Entity (RSE) Licensees**

4. **Authorised/Registered Non-Operating Holding Companies:**
   These companies, which hold controlling interests in APRA-regulated entities, also need to ensure compliance within their group structure.

It's important to note that the reach of CPS 230 extends beyond just the core regulated entities. So even if your organisation isn't directly regulated by APRA, you may still be indirectly impacted by CPS 230. This is because many APRA-regulated entities rely on third-party service providers. If your company falls into this category and provides services (directly or indirectly) to APRA-regulated entities, you may need to adapt your own risk management practices to align with the expectations outlined in CPS 230.



Authorised Deposit-Taking Institutions (ADIs)

This category includes banks, credit unions, and building societies.

Insurers

This includes general insurers (property and casualty insurance companies), life insurers (providers of life insurance and related products) and private health insurers (private health insurance coverage).

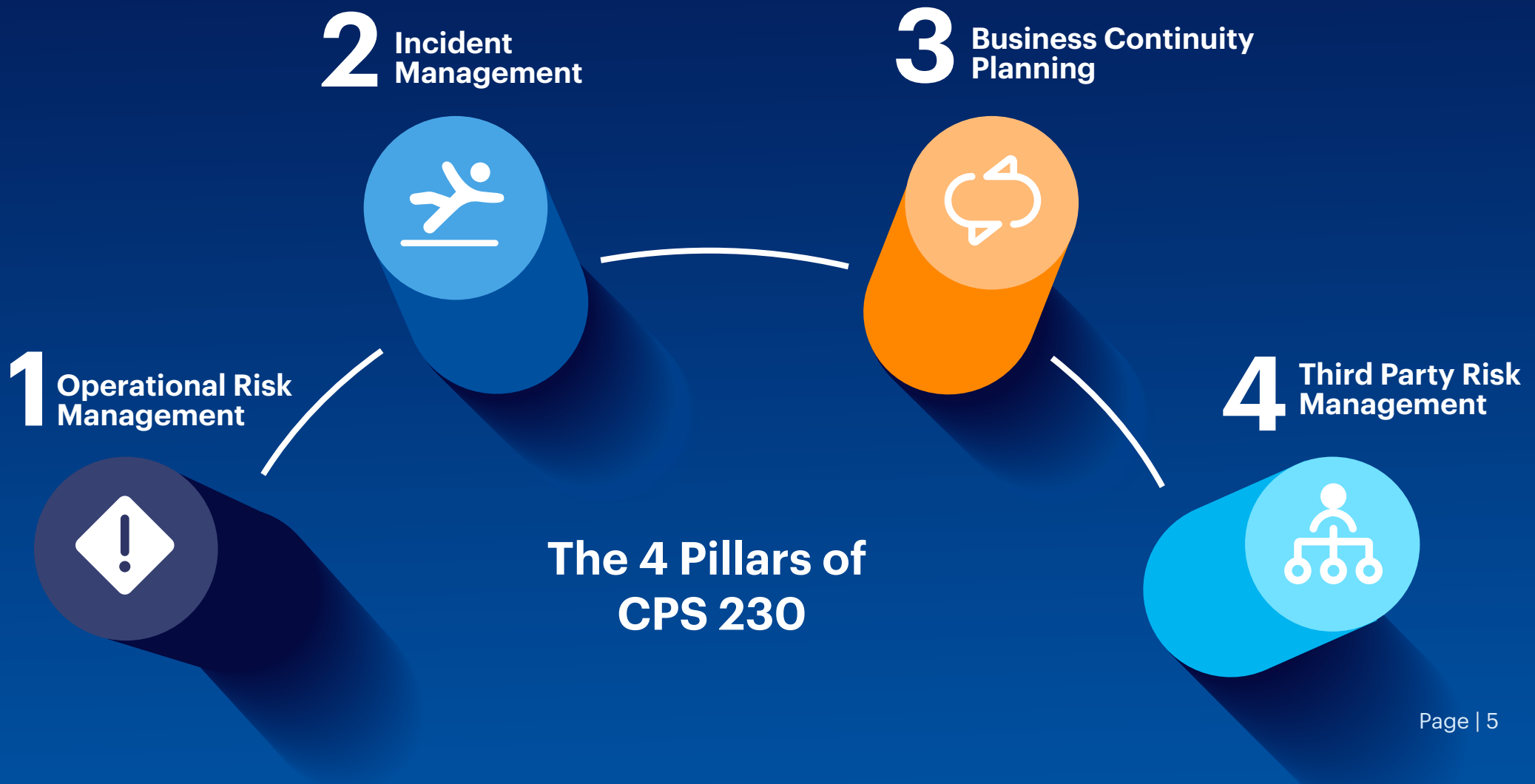
Registered Superannuation Entity (RSE) Licensees

Authorised/Registered Non-Operating Holding Companies

These companies, which hold controlling interests in APRA-regulated entities, also need to ensure compliance within their group structure.

The 4 pillars of CPS 230 for Operational Risk Management

CPS 230 isn't just a set of rigid rules; it's a framework built to ensure sound operational risk management, business continuity planning and third-party risk management. CPS 230 establishes a clear set of rules that guide APRA-regulated entities in their approach to operational risk management. By understanding and adhering to this guidance, APRA-regulated entities can build a robust framework to identify, assess, and mitigate potential risks and ensure long-term operational resilience.



Here we explore the key pillars underpinning CPS 230 and detail how GRC software can support firms to structure their processes in line with the requirements:

1

Operational Risk Management

CPS 230 states that firms must "**Identify, assess and manage its operational risks, with effective internal controls, monitoring and remediation**". CPS 230 highlights the need for a systematic approach to identifying and assessing operational risks. By gathering and analysing data, companies gain a clear understanding of their risk landscape, enabling them to make informed decisions based on factual insights.

To align with the operational risk management requirements outlined in CPS 230 firms must:

Identify & Address Risk

To align with the operational risk management requirements outlined in CPS 230, firms must identify and address operational risks before they cause disruptions. To do this, firms would need to establish an active risk register to pinpoint potential threats and evaluate the likelihood of each risk occurring and the potential severity of its impact.

Risk assessments & Risk Monitoring

Companies will need to carry out regular risk assessments, questionnaires, and surveys and assess operational data to monitor risk levels. In addition, businesses would need to establish a risk appetite with clear tolerance levels and monitor risk levels to ensure they remain within the desired boundaries. The standard recognises that different organisations have varying risk tolerances.

Internal Controls

Organisations must implement a strong system of internal controls to mitigate operational risks. This requires companies to design, implement, monitor, and regularly test their controls to ensure they are effective.

Continuous Improvement

Operational risk management is an ongoing process, not a one-time fix. The CPS 230 standard encourages companies to continuously monitor and improve their risk management practices, adapting to evolving threats and regulatory requirements.

Sound Governance and Culture

The standard underscores the importance of strong governance and a culture of risk awareness within organisations. Effective leadership, clear communication, and employee engagement are all crucial for successful CPS 230 implementation.

2

Incident Management

Effectively managing and resolving incidents is essential for best-practice operational risk management and ongoing operational resilience.

To align with CPS 230 requirements firms must:

Establish a robust incident reporting process

Meeting CPS 230 requirements requires a robust incident reporting process where incidents can easily be logged, categorised, and escalated appropriately.

Investigate and resolve incidents

The standard mandates clear protocols for, investigating, and managing operational incidents through to resolution. Firms should establish investigation templates and carry out root cause analysis to determine the cause of incidents.

Report on Incidents

CPS 230 recognises the importance of learning from incidents that do occur. For a best-practice approach, firms should regularly report on incidents to understand the causes of incidents and identify trends and patterns to prevent recurrence.

Understand the correlation between risk and incidents

Those following CPS 230 guidelines should link incidents back to the originating risks to ensure future occurrences are prevented with the relevant risk-based controls.

