

THE IMPACT OF DIGITALISATION ON GOVERNANCE

MASTER CLASS FROM SABINE EVERAET

THESES

1. Who leads the digitalisation of organisations?

Digitalisation is no longer a “nice-to-have”. It has become essential for organisations to compete and survive. As a result, boards that are responsible for the long-term viability of organisations assume responsibility for leading digitalisation as well.

Boards should address digitalisation through four core pillars of responsibility:

- Validating corporate strategy and ensuring the integration of digital priorities within it;
- Ensuring oversight and risk management of digital strategy;
- Ensuring ethical and legal compliance in digitalisation;
- Fostering a tech-savvy corporate culture.

Together, these four pillars allow boards to approach digitalisation holistically, applying the same level of rigour as they would to any other strategic priority.

2. How should boards guide the development of a digital strategy?

Board members should ensure that organisation’s digital strategy is aligned with overarching business objectives. Once such alignment is established, both the board and the executive management can make coherent and consistent decisions regarding resource allocation and strategic priorities, while balancing short- and long-term returns, opportunities, and risks.

Boards should also ensure that investments extend beyond front-end digitisation and innovation, to include legacy systems' replacement, enabling a future-proof, flexible technology architecture. While a CEO’s tenure may last three to five years, depending on the sector, many legacy replacement initiatives may span eight to ten years. Boards need to incentivise executive management to pursue longer-term investments that may be less attractive in the short term but are critical for long-term viability. Ultimately, by prioritising investments in alignment with business strategy, boards maximise their impact on business growth and competitive advantage.

3. How should boards oversee the implementation of a digital strategy?

While boards do not manage day-to-day operations, they are responsible for overall strategic oversight, including digitalisation initiatives. Boards should focus on progress, impact, and trajectory, rather than just raw numbers. To do this effectively, boards must receive regular updates on the extent to which expected value is being realised against defined scope, budget, and timelines. These updates should also include the scale of value delivered relative to KPIs established upfront.

Examples of relevant metrics include:

- **Digital strategy:** % of revenue from digital channels, ROI;
- **Customer experience:** digital NPS, system uptime, % straight-through processing;
- **Talent and culture:** % of workforce reskilled;
- **Cybersecurity and resilience:** detection and response times;
- **Innovation:** % of new digital offerings;
- **Data and AI:** ethics and data quality reviews.

4. How should boards ensure the management of digitalisation risks?

Apart from opportunities, digitalisation also entails risks:

- **AI-Specific Risks:** With AI models being biased, ethical deployment becomes critical. Transparency and validation are necessary to make AI outputs trustworthy and accurate for business use.
- **Cybersecurity and Data Privacy:** Traditionally, cyber and privacy considerations were addressed at the end of development, but modern approaches emphasise “secure by design” and “privacy by design”, integrating these considerations from the start of software or AI development. Sensitive data must be carefully managed, including cross-border flows, to prevent leaks or misuse.
- **Third-Party Risks:** With much IT work outsourced or cloud-hosted, boards must ensure operational resilience by confirming that third-party providers comply with relevant rules and standards.
- **Digital Disruptors:** New market players can disrupt traditional competition through the application of innovative digital products and solutions that better meet the market needs. This makes the monitoring of such players an important part of strategic oversight.
- **Talent and Retention Risks:** Digital transformation increases demand for skilled personnel and may require organisational restructuring to align talent with new realities. This applies across the organisation, including at the board level.

All these risks should be integrated into the enterprise risk map, with each assessed for likelihood and impact. Based on risk mapping, mitigation plans should be designed to reduce inherent risk while maintaining ongoing board oversight.

5. How should boards ensure compliance in digitalisation?

Boards must ensure that organisations uphold relevant regulations and ethical standards in digitalisation. This involves regulatory awareness, robust governance structures, and responsible stewardship of digital and AI systems.

Key regulations may include:

Data privacy: The EU General Data Protection Regulation (GDPR) safeguards the processing of sensitive information.

AI: The EU AI Act governs ethical AI use, ensuring accountability for oversight of AI model outcomes.

Digital operations governance: The EU Digital Operational Resilience Act (DORA) requires financial institutions and their third-party providers to maintain operational continuity plans to manage system failures and protect broader financial stability.

Cyber resilience: The US-based NIST cybersecurity framework provides structured guidance for boards, covering risk identification, protection, detection, response, and recovery.

Boards can also implement tools to make organisations more agile in responding to regulatory changes. This may include scenario testing, which simulates real-life situations relevant to specific regulations to ensure governance frameworks can respond effectively, and horizon scanning, which involves monitoring the regulatory landscape for upcoming changes.

So, digitalisation itself enables compliance, as many current and upcoming regulations include mandatory implementation of technology.

6. How should boards drive a tech-savvy corporate culture?

Culture is a board responsibility. Boards are critical in fostering digital talent, driving change management, encouraging innovation, and balancing experimentations with taking calculated risks. To cultivate such a culture, boards themselves must reflect it in their composition and activities. Digital competency is increasingly essential; boards that lack it risk becoming unfit for purpose. This does not mean understanding technical details but rather understanding how technology applies to the board's role in guiding the organisation.

Digital competency should be reflected in the board skills matrix to assess existing capabilities and complement board composition. Technical topics should be included in the training agenda, such as blockchain, agentic and generative AI, and transformation processes replacing legacy systems. In some boards, more than 50% of training now focuses on technology.

Board members should actively promote these topics, use technology themselves (such as board portals, collaboration tools, electronic signatures, and AI-based summaries), and engage in continuous self-learning through reading and participating in thematic discussions, workshops and seminars.

The board must ensure that executive management also maintains strong digital competency, as successful digitalisation relies on both board oversight and management execution.

7. How to build a tech-savvy board? Advice to board members

1. Apply the Rule of Three, at least three tech-savvy board members;
2. Understand your board colleagues' appetite for technology. Inspire them and give them confidence to join the digital movement;
3. Start with:
 - Being perseverant in bringing technology as a recurring topic to the board agenda;
 - Linking digital strategy to organisational objectives;
 - Ensuring the board receives regular digital KPI and risk reporting;
 - Maintaining oversight of AI ethics, data governance, and privacy;
 - Conducting an annual cyber-resilience review;
 - Committing to continuous digital learning;
 - Ensuring crisis communication plans are in place.

The theses were developed by the Corporate Governance Center, in collaboration with the Center for International Private Enterprise and as part of the "Responding to Threats of Corrosive Capital in Armenia. Phase III" project, funded by the UK International Development from the UK Government.



For more: