Risk and Compliance Insights

Driving transformation and adding more value in a volatile, complex and interconnected environment.

The Chief Risk Officer's (CRO) mandate has always been to build the capability, culture and ways of working that allow an organisation to proactively manage their risks as a natural part of the business operations.

Financial institutions and major corporates have made real and significant progress on this journey. Risk management is more strategically positioned, better supported by data and technology, more integrated into the business operating model and is helping the business to deliver their strategy and meet the expectations of its customers and regulators.

As the risk environment continues to evolve CRO's will need to help the business navigate a volatile, interconnected, nonlinear, complex, accelerated and at times incomprehensible landscape (the 'new risk landscape') that will require the risk operating model to continue to evolve, innovate and transform.

Progressive CRO's are driving strategic change, leveraging innovation and technology, to build the capability and culture and **a risk operating model that is transparent, consistent, efficient, adaptable and effective**.

THE RISK AND COMPLIANCE OPERATING MODEL

The risk and compliance operating model (distinct from the risk management and compliance framework), and its level of integration, will differ across organisations. However, there are some fundamental building blocks that need to be in place. The risk strategy, governance, appetite and culture compliment the business strategy, objectives and culture and set the expectations. The common risk and compliance lifecycle, simple tools and techniques and aligned data and information allow the business to integrate risk and compliance into the business operating model at an enterprise and operational level. **While the building blocks have been in place for many years, how they are deployed and integrated will need to evolve given the new risk landscape.**

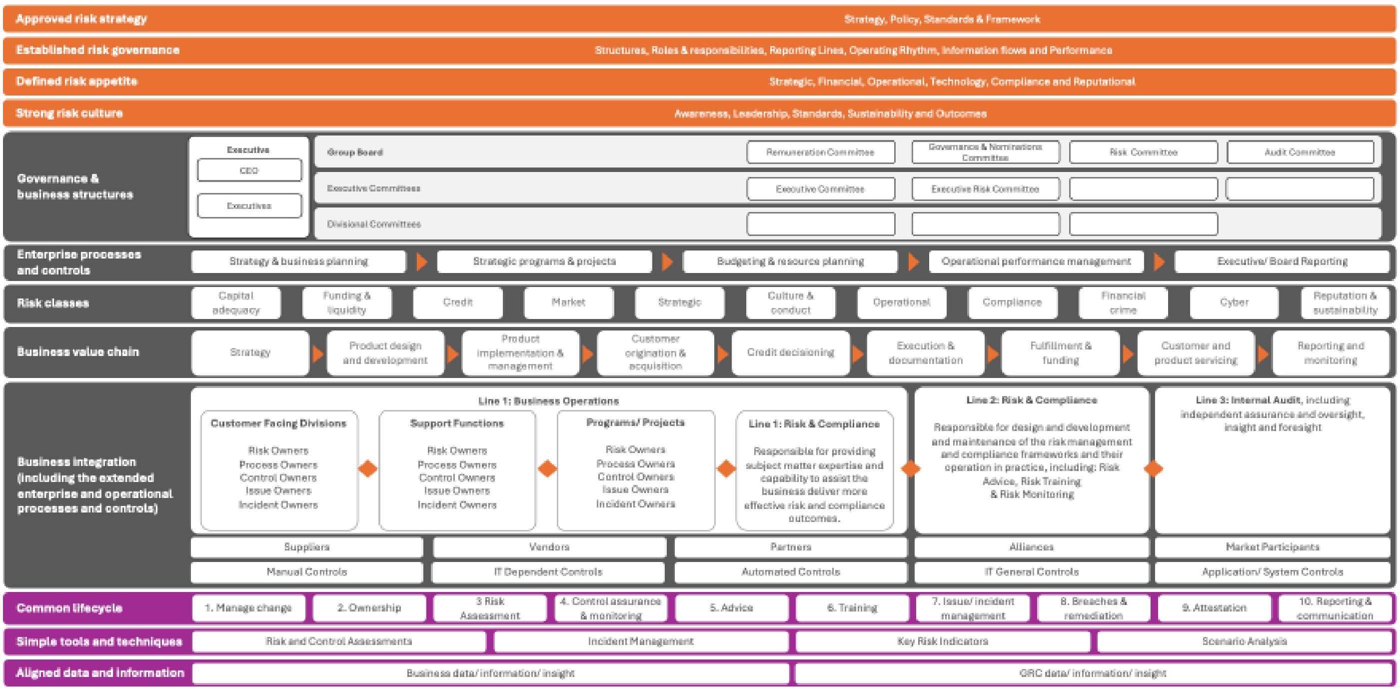

Figure 1: Illustrative elements of a contemporary risk & compliance operating model supporting business integration and uplifting capability and culture.