3

Business Continuity Planning

The ability to respond effectively to disruptions is critical for maintaining operational resilience. Therefore, CPS 230 points out the importance of robust business continuity planning (BCP) to ensure companies can swiftly recover from unexpected events and minimise service interruptions during challenging times.

To align with the business continuity aspects of CPS 230 firms must:

Build a Business Process Register

To align with CPS 230 requirements, firms should build a business process register to capture each critical business process and the systems and staff involved. Firms should capture critical details about the impact when that process goes down and clearly define recovery time objectives (RTO's).

Perform Business Impact Assessments

To meet CPS 230 requirements, firms should conduct regular business impact assessments (BIAs) to understand the impact on operations if that process were to fail.

Formulate Active Business Continuity Plans

Firms should have a fully documented Business Continuity Plan for each critical process identified in the business process register. Firms should also have a structured way to instigate those plans and track their progression and status when they are 'triggered' by an incident – this should include a process for mass notifications and plan progression status tracking.

Scenario Analysis and Stress Testing

By employing scenario analysis and stress testing, companies can proactively anticipate the impact of potential disruptions – helping to identify gaps in BCM plans. This forward-thinking approach involves simulating a range of plausible but severe events and uncovering potential vulnerabilities in systems and processes. By identifying these weaknesses beforehand, companies can proactively develop mitigation strategies, ensuring they are well-equipped to handle disruptions before they occur, pushing organisations to move beyond reactive risk management.

Business Process Modelling

Firms should use business process modelling to explore each of their critical business processes in detail and understand dependency mapping. This will help leaders to understand critical details around the FTE's required, cost, generated revenue, SLAs, KPI's, and industry benchmarks for each process - and the impact when the process fails - paving the way for continuous improvement. It not only helps firms to understand the impact when a particular process goes down, but organisations can use this functionality to perform service efficiency reviews to identify areas of improvement and seek out areas of duplicated time & effort.

4

Third Party Risk Management

According to CPS230 guidance, organisations must effectively manage the risks associated with service providers, with a comprehensive service provider management policy, formal agreements, and robust monitoring – making third-party risk management a top priority.

To meet CPS 230 requirements from a third-party risk management perspective, firms must implement a best practice third party risk management programme, this includes:

Creating a vendor register

Firms must create an online vendor register - creating a profile for each vendor - capturing critical details around, costs, contract, key contacts, Service Level Agreements (SLAs), and Key Performance Indicators (KPIs).

Performing vendor benchmarking & Analysis

Firms should use risk intelligence providers to get real-time updates on supplier finances, sustainability ratings, sanctions listings, and cybersecurity rankings to understand the potential threats from each vendor.

Vendor risk assessments

Firms should carry out regular vendor risk assessments to capture critical details about each supplier and monitor their performance regularly.

Formalised Onboarding & Offboarding

Firms should have a clear process for onboarding and offboarding clients ensuring they are not tied into any unexpected contract requirements and making sure adequate due diligence is carried out on each new vendor.

Performance monitoring

Firms should monitor the ongoing performance of each vendor - making sure they are performing in line with the agreed SLAs and KPIs in their contract. Issues should be logged and addressed to prevent vendor risk from escalating. This encourages a forward-thinking approach that prioritises risk mitigation and contingency planning.

How can GRC software support organisations to operate in line with CPS 230 requirements?

With so many requirements, the introduction of CPS 230 by APRA can be a complex undertaking – especially for those relying on manual processes and spreadsheets.

Implementing GRC software relieves the burden of CPS 230 compliance. These solutions offer best practice frameworks for operational risk management, third-party risk management, incident management, and business continuity planning - straight out-of-the box! When it comes to CPS 230, GRC software shines - transforming CPS 230 compliance from a burden into a strategic advantage.

Here's how GRC software can support with the 4 core pillars of CPS 230 compliance.

Operational Risk Management

GRC software offers a best-practice approach to operational risk management that aligns with CPS 230 requirements. Firms can use the software to build an online digital risk register to log each risk - capturing critical details around its categorisation, likelihood, severity, and impact - using a standardised framework.

GRC software also automates the risk assessment process in line with CPS 230 requirements. Risk assessments are rolled out via automated workflows - staff simply complete online risk assessment forms with all details feeding directly into the platform – building a complete picture of risk exposure. API integrations with other internal systems and data sources can pull live operational data into the GRC platform - enabling firms to further monitor risk levels by looking at a centralised view of live operational data within the platform – providing ample data to build a clear view of risk exposure.

GRC software automates & centralises the collection & analysis of risk data, allowing firms to identify potential threats across all departments and business functions in alignment with CPS 230 recommendations. This data becomes the foundation for setting a risk appetite and tolerance levels (the acceptable amount of risk before intervention becomes necessary). Teams can use the software to set Key Risk Indicators (KRIs) and define a risk appetite to ensure the organisation is operating within the desired risk levels - automated notifications are sent when the risk levels spike – alerting key stakeholders. By integrating risk appetite and tolerance levels, the software can highlight risks that exceed your company's comfort zone, prompting immediate mitigation strategies.

Risk management isn't just about identifying threats; it's also about building a bullet-proof barrier against them. CPS 230 states that firms must have sufficient controls in place to mitigate unwanted risk and keep risk levels within the agreed risk appetite. GRC software helps establish robust internal controls and monitoring processes - facilitating the design, documentation, and implementation of these controls. Firms can build a control register within the GRC platform. Each control can be linked to the relevant risk in the risk register.

Automated workflows can be used to carry out regular control testing and automated control monitoring to ensure the controls are effective. Automated workflows ensure consistent implementation of these controls, while real-time dashboards provide a clear view of their effectiveness. This allows for continuous monitoring and adjustments, ensuring your defences remain strong. The automated control monitoring features within the platform continuously assess the effectiveness of controls, keeping you informed and allowing for proactive adjustments.

GRC software uses workflows to automate the entire risk escalation, treatment, and remediation processes - capturing key actions and providing a complete audit trail of how each risk was treated and when. These transparent, best-practice processes enable an organisation to align its risk management programme with CPS 230 operational risk requirements. Automated reporting and data visualisation tools keep leadership informed, while communication features promote collaboration across departments.

The platforms also offer a wealth of reporting outputs, from risk register summaries and risk exposure reports, to heat maps, bowtie analysis, and Microsoft Power BI dashboards. These tools eliminate time consuming risk reporting, leaving risk teams with more time to analyse risk data – enabling them to advise the business on the best course of action and implement meaningful change.

GRC software provides a structured framework for capturing, classifying, and analysing potential risks across your organisation in line with CPS 230 guidance. This allows for a deep understanding of an organisations risk landscape, enabling firms to prioritise risk effectively and allocate resources strategically.

Sound governance and a culture of risk awareness are essential pillars of CPS 230 compliance. GRC software empowers this journey. It also facilitates clear communication and collaboration across departments, ensuring everyone is on the same page when it comes to risk identification, mitigation, and reporting. This transparency and engagement builds a culture where everyone plays a role in identifying, mitigating, and learning from risks; becoming active participants in safeguarding the organisation.

Incident Management

CPS 230 outlines the importance of comprehensive incident reporting with a view to get visibility of incidents and resolve them quickly to ensure operations continue. Here, GRC software shines again. Incident reporting becomes streamlined, with a centralised platform for capturing details, assigning ownership, and tracking resolution - thereby fostering a structured approach to incident reporting & management.

Teams simply log any incidents, hazards, or near misses via an online incident portal using digital forms with pre-configured fields based on the incident type selected. Once an incident is logged, an automated workflow escalates it to the relevant stakeholders for resolution. A case management workflow is opened for each incident enabling staff to log any actions and tasks that were undertaken to resolve the incident, and everything is date and time stamped and can be traced back to the user.

Many GRC platforms offer external online portals for capturing incident data from third parties and suppliers that could impact operations. These online portals are also great for anonymous incident reporting for sensitive matters like whistleblowing and sexual harassment and misconduct.

