Consideration for the boardroom

Corporate Industries & Public Sector edition

Content

Executive summary

We are pleased to present the inaugural edition of Considerations for the Boardroom, designed for corporate and public sector organisations.

This publication brings together the critical themes reshaping today's operating environment—from resilience and regulation to digital transformation, sustainability, and trust. It is intended as a practical guide to support informed, forward looking decision making at board level.

Below are the key takeaways to inform and enrich your boardroom discussions.

1. Resilience is now a core fiduciary duty, not a technical issue

Cyber, operational, supply chain, and digital disruptions are no longer "IT risks"; they threaten business continuity, public trust, safety, and financial stability. Boards are explicitly accountable for resilience outcomes under rising regulatory and supervisory expectations (e.g. NIS 2).

2. Geopolitics has moved cyber and digital risk into the realm of sovereignty

State sponsored cyber activity, sanctions, and geopolitical volatility directly affect critical infrastructure, supply chains, and data flows. Board decisions now sit at the intersection of strategy, regulation, national security, and economic sovereignty.

3. Regulation (NIS 2, CSRD, Pillar 2, Pay Transparency) changes board accountability

New EU regulations significantly raise expectations for:

- Personal accountability of directors and executives
- Evidence based governance and documentation
- Faster incident reporting and enforceable sanctions

Compliance is no longer a legal exercise; it reshapes operating models, investment priorities, and control frameworks.

4. IT–OT convergence is a blind spot with physical and reputational consequences

The integration of IT systems with operational technology (manufacturing, industrial control, utilities) creates new attack surfaces where cyber incidents can cause real world physical damage and safety events. Boards must ensure investment is prioritized by operational criticality, not IT maturity.

5. Human behavior and digital identity are now the primary risk perimeter

Identity controls, privileged access, and human decision making are the dominant attack vectors—amplified by AI driven phishing and impersonation. Traditional awareness programs are insufficient. Boards must treat identity governance and behavioral resilience as strategic safeguards of trust and authority.

6. Ecosystem and third party dependency risk exceeds internal risk

Cloud providers, IT vendors, and critical suppliers create concentration and contagion risks that boards often underestimate. Resilience thinking must extend beyond the legal entity to include supplier exits, coordinated crisis management, and systemic dependencies

7. Fraud is a value destruction risk—but also a recoverable lever

Fraud erodes cash, distorts procurement, weakens controls, and damages legitimacy. Yet prevention, early detection, and training materially reduce losses. Boards should treat fraud management as a value preservation and continuity tool, not just a compliance cost

8. Supply chain resilience now requires data, AI, and scenario capability

Manual planning and limited supplier visibility are structurally inadequate. AI enabled forecasting, multi tier visibility, and scenario modeling are becoming strategic enablers of continuity and competitiveness, not optional innovation

9. Sustainability has shifted from reporting to strategic risk and value creation

Sustainability affects:

- Cost structures (energy, efficiency)
- Access to capital and insurance
- Market access and tender eligibility
- Talent attraction and retention

Boards must focus on material sustainability issues that drive resilience and ROI, not report volume or box ticking

10. Digital transformation is a leadership and governance challenge

Digital investments succeed only when treated as strategic operating model transformations, not IT programs. ERP, cloud, data, and AI choices shape:

- Long term flexibility and dependency
- Risk exposure and resilience
- Decision quality and trust

Boards must govern digital transformation with the same rigor as capital allocation and risk appetite decisions.

As a board member, the insights in this edition are designed to help you anticipate emerging risks, challenge assumptions, and steer your organisation with clarity and confidence.

Yves Thorn
Partner,
Corporate & Public Sector
Market Leader
E: yves.thorn@kpmg.lu

Xavier Roch Lhotellier
Partner,
Technology Advisory and Alliance Leader,
EU Institutions Market Leader
E: xavier.rochlhotelier@kpmg.lu

Cyber resilience, a board imperative

Strengthening governance, continuity, and trust in an era of digital dependence

Recent digital disruptions across Luxembourg and other advanced economies have hampered identity services, telecommunications, energy networks, and public digital platforms. These incidents temporarily restricted access to critical communications, public administration, and financial services, exposing structural dependencies and single points of failure. They demonstrate how rapidly operational disruptions cascade through markets and erode public trust in our increasingly interconnected world.

In an environment shaped by geopolitical volatility and rapidly evolving cyber threats, cybersecurity enables digital operational resilience and regulatory compliance. Boards carry increasing accountability for safeguarding essential services, critical assets, and systemic stability.

To respond effectively, organizations must pivot from fragmented cybersecurity initiatives toward a holistic resilience strategy. This requires integrating regulatory compliance, operational technology (OT) protection, human factors, and ecosystem dependencies into board-level governance and investment decisions.

Supervisory expectations, incident experience, and market practices point to a common set of resilience challenges requiring direct board attention.

Pillar 1
Geopolitics, regulation, and sovereignty

Cyber risk is now a matter of economic sovereignty, national security, and regulatory enforcement. Rising geopolitical tensions and state-sponsored cyber activity increasingly target critical infrastructure and supply chains. In parallel, the transposition of the second Network and Information Security (NIS 2) Directive will materially raise the bar for governance, accountability, and operational maturity across Luxembourg.

NIS 2 extends regulatory scope well beyond traditional critical infrastructure to include industrial operators, digital service providers, public administrations, and key supply-chain actors. Boards and executive management are explicitly accountable for cybersecurity risk management, incident handling, business continuity, and supply-chain security. Supervisory authorities will expect demonstrable governance, documented risk assessments and tested response capabilities — not just technical controls.

NIS 2 introduces stricter incident reporting timelines, enhanced enforcement powers, and significantly increased sanctions. Organizations must ensure that decision-making processes, escalation mechanisms, and evidence production are operationally embedded and auditable.

Compliance is an ongoing transformation affecting operating models, investment prioritization, internal controls, and third-party governance. Boards must actively steer this transition while balancing resilience with operational performance.

Pillar 2

IT-OT convergence and operational exposure

The convergence of information technology (IT) and OT — such as industrial control systems, manufacturing robotics, and smart meters — expands the digital attack surface. It blurs traditional responsibility boundaries between engineering, IT, and security functions. Connected assets increasingly rely on standard IT components, remote access, and cloud services, introducing exposure pathways never intended for cyber threat environments.