RISK AND COMPLIANCE TRANSFORMATION

The scope and the pace of any risk and compliance transformation will be driven by the **business strategy and major change initiatives; technology advances and changes; regulatory focus and demands; customer behaviours and expectations; the competitive environment and the risk landscape and emerging risks**.

Successful transformations appreciate the need to focus on all elements of the risk and compliance operating model, as illustrated below, and recognise the outcome must add measurable value, drive stronger capability and culture and inform and support strategic and operational decision making across the business.

For that reason, the delivery approach must be pragmatic, agile and collaborative, it must have organisation wide support, and it must focus on integration, capability and culture (and not simply refresh the frameworks).

Governance and reporting	▪ Role of the Board ▪ Corporate and operational governance ▪ Regulator engagement and reporting ▪ Management and board reporting ▪ Risk and compliance reporting and escalation
Lines of accountability model	▪ Lines of accountability model ▪ Roles and responsibilities model ▪ Assurance operating model
Risk and compliance management frameworks	▪ Group policy structure ▪ Risk management strategy ▪ Risk appetite statement ▪ Non-financial/ Operational risk management framework ▪ Technical risk frameworks, including financial risk ▪ Compliance management framework ▪ Control framework ▪ Issue and incident management process ▪ Risk in change framework
Process, risk and control landscape	▪ Value chain and process models ▪ Risk profiles ▪ Control environment ▪ Obligations and requirements management ▪ Resilience and business continuity management ▪ Third party management ▪ Surveillance and assurance
Risk data and systems	▪ Risk data architecture ▪ Risk data governance ▪ Risk data/ information ▪ Business data/ information ▪ Risk and compliance systems ▪ Business operating systems
Risk culture and conduct	▪ Risk culture framework ▪ Risk culture management ▪ Risk culture reporting ▪ Behaviours and conduct
Capability and capacity	▪ Workforce planning ▪ Risk and compliance capability ▪ Leadership capability ▪ Training and development ▪ Awareness and communication
Accountability and performance	▪ Accountability regime ▪ Performance management and reward/ recognition ▪ Consequence management
Strategic change	▪ Strategic planning ▪ Investment and funding decisions ▪ Programmes and change ▪ Operational performance ▪ Business reporting and communication

Figure 2: Areas of increased focus in a major risk and compliance transformation program driven by innovation and technology and defined outcomes.

KEY FACTORS INFLUENCING TRANSFORMATION EFFORTS

The new risk landscape (that is interconnected, volatile, nonlinear, complex, accelerated and at times incomprehensible) requires the business and the risk and compliance functions to be more innovative as they transform, accessing new capability and leveraging technology and AI.

The key factors we see influencing CROs and the how they deliver their risk management strategies, evolve the risk and compliance operating model and deliver value through transformation are show below.

1. Evolving role of the CRO

The CRO's role has moved well beyond its origins as risk protector, with the most effective leaders operating fluidly across the roles of architect, orchestrator, business accelerator and value creator depending on the organisational needs at any given moment. Their defining contribution is increasingly the sponsorship of risk culture, capability and instilling the voice of risk across the whole organisation and their mandate is shaped by how the three lines of defence are evolving, the organisation's data and AI maturity, and the depth of genuine risk ownership embedded in the business and the quality of decision making.

2. Modernising the three lines of defence model

The traditional three lines of defence model is under real and increasing strain as the connectivity, complexity and pace of the risk environment outpace its linear architecture. Leading institutions are responding with more innovative functional structures, including agility across risk teams/domains and data-informed collaboration across disciplines that preserve the clarity of each line's mandate while fundamentally improving the quality and speed of how they work together.