Learning from incidents is crucial for CPS 230 compliance. GRC software facilitates detailed analysis, uncovering root causes and informing future mitigation strategies and controls. This continuous improvement cycle ensures your organisation becomes more resilient with each challenge overcome. Disruptions are inevitable. The key lies in learning from them. The platform also facilitates communication and collaboration across teams, fostering a culture of shared learning and continuous improvement.

Business Continuity Planning

CPS 230 contains clear guidance about being able to continue critical operations within tolerance levels throughout severe disruptions with a credible business continuity plan. Many GRC software platforms offer business continuity planning functionality making it easy to structure processes that align with the CPS 230 best-practice requirements.

Business continuity planning thrives with GRC software. By centralising critical operational data and recovery procedures, GRC software empowers organisations to bounce back quickly from disruptions, minimising service interruptions for customers.

Firms identify their critical business procedures and build a business process register. A BCM plan is created for each critical process capturing detailed step-by-step plans, timescales, Recovery Time Objectives, and stakeholders – ensuring plans are deployable when needed. Teams can roll out Business Impact Assessments (BIAs) in the platform using digital forms sent out via automated workflows. This helps teams understand the impact of any downtime and any dependencies.

Many BCP solutions also offer business process modelling - enabling teams to understand critical processes and perform benchmarking against industry standards. This enables teams to understand the impact of unexpected events in terms of employees affected, man hours lost, and impact on cost and revenue – helping them to prioritise areas with the highest impact. Business process modelling can also be used to identify gaps in your current processes and support continuous improvement efforts.

BCM software can also support firms to carry out scenario and stress testing. By simulating a range of disruptive events, you can identify potential weaknesses in your systems and processes before they become real-world problems. Armed with this foresight, you can proactively develop mitigation strategies and contingency plans, bolstering your overall resilience in the face of unexpected challenges.

When a crisis strikes, BCM software triggers your BCM plans with mass notifications and automated workflows, and you can monitor BCM plan progression every step of the way and address any risks or issues.

Anticipating potential disruptions is a cornerstone of CPS 230. GRC software augmented with BCM capabilities allows you to map critical operations and identify the risks associated with them. By prioritising risk management efforts in these areas, you ensure maximum protection for your core business activities - minimising downtime and safeguarding critical operations.

Third Party risk management

CPS 230 states that firms must effectively manage the risks associated with service providers, with a comprehensive service provider management policy, formal agreements, and robust monitoring. Most GRC software platforms offer third party risk management as part of their wider GRC capabilities.

These solutions enable staff from across the organisation to build an online 'vendor register' to keep a record of any existing or potential vendors or third parties. Staff use online forms for vendor onboarding - capturing critical details regarding contract length, cost, relationship owner, supplier contacts, and any SLA's or KPI's. A formal offboarding process is also established to ensure contracts end smoothly.

Once this database is completed, staff can use the platform to monitor the risk associated with each vendor. Vendor risk assessments, questionnaires, and surveys can be carried out using online forms with all data feeding into the supplier profile in the platform. Vendors can even complete assessment forms themselves using an external online vendor portal – cutting out paper forms and emails.

Many vendor risk solutions link to third party risk intelligence providers. This enables firms to conduct benchmarking and score-carding against industry standards to understand potential risks posed by vendors. These systems check key details regarding financial stability, credit ratings, any previous compliance breaches & fines, any operational risks, supply chain risks, data breaches, insurance claims, any reputational issues, previous news stories, and company history & ownership details. The detail of these checks is linked to each vendor profile in the platform - building a complete picture of potential risk exposure. These checks are continuously run to ensure any new issues are captured and flagged as circumstances change throughout each vendors lifecycle.

Some third-party risk management solutions allow you to pull in live transactional & operational data - relating to supplier performance - into the tool from other systems & data sources via APIs. This allows risk teams to automatically monitor supplier performance against the agreed KPI's and SLA's. Teams can set rules to send notifications when supplier performance drops below the tolerable levels - enabling them to address any issues with the supplier promptly so they can be resolved.