Legacy systems with long lifecycles, limited patching capabilities, and vendor dependency remain widespread. At the same time, safety and environmental constraints often restrict traditional security controls. Cyber incidents in OT environments carry direct physical and reputational consequences. Boards must ensure that risk visibility and investment are aligned with operational criticality rather than technical maturity.

Pillar 3

Digital identity, human risk, and trust

Digital identity is now the primary control plane for access to systems, data, and operational processes. Privileged access and machine identities increasingly define the security perimeter. Simultaneously, human behavior remains the dominant attack vector, amplified by artificial intelligence (AI)-driven phishing, deepfake impersonation, and automated social engineering.

Traditional awareness approaches can no longer counter the speed and sophistication of modern attacks. Organizations must strengthen identity governance and behavioral resilience across employees, contractors, and partners. Protecting trust in decision-making and operational commands is critical where digital manipulation can directly impact physical operations and public confidence.

Pillar 4

Ecosystem resilience and supply-chain dependency

Modern organizations operate within tightly interconnected ecosystems of technology providers and cloud platforms. Concentration risk and hidden dependencies create systemic exposure that often exceeds internal control maturity. A failure at a key provider can rapidly propagate across multiple sectors and markets.

Supply-chain security is a core requirement of NIS 2. Organizations must identify, assess, and manage cybersecurity risks arising from direct suppliers and service providers — including information and communication technology (ICT), cloud, and managed services. Supervisory authorities will expect structured third-party risk management and evidence of continuous oversight across critical suppliers.

Boards must extend resilience thinking beyond organizational boundaries through exit planning and coordinated crisis management with strategic partners.

Pillar 5

Resilience engineering, continuity, and crisis readiness

Resilience must be embedded by design across architectures, operational processes, and change management, not retrofitted. Business continuity and disaster recovery must reflect realistic scenarios, including destructive cyber events and prolonged supplier outages affecting both IT and OT environments.

Rapid detection, containment, and recovery capabilities determine the operational and financial impact of an incident. Executive crisis governance, decision authority, and public messaging must be tested under realistic conditions. Boards play a decisive role in setting resilience ambition levels and ensuring that recovery capabilities are demonstrably effective.

Where to start:

Establishing an objective baseline

For boards, strengthening resilience starts with a clear and objective view of current maturity, risk exposure, and regulatory readiness. Without a reliable baseline, investment decisions remain fragmented and driven by partial information.

Leading organizations begin with a structured maturity assessment aligned with recognized frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This covers governance, protection, and recovery capabilities across both IT and OT environments.

An evidence-based baseline enables boards to clearly identify material gaps, quantify risk exposure, and prioritize investments based on business impact. It also allows the board to define meaningful metrics and key risk indicators to track strategic objectives and remediation over time.

Leading organizations increasingly leverage integrated governance platforms to operationalize this model. These tools provide real-time visibility through continuous monitoring and automated reporting, creating a clear audit trail between regulatory requirements and actual control effectiveness. When embedded correctly, they provide a sustainable foundation for regulatory readiness and board-level oversight.

This approach transforms cyber resilience from a collection of initiatives into a governed transformation program anchored in objective metrics and accountable execution.

Questions that may be raised

Question 1

Do we clearly understand the financial, safety, and societal impact of a major cyber or operational disruption?

Question 2

What's the current maturity level of our cybersecurity risk management framework?

Question 3

Is the board confident that our governance and evidence of compliance meet NIS 2 accountability expectations?

Question 4

Do we have full visibility of IT-OT convergence risks, and is investment prioritized by operational impact?

Question 5

Are our digital identity controls and workforce awareness sufficient to mitigate AI-enabled attacks and credential abuse?

Question 6

Have we identified critical suppliers, cloud concentration risks, and single points of failure, and do we have credible exit and continuity options?

By

Onur Ozdemir
Partner, Information Risk Management
E: onur.ozdemir@kpmg.lu

Internal and external fraud:

A risk to consider and a value lever when managed well

Fraud is more than a financial line item; for many organizations, it's a drain on value and a threat to operational trust. It depletes cash and assets, distorts procurement, and disrupts operations. For public-sector entities especially, it also undermines legitimacy.

The latest Association of Certified Fraud Examiners' (ACFE) occupational fraud report highlights the scale of this risk: organizations lose about 5% of revenue to fraud each year. Among 1,921 cases in 138 countries, the median loss per case was USD145,000, and most schemes lasted 12 months before detection.[1]

Navigating sector-specific risks

For commercial and industrial organizations, fraud schemes often align with the purchase-to-pay and asset lifecycle. Asset misappropriation occurs in 89% of cases, with common methods including billing schemes, theft of non-cash assets, and payment tampering. Corruption is present in 48% of cases and frequently drives bid-steering, conflicts of interest, kickbacks, and supplier collusion.[2]

In the public sector, fraud impacts more than the bottom line. It increases delivery risks, such as re-procurement, contract termination, and supply disruption. It also raises accountability risks when exceptions, emergency sourcing, or policy-driven spending weaken controls.[3]

ACFE data identifies governance pressure points for boards: 32% of cases involve inadequate internal controls, and 19% involve overrides of existing controls. Effective control design is necessary to safeguard integrity.

External threats and the control enironment

External fraud often occurs where counterparties, communications, and financial transactions intersect. Criminals increasingly exploit business processes through payment-diversion techniques, such as changes to supplier bank details, urgent payment requests, and invoice redirection. External fraud isn't just an IT issue; it's a control and governance issue in procurement and treasury.

The FBI's Internet Crime Complaint Center (IC3) 2024 report recorded USD16.6 billion in reported losses in the US. Business email compromise (BEC) alone accounted for USD2.77 billion in losses.[4] This is highly relevant as BEC targets key control points, such as vendor onboarding, approval hierarchies, and payment release.

[1] ACFE, Occupational Fraud 2024: A Report to the Nations, 2024, p. 4.
[2] Ibid.
[3] Ibid, p. 5.
[4] FBI IC3, 2025 Internet Crime Report, April 2025, pp. 3, 10.

Safeguarding market integrity in procurement

Market-integrity fraud in procurement remains a significant risk for both public and private tenders. The Organisation for Economic Co-operation and Development (OECD) defines bid rigging as collusion that harms purchasers by raising prices, reducing quality, and dividing markets. This risk appears in forms such as cover bidding, bid suppression, bid rotation, and market allocation — all of which can be identified through tender analytics and disciplined tender design.