3. Interconnectivity of operational risk and resilience

The boundaries between operational risk classes have dissolved, for example cyber, digital, third-party, fraud, scam and financial crime risks are now deeply interdependent, and each is being accelerated or complicated by AI adoption, technology transformation and the persistent vulnerabilities of legacy infrastructure. In response, the static risk management framework and supporting lifecycle are being fundamentally reconsidered. Data is increasingly functioning as the control, process as the enabler, and automated controls, monitoring and assurance progressively replacing the periodic, manual approaches that can no longer keep pace with the risks they are designed to manage.

4. Regulatory complexity and fragmentation

The regulatory environment facing financial institutions and major corporates operating across multiple jurisdictions has become materially more complex, with significant variability in standards, priorities and expectations across geographies creating a difficult compliance and risk management landscape. This challenge is compounded by the pace of technology innovation, rising geopolitical tensions and the divergence of national regulatory priorities. This is driving a level of fragmentation while the risks themselves are becoming more interconnected and harder to contain within jurisdictional boundaries.

5. Talent, culture and risk capability

The risk and compliance workforce of the future demands digital acumen, including data, AI and technology, alongside the cultural attributes and domain expertise that no technology can replicate, creating a talent profile that needs to be developed and retained. As AI strategies move from ambition to delivery, workforce planning becomes simultaneously more consequential and more difficult, requiring organisations to build, attract and retain individuals who are proficient across both technical and operational domains at a time when the shape of those roles is itself being redefined.

6. AI and technology as the driver and enabler

AI and technology are reshaping the risk function, strengthening monitoring, automation and analytical capability while simultaneously requiring the CRO to govern AI as a material risk in its own right and build the specialised talent to do both at scale. The limitations of data quality, security and underlying technology architecture remain the most significant constraint on realising the full potential of this transformation, which is also actively challenging, and in many cases fundamentally redesigning, the operating models and business models of the business.

7. Data quality and technical architecture improving risk insights

Data quality and technical architecture are the foundation on which the entire risk transformation rests, driving innovation and sophistication across every stage of the risk lifecycle including the GRC platform design, increasing use of process management software as well as best of breed tooling and AI-enabled activities and analytics. When this foundation is genuinely strong, it delivers what frameworks alone cannot: stakeholder confidence grounded in higher quality of risk insight and foresight at the Board, Executive and regulatory level.

8. Demand for responsible AI backed by AI governance

Existing model risk governance frameworks were not designed for the opacity, predictability and pace/ scale of adoption that characterise generative and agentic AI, and extending them requires deliberate design, including clear principles for human 'in-the-loop' or 'on-the-loop' oversight, management of data constraints and external dependencies, and the monitoring of variability in AI-generated outputs. Regulators are increasingly attentive to the fairness, transparency and customer harm implications of AI deployment, and the organisations that invest in responsible AI governance now will realise the benefits of adoption more quickly, more sustainably, and with significantly greater confidence from their Boards and Regulators.

9. Geopolitical risk, climate risk and other emerging threats

Economic volatility and geopolitical complexity are creating a risk environment that is fundamentally less predictable than the one in which most organisations' risk frameworks were designed, with material implications for decisions about market entry, portfolio composition, counterparty exposure and strategic planning horizons. The deeper challenge is the interconnectivity of these risks. Climate, geopolitical, macroeconomic and emerging threats do not behave independently, and their interactions are generating a level of uncertainty that demands scenario planning and stress testing capabilities that are materially different and can support decision making in the new risk environment.

10. Transformation agility, sustainability and return on investment

Building a credible business case for risk transformation, one that encompasses the redesign of the three lines model, a sustainable talent strategy and the technology investment required to underpin both, is a governance challenge that demands the CRO to demonstrate a measurable return on the investment to a Board and Executive. The most significant execution risk is the demand for two-speed delivery: driving major structural and technology change while simultaneously maintaining and continuously improving the quality of BAU risk management activities and meeting any regulatory and customer remediation commitments.

ABOUT RESILIRE BUSINESS CONSULTING

At Resilire Business Consulting we utilise our expertise in governance, resilience and assurance to support Boards, CEOs and Executive Teams to build resilient businesses by helping to create transparent, consistent, efficient, adaptable and effective operating models. **https://resilirebusinessconsulting.com.au**

Contact information: Mike Purvis | 0417 288 244 | mike@resilirebusinessconsulting.com.au