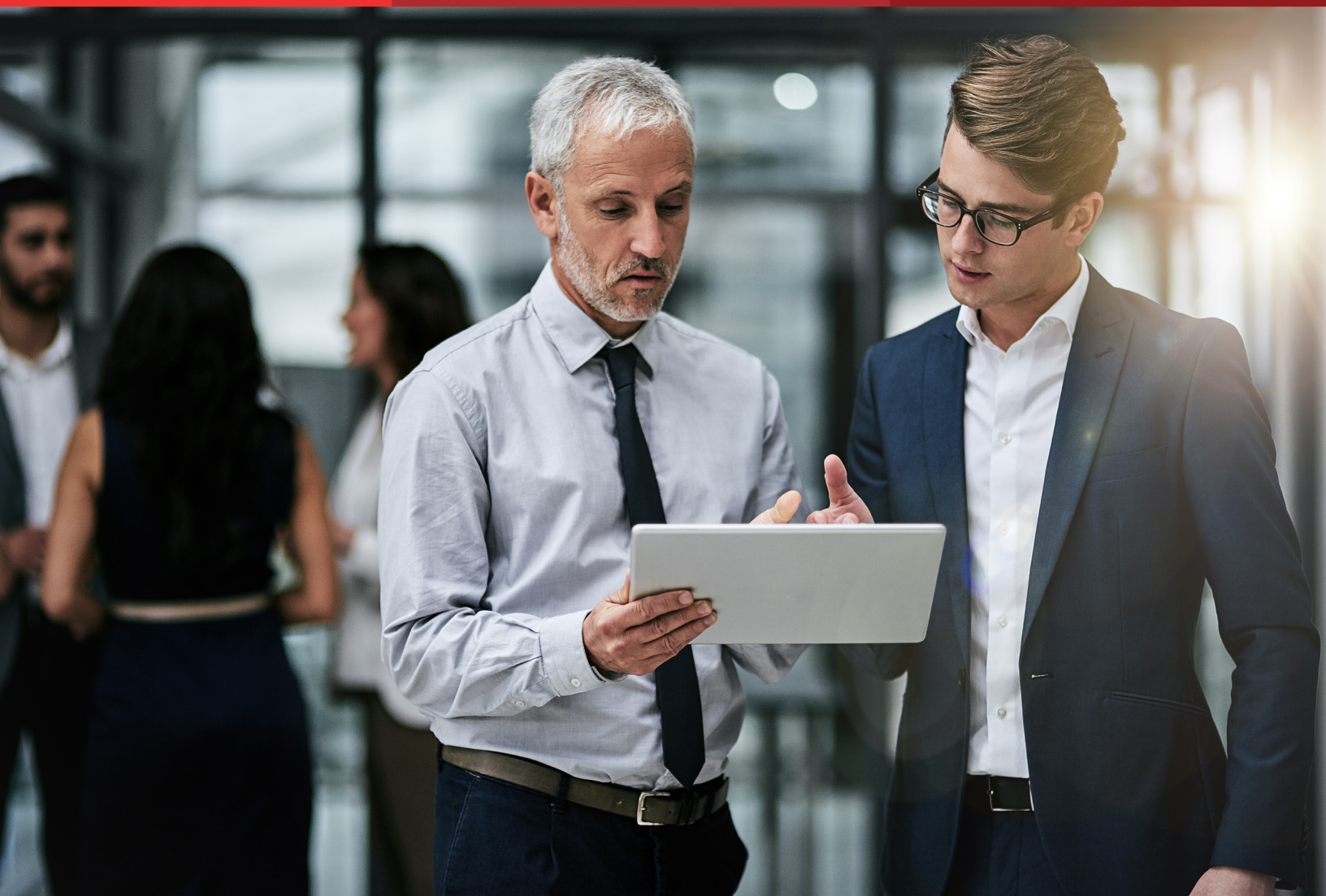
Diligent

# 5 KEY STRATEGIES FOR FINANCIAL BOARDS TO DRIVE DIGITAL RESILIENCE



A crisis can uncover an organisation's inability to adapt to unforeseen challenges, or it can present new opportunities. While many industries struggled in 2020 to adapt to the challenges caused by the COVID-19 pandemic, the financial services industry adapted to the new dynamic relatively swiftly and efficiently.

Financial organisations accelerated their digital roadmaps to create productive virtual environments for distributed teams and made the transition to digital channels and touchpoints for customers relatively quickly. Australia's historic, rapid take up and acceptance and of new technologies and innovations in financial services also left it well placed to adapt.

Leaders are now shifting gears, however, widening their lens from short-term success to long-term sustainable growth. Digital resilience has emerged as a prime focus for financial boards that want to ensure their organisations not only survive the next crisis, but actively thrive. Below are five key strategies for boards to create an enterprise-wide culture of resilience.

## 1 ALIGN TECHNOLOGY WITH BUSINESS STRATEGY

Technology has become essential to an organisation's strategic objectives and operational models. The role of technology within the organisation can no longer be viewed as a siloed function but must be elevated as an integral aspect of operating. As companies navigated the challenges of the pandemic, these siloes started to come down.

For boards to take an active role in ensuring alignment between technology and business, there need to be open channels of communication among leaders, management and technology teams.

Disruptions caused by the pandemic have highlighted the critical role of technology in crisis management and business continuity. As boards rethink their strategy for business resilience, they need to account for technology's role in enabling a robust yet agile foundation for organisations to pivot and stabilize.

### Recommended Actions

- Empower management to respond in the moment by developing an agile, flexible operation from the top down to react quickly to changing markets, demands and environments.
- Facilitate secure communication among boards, executives and management teams to make collaborative decisions around urgent digital initiatives. Support this collaboration with a digital governance platform that enables rapid implementation across the organisation.
- Revise board metrics to go beyond traditional measures of 'on time' and 'on budget'. Track the progress made on initiatives tied to larger business goals such as agility, customer centricity and overall security, thus enabling the organisation to be more resilient.

## 2 ENABLE STRATEGIC OPERATIONAL RISK MANAGEMENT

New ways of working have introduced layers of complexity to financial institutions' already complicated risk environment. To navigate this dynamic risk landscape, boards need to empower their companies to embed strategic risk management frameworks that provide risk oversight and transparency across the entire organisation.

Financial institutions are pressed to anticipate risks well in advance, and to develop and support rock-solid infrastructures across all their subsidiaries. Organisations need a solution that supports future growth while also ensuring compliance and identifying risks and reputational red flags.

For Australian Prudential Regulation Authority (APRA) regulated financial services firms this starts with the key prudential standard, CPS 221. CPS 221 requires all entities to have a risk management framework that provides 'a structure for identifying and managing each material risk to ensure the institution is being prudently and soundly managed, having regard to the size, business mix and complexity of its operations.' All financial services boards need to keep this uppermost in their minds and be constantly asking if effective risk management systems are in place and working.

Even without the regulatory requirement, an investment in better risk, compliance, entity governance and reputational monitoring software accelerates operational maturity. This enhances an organisation's ability to achieve the three most important goals of any business: growth, profitability, and brand equity.

Boards should focus on strengthening their organisation's operational governance. Mismanaged or undermanaged operational governance can often be a challenge due to the fragmented and decentralised nature of business today. It can cause poor information flow, inefficient coordination between teams, slow market response times and costly blind spots. To ensure effective oversight and always provide strong outcomes, companies must proactively re-evaluate their operational governance workflows, so practices, policies and plans are up-to-date, effective and ready when needed.

Third party risks are also requiring significantly more oversight as they are increasing being seen as a potential source of business disruption or other risk of loss such as a data breach. For those supervised by APRA, CPS 231 (or SPS 231) covers the outsourcing of business processes and operations. The bar continues to be lifted in this area.