External fraud isn't a single threat; it's a portfolio of risks. These include cyber-enabled payment theft, procurement collusion, and product or service-integrity issues that can compromise safety and damage reputations. Boards should expect fraud to cause operational disruption and increased stakeholder scrutiny, including delayed projects, repeated tenders, legal disputes, and reduced public trust.

The power of proactive detection and training

The positive finding is that prevention and early detection significantly reduce losses and duration. Boards have substantial influence over these outcomes.

ACFE data shows that tips are the most common detection method (43%), with web-based (40%) and email (37%) reporting now surpassing telephone hotlines (30%). Importantly, tips come from employees (52%), customers (21%), and vendors (11%), underscoring the need for third-party reporting.[5]

Training is critical: organizations without fraud-awareness training suffer nearly double the median losses compared to those that train both employees and managers.[6] For external payment diversion, readiness is key. IC3 reports that prompt action through the Financial Fraud Kill Chain[7] in 2024 addressed 3,020 complaints and successfully froze nearly USD850 million in attempted theft.[8]

A systemic approach for the boardroom

Boards should consider anti-fraud capability not as a control expense, but a means to avoid losses, detect issues faster, and maintain trust. It ensures operational continuity, protects procurement credibility, and reassures stakeholders of effective risk management.

Boards should approach fraud risk management as a system with four essentials:

1. End-to-end purchase-to-pay integrity
2. Accessible reporting channels for employees and third parties with strong anti-retaliation measures
3. Procurement-market integrity controls aligned to OECD guidance
4. A tested playbook for rapid response and fund recovery.

[5] ACFE, Occupational Fraud 2024, p. 4.
[6] Ibid, p. 42.
[7] The Financial Fraud Kill Chain is a process for recovering large international wire transfers stolen from a victim's bank account.
[8] FBI IC3, 2025 Internet Crime Report, p. 13.

Questions that may be raised

Question 1

Where are our primary "trust points" — such as vendor onboarding, contract changes, invoice approval, or payment release — and could a single person or a compromised mailbox move funds end-to-end today?

Question 2

What is our current override rate for procurement and payment controls, and how does the Audit Committee challenge these exceptions, including executive overrides?

Question 3

Do suppliers, contractors, and customers have a safe, simple route to report concerns, and do we measure how quickly these tips are handled?

Question 4

Are we verifying changes to supplier bank details out-of-band via independent callbacks to mitigate "change-to-first-payment" risk?

Question 5

Do we have a rehearsed rapid-response path to stop losses at the bank level, and what's our median time from detection to initiating recovery?

Question 6

How are we detecting and deterring bid-rigging — such as cover bidding or market allocation — and are tender designs proactively reducing collusion opportunities?

Question 7

Are we investing in fraud-awareness training at all levels, and can management demonstrate its impact on losses, detection speed, and reporting culture?

By

Giovanna Giardina
Partner, Risk Consulting
E: giovanna.giardina@kpmg.lu

Andrea Marchetto
Senior Manager, Risk Consulting
E: andrea.marchetto@kpmg.lu

Supply chain reinvented:

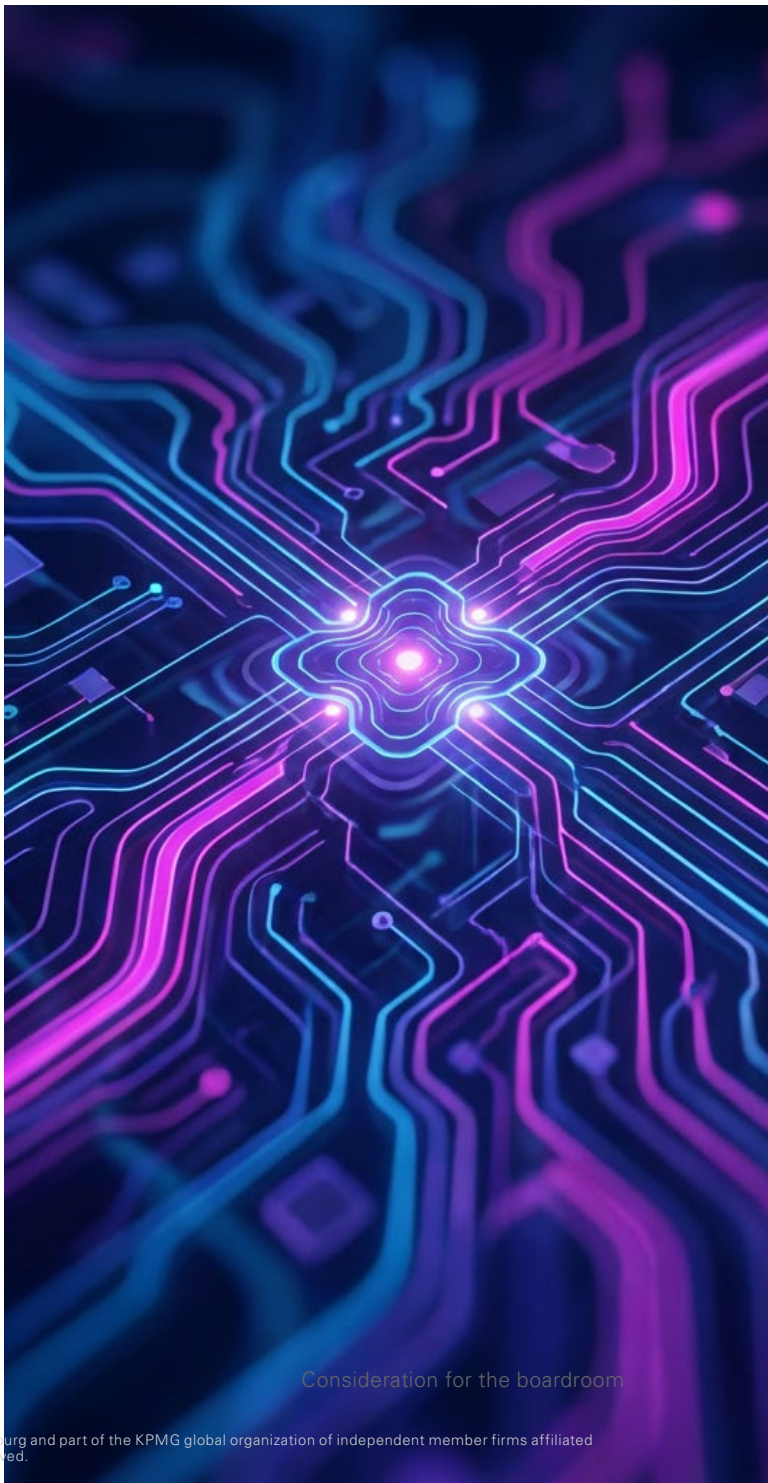
Turning disruption into opportunity with AI

Supply chains in Luxembourg and around the globe are under unprecedented pressure. Disruption is the new normal. With limited visibility and rising uncertainty, manual processes are no longer enough. AI and digital solutions are driving a fundamental shift, offering the resilience, agility, and trust necessary to navigate today's market.

In today's volatile global environment, supply-chain leaders face a relentless barrage of challenges that threaten operational continuity and strategic growth. From geopolitical tensions to regulatory upheaval, the complexity of managing end-to-end supply chains has never been greater for companies in Luxembourg.

In 2024, goods valued at approximately USD16.21 billion were exported from the Grand Duchy,[9] and the country's annual freight transport volume is expected to reach 17.39 billion ton-kilometers by 2030.[10] These figures underscore the nation's pivotal role in international trade and the high stakes involved.

As disruption becomes the norm, forward-thinking organizations are leveraging AI to transform risk into resilience and agility.



Six core challenges facing modern supply chains

1. Opaque supply-chain components and materials

Supply chains today are global, multi-layered, and increasingly complex. Yet, many organizations still operate with limited visibility beyond their immediate suppliers. According to a KPMG supply chain report, 43% of companies have little to no visibility into their Tier 1 suppliers,[11] let alone deeper layers. This opacity exposes businesses to unexpected disruptions, quality issues, and compliance risks.

[9] Statista, „Luxembourg: Export of goods from 2014 to 2024," accessed 10 March 2026.
[10] Statista, „Freight Forwarding - Luxembourg," accessed 10 March 2026.
[11] KPMG, The future of supply chain, September 2023, p. 7.

2. Lack of automation in scenario analysis and planning

Traditional planning relies heavily on manual scenario modeling, which is both time-consuming and limited in scope. Human-driven processes struggle to keep pace with modern risks, resulting in static plans that quickly become outdated. Without the ability to rapidly generate and test multiple scenarios, organizations remain ill-equipped for a dynamic risk landscape.

3. Global political instability

The global landscape is marked by trade wars, sanctions, climate events, and regional conflicts that can upend established supply routes overnight. Recent shifts in trade policies and climate-induced incidents have underscored the fragility of global networks. These disruptions can reduce industrial production by up to 5%[12] and threaten billions in economic value.

4. Global regulatory complexity

Compliance is no longer a local issue. Supply chains must navigate a patchwork of global regulations covering sustainability, emissions, data privacy, and labor standards. For Luxembourg — with its central European location and reliance on cross-border flows — the challenge is intensified. Compliance failures result in costly fines, reputational damage, and operational delays.

5. Prioritizing short-term gains over long-term strategy

Many organizations prioritize immediate operational efficiency at the expense of long-term resilience. This short-termism manifests as just-in-time inventory strategies and minimal safety stocks. While these approaches can reduce costs in stable times, they leave businesses exposed during disruptions, forcing expensive last-minute interventions and undermining customer trust.

6. Confidence in short supply

Trust is the currency of effective supply-chain management, particularly in Luxembourg's collaborative business ecosystem. Yet, opaque processes, inconsistent data, and fragmented communication erode confidence between partners, suppliers, and customers. Without trust, collaboration falters and the ability to respond collectively to disruption is compromised.

[12] Peter Iglinski-Rochester, "Why are supply chains facing disruptions, and how long will they last?," World EconomicForum, 5 July 2022.

Building resilience:

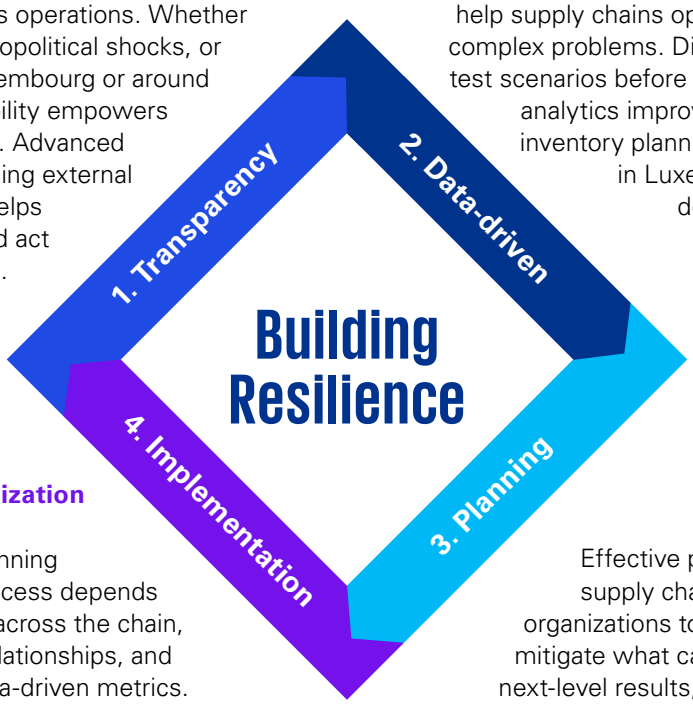
Four essential ingredients for a stronger supply chain

Transparency across the process

Resilience starts with visibility. Leaders need a clear, real-time view across the entire supply chain, including suppliers beyond Tier 1. This means knowing what's coming, when, and from whom. Early collaboration with logistics partners builds trust and streamlines operations. Whether facing natural disasters, geopolitical shocks, or regulatory changes, in Luxembourg or around the world, end-to-end visibility empowers timely, confident decisions. Advanced scenario modeling, combining external signals and internal data, helps organizations spot risks and act before disruptions escalate.

Leveraging data-driven insights

Analytics turn data into actionable insights. AI algorithms, predictive analytics, and digital twins help supply chains optimize efficiency and solve complex problems. Digital twins allow leaders to test scenarios before making changes.Predictive analytics improve demand forecasting and inventory planning. As a result, companies in Luxembourg can make smarter decisions, orchestrate faster responses, and support continuous improvement.



Implementation and realization

Visibility, analytics, and planning converge in execution. Success depends on orchestrating activities across the chain, building trusted supplier relationships, and basing collaboration on data-driven metrics. Leaders must evaluate suppliers beyond Tier 1 and track goods from origin to delivery. Effective planning predicts and mitigates risks, from weather to strikes. Emerging technologies like AI and low-code platforms safeguard operations and drive incremental value quickly, with 55% of CEOs in Luxembourg expecting a return on their AI investments within 1 to 3 years[13]. Optimizing assets, enhancing productivity, and improving processes become routine.