Potential risks relating to each vendor can be logged in an online 'vendor risk register' within the platform and mapped to the relevant vendor. Firms can then monitor risk levels using the results from risk assessments, vendor intelligence checks, and any operational data pulled into the platform via APIs. Firms can then set various controls to lower risk levels. Risk teams can build a control library within the platform and carry out regular control checks & testing to make sure the controls are effective in reducing risk.

The third-party risk dashboards & reports available within the solutions give risk teams complete oversight of each vendors performance and any potential problems. With all this information stored centrally and easily accessible, the software automatically creates a fully auditable vendor selection process.

A fully functioning third-party risk management process facilitated by GRC software makes it easy for decision makers to compare vendors and make important decisions regarding vendor selection. Vendor risk management tools provide a holistic view of the overall vendor risk landscape in an organisations' supply chain - highlighting potential risks, weaknesses, and performance issues - allowing firms to resolve issues promptly - ensuring they are working with a network of reliable vendors.

Providing Proof of Compliance with CPS 230

To achieve compliance with CPS 230, it's not enough to have a risk management programme, a third-party risk programme, and business continuity plans - organisations must provide proof of the effectiveness of those processes to regulators. GRC software can support firms to demonstrate compliance with CPS 230 requirements through best-practice regulatory compliance functionality.

Teams can set up an 'obligations library' - capturing all the requirements outlined in CPS 230, and implement workflows, step-by-step processes, and checks to monitor compliance with the requirements. This empowers firms to identify and address any compliance gaps proactively. The process is fully documented, and automated reporting outputs can provide proof of compliance to regulators.

Regular audits are essential for ensuring adherence to CPS 230. The audit capabilities available in GRC software can also simplify this process by allowing you to plan and schedule internal & external audits, assign tasks, and track findings & audit outcomes.

Conclusion

CPS 230 isn't just a set of compliance requirements; it's a proactive approach that prioritises risk identification, mitigation, and continuous improvement. By adhering to its principles, companies can build a fortress against disruptions, fostering trust with stakeholders and ensuring uninterrupted service delivery to their customers. CPS 230 is designed to empower APRA regulated entities to effectively manage operational risks and safeguard their long-term stability.

Achieving CPS 230 compliance isn't a one-time event; it's an ongoing journey. Implementing dynamic operational risk management, vendor risk management, and formulating business continuity plans that meet CPS 230 requirements can be daunting and doesn't happen overnight. But by using GRC software, firms can fast-track their way to CPS 230 compliance.

