



Risk transformation and the intersection with business transformation

Risk maturity is a measure of an organisation's risk management capabilities and culture. As organisations raise their risk maturity, it enhances elements across governance and framework, processes, people and organisations, methodologies, systems and data at different speeds. This article is the second in a [two-part series on business and risk transformation](#), prompted by Australia's current regulatory environment. Here, we dive into some of the effective approaches organisations take when uplifting the design of their risk management, and the synergies they have with business transformation.

One of the fundamental areas to start driving change is through an organisation's framework. As an organisation matures, it is expected to have an Enterprise Risk Management Framework (ERMF) that continues to be fit-for-purpose and cover the latest and emerging risk-related trends. The framework typically encompasses details around the risk management strategy, risk appetite, and clarity around the three lines of defence. Organisations also have continuous review and monitoring of supporting policies, standards, guidelines, handbooks and other tangential material.

Organisations that may be further along in their maturity come to recognise the importance of addressing product-related issues and incidents through uplifting risk fundamentals. Since the Australian Securities and Investments Commission's Design & Distribution Obligations and Product Intervention Powers went into effect,¹ ASIC-regulated entities have invested more into product remediation programs, monitoring programs, and enhancing rigour around the product management lifecycle. They have been taking the opportunity to identify risks across the end-to-end product value chain and enhance controls and product risk management practices where practicable.






Risk culture is another key area for organisations. This may entail an evaluation of existing performance metrics, incentive structures, and assessment of whether desired risk behaviours are rewarded and/or what the consequences would be for misconduct and/or non-desirable risk behaviours. Entities regulated by the Australian Prudential Regulation Authority (APRA) should utilise guidance from APRA's Risk Culture 10 Dimensions, which takes into account aspects across risk architecture and risk behaviours including leadership, decision-making and challenge, and communication and escalation.²

¹ Australian Securities and Investments Commission "RG274 Product Design & Distribution Obligations".

² Australian Prudential Regulation Authority "Risk Culture 10 Dimensions," Accessed 16 August 2023.

Enhancing the Design of Risk Management

Below are areas organisations should consider.

Elements	Risk Management Design Sample Focus Areas
 <p>Governance & Framework</p>	<p>Risk management framework</p> <ul style="list-style-type: none"> • Governance structure, supporting documents, and accountabilities <p>Risk management strategy</p> <ul style="list-style-type: none"> • Transparency around methodologies and procedures for current and emerging risks across the organisation • Value chain governance and how to respond to market opportunities • Governance decisions for risk assumptions, constraints, priorities, tolerance, etc. <p>Risk appetite framework and statement</p> <ul style="list-style-type: none"> • Risk taxonomy, metrics and tolerances consistently applied across artefacts • Risk reporting across divisions that aligns back to the divisional and group risk appetite statement to ensure the right quantitative data and qualitative insights are being reported in the respective forums • Continual monitoring of risk categories and events as part of the risk taxonomy <p>Governance forums, accountability and decision-making</p> <ul style="list-style-type: none"> • Clarity and transparency around enterprise and divisional risk forum responsibilities, terms of reference and delegation authority for decision-making. Noting the Financial Accountability Regime (FAR) imposes a higher responsibility and accountability framework on the industry and its leaders
 <p>Processes</p>	<p>Process modelling</p> <ul style="list-style-type: none"> • Understanding critical and non-critical business processes and identifying risk, controls, obligations, third-party providers and key data dependencies. Leverage design-thinking workshops • Reassess inherent risk ratings and control adequacy. Revise risk profile as appropriate
 <p>People & Organisations</p>	<p>Three lines of defence</p> <ul style="list-style-type: none"> • Periodic review of target operating model across three lines of defence, assessing and aligning capability and skills, ensuring alignment to organisational design principles, entity, and business unit strategies <p>Risk culture framework</p> <ul style="list-style-type: none"> • Appropriately incentivise and encourage right behaviours and conduct • Propagating a risk-aware mindset that recognises the uncertainty of activities within the product value chain and proactively seeks to identify, analyse and respond to risks • Receptive initiatives that uplift risk culture by considering APRA's Risk Culture 10 Dimensions • Regular pulse checks of risk culture across all levels of seniority and functions within the organisation • Invest in risk awareness training through in-person experiential workshops for all functions to better appreciate risk management in their daily work
 <p>Methodologies</p>	<p>Design-thinking</p> <ul style="list-style-type: none"> • Apply double-diamond to reach an agreement of the problem area(s) to address and solutionise • Apply Rose, Bud and Thorns throughout existing risk management, operations and business processes • Prioritisation matrix and roadmap for uplift opportunities
 <p>Systems & Data</p>	<p>Risk reporting</p> <ul style="list-style-type: none"> • A standardised baseline of reporting requirements and attributes that form the foundation for ease of cross-functional comparison, product-led and/or enterprise aggregated risk reporting and insights • Definition of what meaningful risk reporting consists of and how data should be presented • Periodic review of organisation's risk taxonomy, risk event categories, matrix and ratings to reflect macroeconomic changes, industry trends, regulatory requirements and other factors • Ensure central governance, risk and compliance tools are fit-for-purpose and can integrate with relevant software and other technology • Clarity of data lineage, reduced time lag for data reporting, ease of data extraction, and design of data presentation

Practical tips

When it comes to enhancing risk management practices, there is no one-size-fits-all. An organisation's regulated nature, size and maturity may also determine the appropriate level of detail and uplift needed. It's important to ensure the organisation isn't overengineering its risk transformation. Risk management isn't meant to hinder the growth of a company — rather, it should enable an organisation to identify, measure and manage risks according to its risk appetite, with the end goal of better managing the business, among other benefits.