Integrated planning

Effective planning is the backbone of supply chain performance. It enables organizations to anticipate what's coming, mitigate what can't be predicted, and drive next-level results, Cross-functional planning, powered by AI, brings together business leaders to optimize inventory, capacity, and network strategies. Integrated AI planning leverages discriminative, generative, and prescriptive AI to forecast demand, address equipment issues, and determine optimal shipping approaches. For the back office, AI streamlines workflows, enhances visibility, and automated

[13] KPMG, KPMG 2025 Global CEO Outlook, 2025.

KPMG use case:

AI-driven transformation in telecommunications

A leading telecommunications manufacturer faced severe disruptions during the COVID-19 pandemic, resulting in delayed orders, unpredictable revenue, and inconsistent financial reporting. KPMG implemented an integrated planning solution powered by specialized supply-chain software and AI.

By leveraging advanced forecasting, scenario-modeling, and multitier supplier allocation, the company gained deeper visibility and control over its operations. These initiatives delivered sustainable gains in revenue accuracy, increased employee productivity, and enabled proactive responses to market shifts. This AI-driven transformation turned a major disruption into a breakthrough — a result equally achievable for companies operating in Luxembourg.

For more insights into AI-driven supply chain transformation, please read our report, Unchain the supply chain.

The future of supply-chain leadership

Disruption is no longer a risk to be managed, but a reality to be mastered. By harnessing AI and embracing a holistic approach to visibility, planning, compliance, and trust, supply chain leaders in Luxembourg can build organizations that are both resilient and competitive.

With 60% of CEOs in Luxembourg prioritizing AI as a top investment and 45% believing their business is ready for AI adoption,[6] this journey begins with a commitment to transparency and continuous innovation. Those who act now will be best positioned to turn today's challenges into tomorrow's opportunities.

For a deeper analysis of how AI can transform your response to global volatility, please read our report, The disruption dilemma in supply chain.

Questions that may be raised

Question 1

How much real-time visibility do we have across all tiers of our supply chain, and where are the blind spots?

Question 2

Are we prepared to respond to sudden geopolitical events or regulatory changes that could disrupt our operations?

Question 3

What's our current approach to integrating AI and digital solutions, and where are the most critical gaps?

Question 4

How do we ensure data quality and security throughout our supply chain, especially when working with external partners?

Question 5

Are we leveraging predictive analytics to optimize inventory, demand forecasting, and supplier performance?

Question 6

How agile and proactive are our planning processes — are we still relying on manual scenario building?

By

Ugo Platania
Partner, Management Consulting, Global Sector Leader Steel & Metals
E: ugo.platania@kpmg.lu

Sustainability lens to strengthen resilience

Sustainability is no longer optional. Boards must shift their mindset to view sustainability as a strategic vector that reshapes costs, mitigates risks, and enables competitive advantage.

While sustainability has been a fixture on board agendas in recent years, it was often viewed merely as a regulatory requirement or a marketing tool. However, against the backdrop of geopolitical tensions, economic headwinds, and the global ripple effect of AI, the conversation is shifting. Businesses are now refocusing on tangible drivers of long-term value and operational resilience.

Paradoxically, the recent dynamic changes in sustainability regulation and backlash against environmental, social and governance (ESG) factors have acted as a catalyst for clarity. This forces companies to fundamentally re-evaluate the purpose of their sustainability reporting and focus on what really matters.

According to the latest Copernicus Climate Change Service report, 2025 ranked as the third-warmest year on record.[14] Continued rises in global temperatures and extreme weather events are causing asset damage and supply-chain disruptions, transforming climate adaptation into a business imperative.

Luxembourg specific

Despite global turbulence around ESG, the KPMG 2025 CEO Outlook report indicates that most corporate leaders remain strongly committed to their sustainability goals. Sixty-one percent of CEOs say they are on track to hit their 2030 net zero targets, compared to just 51% in 2024.

Key Luxembourg highlights:

- **Strategic alignment**
  50% of Luxembourg CEOs align sustainability goals with their core business strategy to demonstrate value to stakeholders.
- **Deep integration**
  85% have fully embedded sustainability into their business, recognizing it as critical to long-term success.
- **Net-zero confidence gap**
  Only 40% of Luxembourg CEOs are confident about meeting 2030 net-zero targets, compared to 61% globally.
- **Investment discipline**
  40% of Luxembourg CEOs integrate both the costs and potential return on investment (ROI) of sustainability initiatives into major capital decisions.

[14] Copernicus Climate Change Service, Global Climate Highlights 2025, January 2026, p. 7.

Market forces and the social license to operate

The strategic direction of the global economy is increasingly shaped by market forces rather than regulatory bodies. Capital markets, insurers, and global supply-chain partners are now the primary drivers of change.

Data-privacy breaches, labor-rights violations, and product-safety failures are no longer just reputational risks; they're events capable of triggering consumer boycotts and exhaustive regulatory scrutiny. Such failures may even threaten a company's social "license" to operate.

Sustainability must, therefore, remain a core concern for finance and enterprise risk management teams.

Mindset shift

Sustainability drives business value when it's fundamentally aligned with long-term strategic objectives. When embedded into the business model, sustainability thinking creates a material difference in financial performance and operational reality.

1. Broadened risk-management

Risk management is a core part of a board's fiduciary duty. By analyzing business activities through both an "outside-in" lens — how external factors affect the company — and an "inside-out" lens — how the company impacts its environment — organizations gain a more comprehensive picture of existing and emerging risks and opportunities. Cross-functional team discussions further reveal the nuanced interconnections and complexities of modern business.

The Corporate Sustainability Reporting Directive's (CSRD) double materiality assessment (DMA) requirement illustrates this approach in practice. While it may initially appear overly comprehensive, the DMA provides an effective risk-management framework that balances risk identification with impact identification and opportunity recognition, enabling companies to form a more complete view of their activities

2. Operational resilience and efficiency gains

When sustainability is embedded into risk assessment, strengthened operational resilience and adaptation follow naturally. Companies can unlock tangible value by concentrating on what's materially relevant for their specific business model. The board is uniquely positioned to help define three to five "top-of-mind" priorities that directly tie back to long-term value creation.