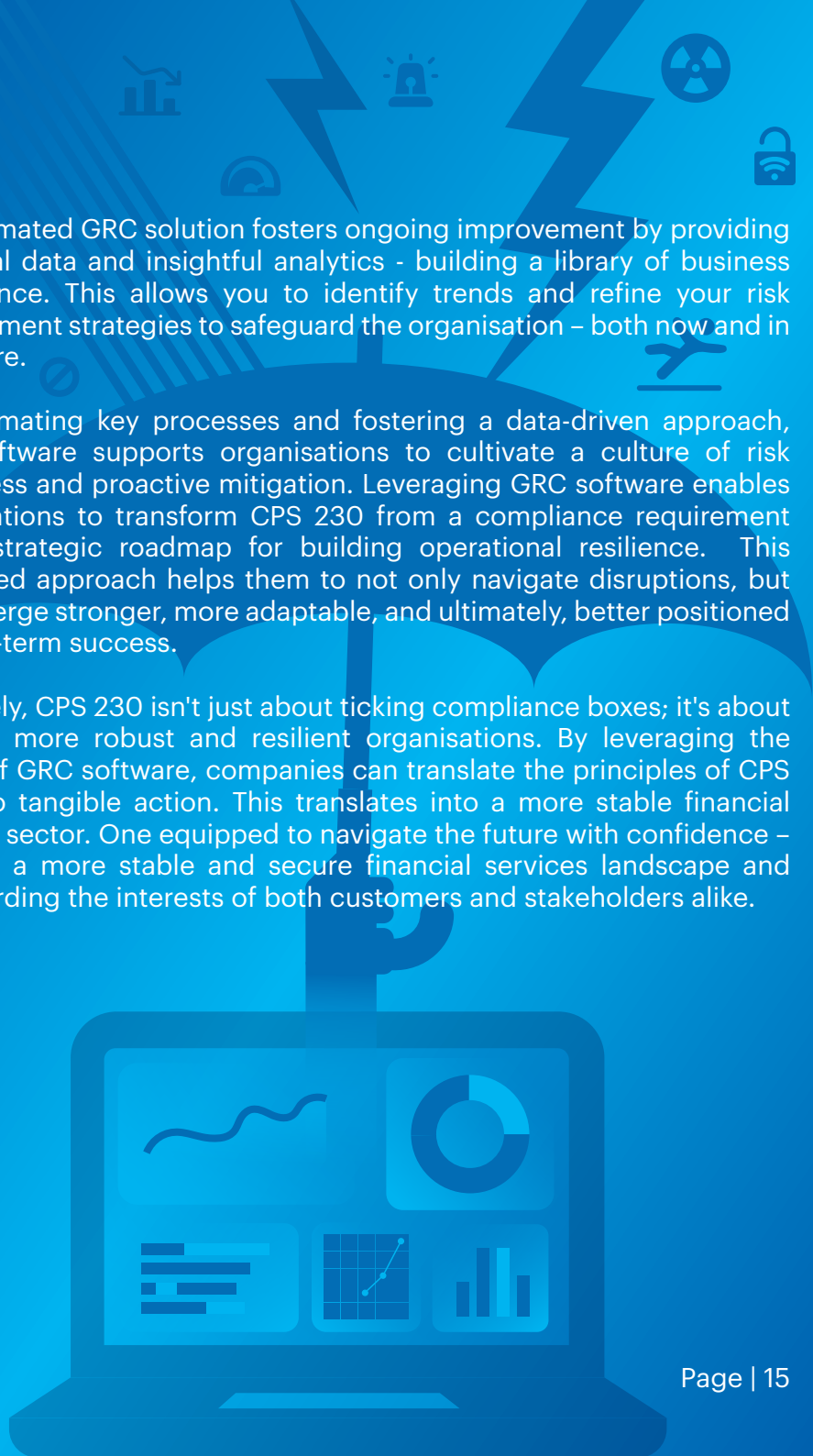
When it comes to CPS 230, GRC software emerges as a powerful ally - offering best-practice frameworks to implement processes that align with CPS 230 requirements. Imagine a platform that streamlines and automates every aspect of CPS 230 requirements including; operational risk management, third-party risk management, business continuity planning, scenario & stress testing, and incident management. The platform automates data collection and analysis through insightful reports, painting a clear picture of the overall risk landscape. This comprehensive view empowers organisations to prioritise risks effectively and allocate resources strategically.

GRC software empowers organisations to not just meet CPS 230 compliance requirements, but to add real value to their organisation - cultivating a culture of risk awareness & proactive mitigation, paving the way for long term operational resilience. These software platforms ensure everyone plays a role in identifying, mitigating, and learning from risk. This collaborative approach fosters a proactive environment where disruptions are anticipated and addressed before they escalate into major issues.

An automated GRC solution fosters ongoing improvement by providing historical data and insightful analytics - building a library of business intelligence. This allows you to identify trends and refine your risk management strategies to safeguard the organisation – both now and in the future.

By automating key processes and fostering a data-driven approach, GRC software supports organisations to cultivate a culture of risk awareness and proactive mitigation. Leveraging GRC software enables organisations to transform CPS 230 from a compliance requirement into a strategic roadmap for building operational resilience. This integrated approach helps them to not only navigate disruptions, but also emerge stronger, more adaptable, and ultimately, better positioned for long-term success.

Ultimately, CPS 230 isn't just about ticking compliance boxes; it's about building more robust and resilient organisations. By leveraging the power of GRC software, companies can translate the principles of CPS 230 into tangible action. This translates into a more stable financial services sector. One equipped to navigate the future with confidence – creating a more stable and secure financial services landscape and safeguarding the interests of both customers and stakeholders alike.



About Camms.

Camms offers a powerful GRC platform that can be specifically configured to align with the requirements of CPS 230.

Key capabilities include:

Risk Management

Establish a digital risk register and roll out risk assessments and control checks online - with all data feeding into the platform. Set up a control framework to successfully reduce unwanted risk. Monitor risk levels against KRI's and your risk appetite. Use automated workflows to escalate risk and implement risk treatment actions. Access dashboards & reports to understand key actions and provide a holistic view of risk. Link risk to your strategic objectives to achieve your goals.

Incident Management

Report incidents, near misses, and emerging risks via online incident forms that feed directly into the platform. Use automated workflows to conduct investigations, determine impact, perform route cause analysis, and monitor cases until closed. Use reports & dashboards to spot trends and introduce controls to reduce reoccurrence and link incidents back to the originating risks.

Third Party Risk Management

Build an online library of all your vendors - capturing critical details regarding contract, pricing, SLAs, and KPIs. Monitor supplier performance. Formalise the onboarding and offboarding process. Use Benchmarking and scorecards to rate and select vendors and understand any potential threats.

Business Continuity Planning

Identify business critical processes and build a business process register. Create best-practice BCM plans linked to each critical business process and conduct regular Business Impact Assessments (BIAs). Conduct business process modelling and carry out scenario and vulnerability testing. Activate BCM plans based on incidents logged and track recovery progression.

Compliance

Build a comprehensive obligations library of relevant regulations, legislation, policies, and internal procedures – including CPS 230 - and monitor compliance. Implement a best-practice regulatory change management workflow. Receive notification of upcoming regulatory changes from your preferred content provider. Implement a best-practice policy management process. Introduce best-practice compliance processes for conflicts of interest, sanctions checks, bribery & corruption, anti-money laundering, disclosures, whistleblowing, gifts & hospitality, and feedback & complaints.

Audits & Inspections

Schedule and manage internal and external audits – including your CPS 230 audit. Formalise the results and use automated workflows to implement the required actions. The platform provides a complete history of all your audits and their findings and any outstanding actions or compliance failures.

Cyber & IT Risk Management

Build a cyber risk register, monitor cyber risk, and implement the relevant controls. Access frameworks to ensure compliance with data privacy regulations like CPS 234, ISO 27001, GDPR & NIST. Manage & resolve cyber incidents.

ESG

Plan out an environmental, social and governance (ESG) strategy and monitor progress. Manage ESG related risks, incidents, and compliance obligations. Confidently report on the progress of key metrics and ESG initiatives.

Workplace Health & Safety

Maintain workplace health & safety registers, identify & address hazards, and create & track actions to resolve issues. Staff can report incidents, log hazards & near misses, and carry out safety checks via the mobile app.

Benefits include:

- Highly configurable
- API Integrations
- Automated workflows & alerts
- Effortless reporting
- Enhanced collaboration
- Better visibility
- Clear insights to support decisions
- Integrated GRC

Discover How Camms Is Supporting Organisations to Meet CPS 230

Find out how the Camms cloud-based GRC platform supports organisations to structure processes in line with CPS 230 requirements to effectively manage operational risk, mitigate third-party risk, and resolve incidents to keep operations running in a crisis.

Digitise your risk management process, resolve incidents, monitor compliance, administer policies & regulations, implement robust business continuity plans, and roll out your corporate strategy – all within one platform.

Structure your GRC processes to meet CPS 230 requirements with ease and provide proof of compliance to regulators with insightful dashboards and reports.

Empower your organisation to navigate the complexities of CPS 230 - paving the way for a more resilient and compliant future.

Visit Website **Request Demo**

Camms.

Software to Change Tomorrow.