Driving Efficiencies: The Intersection Point

Regulators such as APRA have started to highlight the importance of integrating business process management and risk management. APRA's new Prudential Standard CPS 230 Operational Risk Management looks at strengthening the operational resilience of APRA-regulated organisations. CPS 230 requires an APRA-regulated entity to manage its operational risks by assessing the impact of business and strategic decisions on the entity's operational risk profile and resilience, implementing operational risk controls and identifying and responding to operational risk incidents. Such organisations are required to have better transparency around the value chain of their critical processes. This includes developing and optimising business continuity plans, monitoring compliance, and reporting on any failures to comply. These requirements exemplify the focus regulators are placing on an integrated business process and risk management approach — potentially a good benchmark for non-APRA regulated entities as well.³

For clarity around what risks apply across an end-to-end business or product lifecycle for example, risk events can be mapped out across the respective value chain, to consider what risks the business and/or product may encounter for each process. Once risks are identified, businesses can allocate a rating to better understand the organisation's susceptibility. An organisation may want to consider specific exposures within its products and processes that could impact operational risk. For example, new customers must go through a Know-Your-Customer verification check. If not done properly, the organisation could be onboarding customers that don't fit the organisation's risk appetite. Another example

is if products aren't properly designed for their target markets, such as if a credit card designed for low-income earners actually has very high fees and interest rates built in. This could directly upset the targeted customer base, leading to a poor reputation and penalties for failure to meet consumer-related regulatory requirements.

In addition to understanding risks across the value chain, it is also important for an organisation to adopt a growth mindset by evaluating the effectiveness of existing controls and determining control uplift opportunities. These can be identified through internal testing and performance monitoring, and can take the form of simplification, streamlining, enhancement or creation of controls. For example, new controls can be introduced to address emerging risks, redundant or ineffective controls can be collapsed, and existing controls can be strengthened through automation and standardisation.

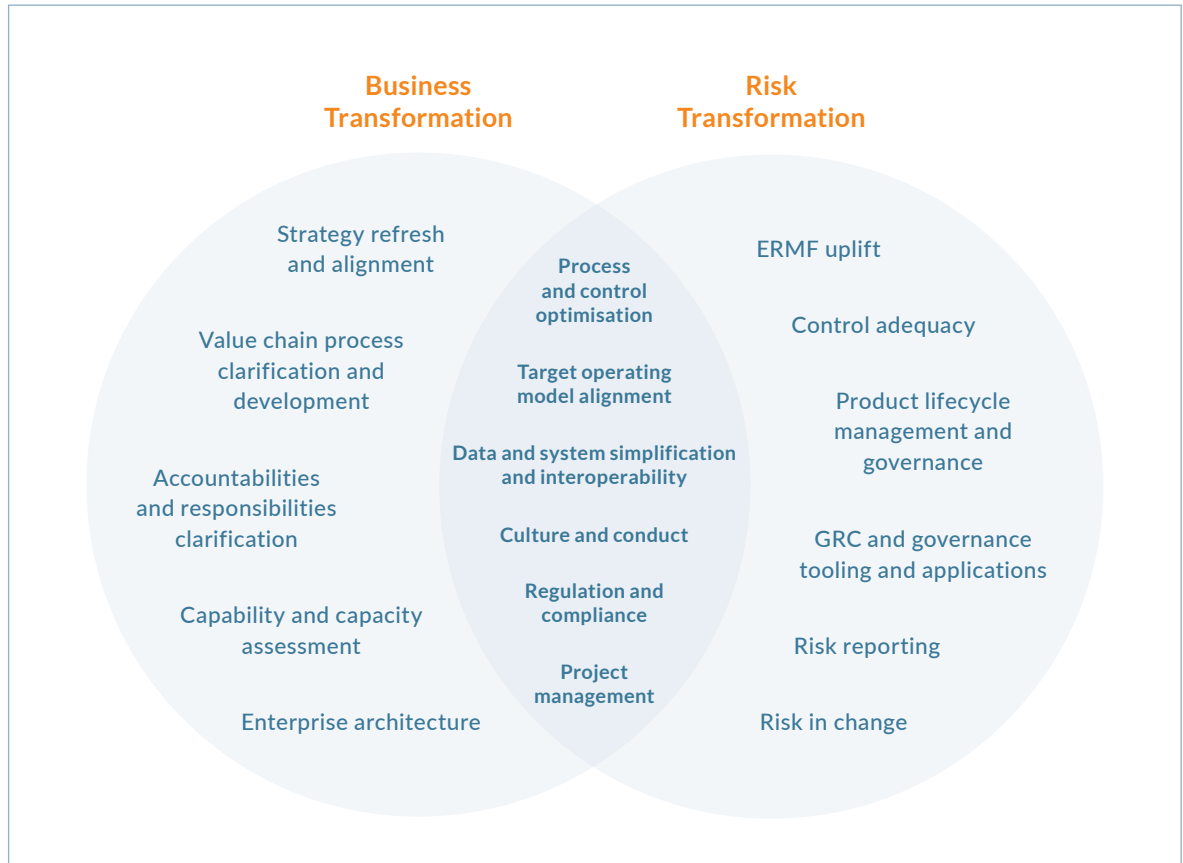
Organisations often use a combination of control types based on their specific needs and resources, with the preference to automate where possible to reduce human error, and to prevent the risk from occurring in the first place. Two common classifications used to categorise risk management controls are:

1. Preventative vs. detective controls:
 - Preventative — a control implemented to prevent a risk from occurring
 - Detective — a type of control that seeks to reveal problems in the organisation's processes after they have occurred
2. Automated vs. manual controls:
 - Automated — a system control that automatically identifies and mitigates when a process goes beyond a risk-tolerance level
 - Manual — manual inspection of a risk event to determine if it is within the acceptable risk level

³ Australian Prudential Regulation Authority "Operational risk management," Accessed 14 August 2023.

In Figure 1 below, we illustrate the common areas where risk transformation intersects with business transformation. When undergoing both business and risk transformation, consider the synergies and outputs that can be better worked on together. What operating model inefficiencies have been uncovered in the product business? Are there handover points that can be streamlined? How can we ensure there is one single source of truth for data? How can we ensure systems integrate and can produce dynamic reporting?

• • • **Figure 1: Sample intersection between business and risk transformation**



Implementation, Embedment and Benefits Realisation

After the design phase, organisations gradually then transition into the development, implementation and embedment phases for change initiatives. This article does not explore these phases due to the sheer content that would be needed, but ensuring an effective change and communication strategy and plan is a key factor for these subsequent phases.

Phasing out the changes across cohorts or workstreams, and deciding when and how to communicate, may allow for learnings to be applied for the remaining change areas. Appropriate monitoring mechanisms are often used throughout embedment and beyond. Checks for adherence against objectives and stakeholder feedback are some ways to carry out monitoring. It is important to monitor benefits realised, taking note of any learnings to apply during the warranty period and for any related future projects or business-led initiatives.

Below are some real-life client examples to whom our subject-matter experts have provided support in delivering risk transformation initiatives.

Examples of Tangible Benefits

Streamlined Controls: One member-owned organisation simplified and enhanced controls across its product value chain, leading to 20+ optimised processes, 20+ risk and control taxonomy uplift opportunities. This indirectly prevented the organisation from further non-compliance penalties and adverse reputational impact.

Enhanced Governance: A banking division established a centralised risk product governance team through target operating model design and implementation, resulting in clearer accountability and more efficient decision-making around product-related risks. Product incidents became transparent and any regulatory breaches followed a standardised process for internal and external intervention.

Modernised Governance, Risk & Compliance (GRC) System: An outdated GRC system was replaced with a new, cloud-based off-the-shelf solution offering better reporting, and improved collaboration capabilities.

Product Governance System: A bank implemented a central enterprise-wide product governance Software-as-a-Service (SaaS) solution for easy monitoring of product performance, and product lifecycle management. This solution replaced 6 systems with 1, and saved 50% time spend in product management monitoring and 90% of time spent preparing product risk reporting documents.

The Ongoing Process of Risk Management

Risk management is an ongoing affair where an organisation's risk controls can be adjusted depending on business needs and drivers. Changing macroeconomic, market, geopolitical, artificial intelligence and other strategic risks require businesses to be more agile than before. Businesses should not only react to these conditions but pre-empt and mitigate the likelihood and/or impacts of them so that they can continue to operate into the future. Risk management should not be isolated to risk professionals, but rather embedded into every staff's remit and mindset. With the right level of risk intel, businesses can then be equipped to make better-informed decisions.

Conclusion

We have explored approaches and elements of both business and risk transformation, as well as their intersection points. Effective business transformation relies on a strong foundation of risk management, and effective risk management should be underpinned by clear business management objectives. By proactively addressing risks, organisations can unlock new opportunities and achieve sustainable long-term success.

Acknowledgement

Ruby Chen, Kalina Hall, and Anthony Le contributed to this piece.

Contacts

Ruby Chen
Director, R&C-Core
Protiviti
ruby.chen@protiviti.com.au

Anthony Le
Manager, R&C-Core
Protiviti
anthony.le@protiviti.com.au

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the *Fortune* 100 Best Companies to Work For® list for the 10th consecutive year, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti is a wholly owned subsidiary of Robert Half Inc. (NYSE: RHI).