Certain topics deliver value regardless of reporting obligations, such as energy monitoring, waste reduction, and resource efficiency. Redesigning and optimizing operational processes may translate directly into short-term cost savings. Measuring greenhouse-gas emissions or energy intensity often reveals previously invisible inefficiencies.

The principle is straightforward: what gets measured gets improved. Reporting ESG key performance indicators (KPIs) alongside financial metrics ensures that progress is tracked with equal rigor.

Luxembourg specific

Making energy-efficient investments can also attract beneficial tax incentives. In Luxembourg, a business engaging in an ecological and energy-transition project may qualify for a tax credit. This can reach 18% for both investments and operating expenses.

3. Access to capital

Banks, insurers and investors increasingly price sustainability risks into credit conditions, insurance coverage, and valuation assumptions. For example, as extreme climate events become more frequent, lenders are factoring sustainability performance into loan premiums and capital access. Green and sustainable financing has gained significant prominence, and many institutional funds now limit their investments to companies that meet minimum sustainability thresholds.

4. Market opportunities

Increasingly, meeting customer sustainability requirements has become a prerequisite for supplier consideration and tender participation. Sustainability requirements — including ESG questionnaires, EcoVadis certifications, and third-party assurance — are becoming standard components of most tenders, directly impacting growth prospects.

5. Strengthening your supply chain

Recent trade embargoes, sanctions and regulatory developments have made it clear that businesses don't operate in a vacuum. Initiatives like the EU Carbon Border Adjustment Mechanism (CBAM) and the EU Deforestation Regulation (EUDR) require companies to understand their dependency on natural resources. To get the full picture, companies must look beyond their own operations to examine their entire supply chain.

6. Attracting new talent and enhancing employee retention

Employee retention and talent attraction directly impact operational business continuity. Companies that lose key workers may face hiring costs, knowledge gaps, and productivity disruptions that directly affect business performance. Sustainability initiatives foster greater employee engagement, especially when companies genuinely involve their workforce in conversations around fair labor practices, community impact, and workplace equity.

Compliance fulfils obligations, but integration improves decisions.

Strategic approach to sustainability reporting

Lengthy "virtue-signaling" sustainability reports are falling out of favor. Regardless of regulatory requirements, sustainability reporting should be viewed as a strategic instrument. The real value lies in the associated organizational changes that support the reporting process and the integration of data insights into decision-making.

Practical guidance for decision-making

1. **Integrate sustainability into core strategy:** It shouldn't be a standalone initiative.
2. **Align internally across functions:** Cross-functional alignment is essential for a comprehensive operational roadmap.
3. **Establish structured governance and accountability:** Robust governance ensures process integrity and control as the business environment continues to evolve.

Trend predictions for 2026 that impact sustainability

- EU regulatory pace. The pace of new sustainability regulations is expected to slow as significant changes crystallize through the "Omnibus" package, including the CSRD and the Corporate Sustainability Due Diligence Directive (CSDDD). Companies should use this time to develop practical sustainability business cases.

- Global standards. International sustainability standards issued by the International Accounting Standards Board (IASB) will continue to form a global baseline. Multinationals should prioritize interoperability between standard frameworks and identify core metrics to report.

- AI and transparency. AI will continue advancing digitalization, enabling streamlined reporting and deeper insights. Stakeholders will increasingly expect high-quality sustainability data, which may drive companies to seek third-party assurance to enhance credibility even when not legally required.

Questions that may be raised

Question 1

What sustainability topics are most closely linked to our core business model and strategy in the short, medium and long term? Are these factored into all key decisions, such as capital expenditure (CapEx) and mergers and acquisitions (M&A)?

Question 2

Are sustainability risks fully embedded in our enterprise risk-management framework?

Question 3

Do we have a clear map of all mandatory and voluntary ESG reporting requirements across our operating geographies, and a strategy to fulfill them while effectively telling our company's story?

Question 4

Which sustainability metrics should be reviewed alongside financial KPIs at the board level, and why?

Question 5

How do we ensure our sustainability information is reliable for high-stakes decision-making?

By

Olga Danilenko
Director, ESG Assurance
E: olga.danilenko@kpmg.lu

Stephan Lego-Deiber
Partner, IFRS Leader
E: stephan.legodeiber@kpmg.lu

Digital transformation as a catalyst for long-term value and institutional strength

Digital transformation transcends mere technology trends. For Luxembourg's corporate leaders and public decision-makers, it acts as a powerful catalyst for value creation, resilience, and trust — when governed with intent and clarity.

Across industries and public institutions, digital capabilities now shape service delivery, risk management, talent attraction, and confidence building with citizens, customers, regulators, and markets. Leading organizations reimagine digital transformation not as a technical journey, but as a strategic evolution of the operating model.

This is where boards and senior leadership make the difference.

A uniquely Luxembourg opportunity

Luxembourg is well-positioned to lead by example. Its size, institutional proximity, and strong public-private collaboration allow decisions to translate into rapid impact. Digital transformation offers a unique opportunity to:

- Strengthen the quality and continuity of public and corporate services
- Increase transparency and regulatory effectiveness
- Enhance productivity and cost discipline
- Reinforce Luxembourg's attractiveness as a trusted digital and economic hub.

This proximity means digital decisions are highly visible and their effects widely felt. Success builds confidence across the ecosystem, while misalignment quickly becomes systemic. This reinforces the need for holistic, well-governed transformation.

From digital ambition to digital confidence

Over the past decade, organizations have invested heavily in cloud, data platforms, ERP systems, automation, and AI. While necessary, these investments are insufficient.

Leading organizations are distinguished today by their ability to turn digital ambition into digital confidence that:

- Services will remain available under stress
- Data can be trusted for decisions and reporting
- Technology choices support long-term strategy
- Transformation delivers tangible value.

This confidence stems not from tools, but from coherent governance and integrated decision-making.

Digital transformation as a value engine

When aligned with strategy, digital transformation drives value across five key pillars

1. Strategy and capital allocation

Digital investments enable sharper prioritization, better trade-off insights, and more disciplined capital deployment. Data-driven visibility supports more robust, forward-looking decisions.

2. Operations and service delivery

Modern platforms, automation, and redesigned processes improve reliability, reduce manual effort, and increase responsiveness for all stakeholders.

3. Risk management and resilience

Integrated digital environments enhance traceability, control, and early issue detection, strengthening operational and regulatory resilience.