### Recommended Actions

- **Anticipate and manage operational risk by using predictive models. Access to the right compliance tools can also help assess third-party risk to the business and ensure the proper controls are in place to identify and mitigate risks.**
- **Support sustainable growth by improving governance practices to strengthen your company's long-term viability, enhance value and pave the way for growth. Address governance deficits to ensure your organisation is well equipped to prevent and manage operational risks.**
- **Protect brand reputation by monitoring your peers on key risk and compliance topics; measure industry and company perception; and anticipate material legal, regulatory and reputational risks.**

[1] https://www.legislation.gov.au/Details/F2019L00669

## 3 EVALUATE THE BOARD'S ABILITY TO MANAGE MODERN CHALLENGES

As businesses come to grips with the new, post-pandemic normal, topics in boardrooms are widening well beyond the traditional pursuit of growth and revenue to new priorities focused on the evolving business landscape: managing new risks posed by accelerated innovations, addressing activist demands, and spearheading environmental, social and governance (ESG) initiatives.

Tackling this wide range of issues calls for diverse perspectives and diverse representation on the board. Boards will need to look beyond traditional methods of sourcing new directors. Many still rely on a small number of recruiter networks or references. This can compromise the organisation's success; a board's inability to refresh itself thwarts innovation, diversity and growth. Building diversity in the leadership pipeline ensures boards gain contrasting insights, different voices and unique perspectives, all of which are critical to improved business performance.

### Recommended Actions

- Replace traditional methods of board recruitment from within the organisation or restricted reference networks with processes and tools that can help build a more diverse board.
- Access a platform like Diligent Director Network, which provides nominating committees with data from across 24 global markets and 40 indexes – including more than 5,500 companies and detailed biographies of more than 250,000 directors and executives.
- Ensure that your board composition reflects the organisation's diversity needs in terms of skill sets, perspective, experience, and demographics (including ethnicity, race, level of experience, gender and geography). Board composition also should represent constituent voices and align with strategic goals.

## 4 EQUIP BOARDS WITH ACTIONABLE CYBER SECURITY OVERSIGHT

A recent study be Dell Technologies, estimated that eight in 10 organisations fast-tracked digital transformation programs in 2020, with 74% investing in on-demand digital services and 79% re-inventing their business models.[2] Digitization at this pace has often focused on adaptability, at times overlooking the gaps and vulnerabilities created in the process. Digitisation at this scale has also meant increased exposure, opening up a larger attack surface for cyber threats. Moreover, the magnitude of cyber-attacks at SolarWinds and FireEye have exposed the vulnerabilities of the global network on which the new business models are built.

[2] https://www.delltechnologies.com/en-us/perspectives/digital-transformation-index.htm#scroll=off

Cyber-security has long been on the radar of financial services boards. But as the risk has increased and digital resilience becomes core to operating models, boards must take a more hands-on approach, ask the right questions and place cyber-security prominently on the board agenda. Additionally, boards must model the security-first behavior they expect the organisation to adopt.

Board members need not be experts on cyber-security, but they need to be prepared to ask management: What steps is the organisation taking to improve its security and compliance posture? How do our cyber-security capabilities stack up against those of our competition? Boards need to understand that it is no longer a matter of the cyber-security of the organisation alone, but also the posture and preparedness of suppliers, integrations and employees. Conventional risk-management systems need to be replaced with new models of cyber risk oversight that provide boards, executives, and management with a comprehensive view into the organisation's risk-preparedness plan and highlight potential threats across the business ecosystem.

'Security by design' should also be a guiding principle for executives and directors. This ensures that there no after the event, retrofitting of information security and security measures. Directors should always be asking about the information security and privacy considerations for new technology investments and business initiatives, more generally.