4. Market and public trust

Consistent, transparent digital services reinforce credibility and confidence — key assets in competitive markets and public administration.

5. Talent and workforce

Digital transformation creates more attractive, purpose-driven roles and enables new ways of working that support engagement and retention.

Technology choices as leadership choices

Digital transformation inevitably involves technology decisions — cloud platforms, core systems, data architectures, and AI solutions. Yet their true impact lies beyond technical specs. Each major digital choice influences:

- Dependency on external ecosystems
- Flexibility to adapt to regulatory or policy changes
- Ability to scale innovation responsibly
- Resilience of long-term cost structures and operational agility.

Boards that approach these decisions through a 360-degree lens — combining strategic intent, risk awareness, operational impact, and people considerations — are best positioned to unlock sustainable benefits.

Data and AI as enablers of better decisions

Data and AI are often described as accelerators. In practice, their greatest contribution is decision quality. Trusted data improves:

- Financial and operational oversight
- Regulatory reporting and transparency
- Policy design and evaluation
- Customer and citizen experience.

AI, when embedded responsibly, augments human judgment, supports consistency, and frees capacity for higher-value activities. Successful organizations treat AI as part of their operating model, with clear accountability and human oversight.

Transformation anchored in people and culture

No digital transformation succeeds without people. Skills, leadership, incentives, and change capacity dictate whether new capabilities are adopted and sustained. Leading organizations invest as much in clarity, communication, and ownership as they do in technology.

Boards play a critical role by:

- Setting clear expectations for accountability
- Supporting cross-functional collaboration
- Ensuring leadership alignment and capability building.

This human dimension is often the decisive factor between transformation that delivers and transformation that stalls.

A balanced view on risk and opportunity

Digital transformation introduces new dependencies and risks, but when managed holistically, it also strengthens control and resilience. By integrating digital initiatives into enterprise risk management, organizations gain:

- Better visibility across processes and suppliers
- Improved continuity and contingency planning
- Stronger governance over critical data and systems.

The objective is not risk elimination, but the intelligent balance of risk in pursuit of long-term value.

Questions that may be raised

Question 1

How does digital transformation directly support our long term mission and strategy?

Question 2

Are digital investments clearly linked to value, resilience, and trust?

Question 3

Do we have confidence in the quality and governance of our data?

Question 4

Do our technology and platform choices align with our risk-appetite and sovereignty considerations?

Question 5

Is our organization equipped — culturally and skill wise — to sustain transformation?

Question 6

Do we review digital performance with the same rigor as financial performance?

By

Xavier Roch Lhotellier
Partner, Technology Advisory and Alliance Leader, EU Institutions Market Leader
E: xavier.rochlhotellier@kpmg.lu

Gianni Segoloni
Director, Digital Services & Technology, Microsoft Alliance Lead
E: gianni.segoloni@kpmg.lu

Digital transformation at the core of strategy

Strengthening execution, resilience and trust through strategic digital choices

Digital transformation transcends simple technological upgrades. In Luxembourg's corporate and public sectors, it increasingly represents the structural backbone through which strategy is executed. Strategic decisions — from cloud platforms and enterprise resource planning (ERP) to data and AI — now define how organizations operate. These choices dictate their resilience under pressure and their credibility among regulators, markets and citizens.

When digital transformation is treated as a downstream IT topic, organizations struggle to realize value, absorb change, and manage risk. Conversely, when embedded at the heart of strategy, it becomes a powerful enabler of long term value, institutional strength, and trust.

A Luxembourg specific strategic imperative

Luxembourg's ecosystem thrives on the close interdependencies between public administrations, regulated industries, and shared service providers. Expectations for continuity, transparency and control are high, while tolerance for disruption remains low. In this environment, strategic ambitions lacking digital enablement are increasingly unfeasible.

Digital transformation offers a unique opportunity to simplify complexity, improve execution discipline, and reinforce confidence across the ecosystem. However, fragmented or poorly governed initiatives can quickly introduce structural fragility. The challenge for boards is therefore not technological ambition, but strategic coherence.

From strategy to an executable operating model

Digital transformation translates strategy into execution. Modern ERP systems, cloud based platforms, and integrated data architectures establish a shared operational backbone across finance, operations, and service delivery. These systems replace manual processes and local workarounds with standardized workflows, real time visibility, and clearer accountability.

This foundation empowers leadership teams to steer organizations with greater precision. Strategic priorities are operationalized more consistently, performance is monitored more reliably, and trade offs between cost, service quality and risk become more transparent. In this sense, digital transformation strengthens strategic control, rather than diluting it.

Automation and AI as strategic enablers

Beyond efficiency tools, the strategic value of automation and AI lies in reshaping work and decision-making. When automation is embedded end to end across processes — supported by ERP and cloud platforms — it eliminates operational friction and enhances service reliability.

AI further augments this model by streamlining decision preparation, prioritization, and forecasting. In sectors facing demographic pressure, skill shortages, and rising expectations, this combination redeploys human capacity toward judgment, oversight, and value adding activities. The result is a more sustainable, productive operating model.

Data as a foundation of confidence

Data sits at the core of ERP, automation and AI. Trusted data enables accurate reporting, informed decisions, and credible engagement with regulators and stakeholders. Conversely, fragmented ownership and inconsistent data quality undermine even the most advanced digital capabilities.

Data governance is not a compliance exercise; it's a foundation of confidence — in the figures, in the decisions and in the organization's ability to defend its actions. Organizations that invest in clear data ownership and quality standards strengthen both performance and trust.

Cloud as a resilience and adaptability lever

Cloud platforms are central to modern digital strategies, enabling scalability, rapid deployment, and improved recovery. However, cloud choices also shape long term dependency, flexibility, and risk exposure.

In Luxembourg's interconnected environment, these choices extend beyond individual organizations. When governed strategically, cloud platforms enhance resilience and innovation. Approached narrowly, they may introduce concentration risk and constrain future options. This requires board level ownership of platform decisions, grounded in strategic intent and risk appetite.

Trust as an integrated outcome of good design

Well governed digital transformation earns trust through reliable execution. Consistent processes, traceable data, and resilient platforms reinforce confidence among citizens, customers, regulators and partners. Trust is not achieved through communication alone but through predictable, transparent digital behavior, especially during moments of stress.

An integrated, 360 degree leadership perspective

Successful digital transformation avoids isolated technology initiatives. It requires integration across strategy, operations, risk management, finance, and people. ERP, cloud, automation, AI, and data must align with capital allocation, regulatory obligations, workforce capability, and supplier dependency management.