## Recommended Actions

- Equip boards with the information they need for adequate cyber-security risk oversight: cyber-security frameworks detailing where data is and how it operates, cyber management strategies led by someone with cross-organizational responsibility, and an economic and empirical risk assessment.
- Find alternatives to unsecure, legacy communication channels. Many directors use unsecure channels such as personal email and texting to communicate about their organisation's most sensitive topics. Organisations must secure board and executive communication with an encrypted messaging platform that protects sensitive company information, while keeping people informed of relevant updates in real time.
- Implement a risk dashboard to facilitate board visibility. As boards transition to new styles of oversight, they need more information, delivered more efficiently and frequently. Implement a risk dashboard that offers directors clear visibility into cyber-security risk factors affecting their organisation, peers, competitors and third parties.

## 5 MAINTAIN A CLEAR LINE OF SIGHT OVER REGULATORY COMPLIANCE

The focus for many financial boards during 2020 was clearly on COVID-19. Its impact business activities, loan portfolios and economic conditions remains a standing agenda item in 2021. Boards, risk committees, and risk and compliance managers have however watched a continued stream of enforcement action in relation to failures to comply with a myriad of APRA requirements, Austrac's AML/CTF Know You Customer and transaction reporting requirements, and the Australian Securities and Investments Commission's (ASIC) AFSL /ACL license conditions. The cost and reputation impact to a financial services group of failing to identify and comply with regulatory requirements remains high.

Financial services firms need to be well organised and resourced to meet to long list of compliance requirements. Boards and their subcommittees needed to regularly undertake deep dives on compliance activities using internal and external resources to robustly challenge management on compliance activities. This also extends to conduct and risk culture. Regularly scheduled reviews – probing the effectiveness of risk and compliance frameworks - is essential. ASIC provides compliance guidance for AFS licensees in its regulatory guidance note, RG 104.[3]

### Recommended Actions

- Review your compliance reporting to ensure it is giving you insights into what is happening. Ask management to provide regular reports on how the compliance programs are working. Review compliance reports critically looking for red flags that may indicate be ongoing – potentially systematic - compliance issues.
- Ensure that periodic reviews are undertaken by both internal and external audit of your key compliance requirements. Also ask management for reporting on forthcoming regulatory initiatives across all key regulators.
- Participate or even organise peer industry round tables with directors of similar organisations. Often the audit firms organise roundtables for directors to meet discuss industry issues.

# The Need for Modern Governance

For organisations to thrive in these dynamic times, leadership and governance practices must continue evolving.

Organisations need to reassess, reprioritise and reinvent their strategies. Boards must continue to digitise their practices to drive resiliency and transform corporate governance into a strategic advantage.

Modern governance equips organisations with the security, foresight and accountability to withstand challenges and drive change. Diligent enables this transformation through its modern governance solutions that empower boards, management teams and organisations with the technology, insights and processes they need to endure and thrive.

[3] https://download.asic.gov.au/media/5585990/rg104-published-1-april-2020-20200506.pdf

Diligent

a MODERN GOVERNANCE company

### About Diligent

Diligent is the pioneer in modern governance. Our trusted, cloud-based applications streamline the day-to-day work of board management and committees, support secure collaboration, manage subsidiary and entity data, and deliver insights that empower company leaders to make better decisions in today's complex landscape. With the largest global network of corporate directors and executives, Diligent is relied on by more than 19,000 organisations and nearly 700,000 leaders in over 90 countries. With award-winning customer service across the globe, Diligent serves more than 65% of the ASX, 50% of the Fortune 1000, and 70% of the FTSE 100.

## Trusted by over 700,000 leaders and 19,000 organisations across the globe






### Highest security standards

- 256-bit encryption
- Remote locking
- Two-factor authentication

### Industry-leading support

- 24/7/365 support
- White glove service
- Unlimited user training

### Compliance Attestations

- ASAE 18 audits
- ISO-certified
- Third-party security testing

## For more information or to request a demo:

Call: **1-800-676-207** • Email: **info@diligent.com** • Visit: **diligent.com/au**