This integrated perspective ensures that digital transformation delivers tangible value while cementing resilience and institutional credibility.

Questions that may be raised

Question 1

How does digital transformation actively enable our strategy and long term objectives?

Question 2

Are ERP, cloud, automation and AI investments prioritized based on value and impact rather than technology cycles?

Question 3

Do we have confidence in the quality and governance of the data used to steer the organization?

Question 4

Are automation and AI improving decision making and service quality with clear accountability?

Question 5

Do platform and cloud choices align with our risk appetite and long term flexibility needs?

Question 6

Are we governing digital transformation as a strategic program rather than a collection of initiatives?

Question 7

Is resilience and trust embedded by design in our digital operating model?

By

Xavier Roch Lhotellier
Partner, Technology Advisory and Alliance Leader, EU Institutions Market Leader
E: xavier.rochlhotellier@kpmg.lu

Gianni Segoloni
Director, Digital Services & Technology, Microsoft Alliance Lead
E: gianni.segoloni@kpmg.lu

Creating value through experience

Why customer experience serves as a strategic lever for corporations and the public sector

Experience is no longer a byproduct of service delivery; it's a strategic outcome. For decades, corporations and public-sector organizations approached performance through the lenses of efficiency, compliance, and scale. Customer experience (CX), when addressed, was often treated as a secondary concern — relevant, but rarely decisive.

That hierarchy has been inverted.

Today, corporate clients, suppliers, partners, and citizens bring expectations shaped by the best experiences they encounter elsewhere. They no longer differentiate between "consumer" and "institutional" interactions. They simply compare, raising the bar for every organization they engage with.

According to a recent KPMG study, organizations that deliver superior experiences consistently outperform their peers on satisfaction, trust, loyalty, and long-term value creation. In complex business-to-business (B2B) and public environments, where relationships span years and involve multiple stakeholders, these effects are amplified.

Experience serves as a strategic lever that directly dictates adoption, resilience, and legitimacy.

From isolated touchpoints to total experience creation

Experience is not a delivery, it's a collective production. A critical misunderstanding around CX is the belief that it can be improved by fixing individual touchpoints. In corporations and public-sector bodies, this fragmented approach is particularly limiting.

Stakeholders rarely experience an organization through a single interaction. Their journeys cut across departments, systems, and time: from onboarding and eligibility assessments to approvals, service requests, and audits. Each handover introduces friction. Each inconsistency creates doubt.

Customers increasingly judge organizations on the coherence of their journey rather than on isolated moments. This makes the concept of total experience (TX) creation essential.

CX can't be dissociated from employee experience, partner experience, or digital experience. An overwhelmed frontline agent, a fragmented data landscape, or a misaligned partner ecosystem will inevitably surface in the experience delivered externally.

Leading organizations design experience as an end-to-end system, aligning processes, technology, and behaviors around the outcomes that matter most.

Experience as a driver of trust and institutional legitimacy

Trust is built through managed complexity, not empty promises. In corporate and public-sector contexts, trust is operational currency. It determines whether clients renew contracts, whether partners collaborate, and whether citizens adopt services or comply with policies.

Experience plays a crucial role in cementing trust, especially during times of complexity or stress. When processes are opaque, responses slow, or responsibilities unclear, trust erodes rapidly. Conversely, clarity, consistency, and a sense of fairness strengthen legitimacy.

KPMG's research consistently shows that emotional drivers — such as reassurance, confidence, and feeling understood — are critical even in rational, high-stakes environments. This challenges the assumption that B2B and public interactions are purely functional.

Experience, in this sense, becomes a stabilizing force. It reassures stakeholders that the organization is in control, attentive, and aligned with their interests.

AI and the rise of ambient intelligence

The next leap in CX will not be conversational; it will be contextual. AI is already reshaping how organizations operate. Yet much of today's adoption remains focused on incremental productivity gains: drafting documents, summarizing information, and accelerating individual tasks.

The real transformation for corporations and public-sector organizations lies in the emergence of agentic AI and ambient intelligence.

Rather than reacting to prompts, ambient intelligence operates in the background. It listens, observes, connects signals, and acts proactively. In customer service and case management, this represents a profound mindset shift. AI no longer waits for a request; it anticipates needs, supports decisions, and orchestrates experiences across channels and moments.

This is particularly impactful in sectors where interactions are complex, regulated, and high-volume. AI can guide users through intricate journeys, support frontline staff with real-time context, and ensure continuity across fragmented systems. When designed responsibly, it augments human judgment rather than replacing it.

However, this evolution raises fundamental questions around ethics, transparency, security, and privacy. When intelligence becomes ambient, governance can't be an afterthought. Trust in the experience is now rooted in the integrity of technology that operates without a direct human prompt.

Considering the TX is essential when envisioning agentic AI implementation. It requires evaluating the entire journey and identifying the decision-making points and underlying business rules. The organizations that stand out are those that consider value generation globally.

From technology adoption to value-oriented CX governance

CX transformations fail not from a lack of tools, but from a lack of prioritization. Many organizations invest heavily in CX and digital initiatives, yet struggle to demonstrate tangible value. The reason is rarely technological; it's structural.

Experience transformation cuts across silos. Without clear governance, initiatives multiply, priorities compete, and value dissipates. Technology decisions are often made locally, while experience outcomes remain global.

A value-oriented CX strategy requires explicit governance mechanisms. Leaders must define which experiences matter most, how success is measured, and how trade-offs are arbitrated across the transformation portfolio. This includes aligning AI investments, service redesign, and process simplification around shared value objectives — whether financial, operational, or societal.

In this model, CX is a strategic investment discipline, guided by executive intent and sustained by accountability.

Experience as a leadership responsibility

Experience is where strategy becomes tangible. Ultimately, CX in corporations and the public sector isn't a design challenge; it's a leadership one. It reflects how clearly an organization understands its purpose, how well it aligns its capabilities, and how seriously it takes the trust placed in it.

Organizations that lead through experience don't chase trends. They use technology, including AI, to reinforce coherence, empower people, and create value that's felt as well as measured.

In an environment of rising expectations and constrained resources, experience represents the most powerful lever that leaders possess to deliver sustainable impact.

If you'd like to dive deeper into these findings, our Global Customer Experience Excellence (CEE) 2025–2026 report provides the full analysis.

Questions that may be raised

Question 1

Which experiences truly matter most to our clients, partners, or citizens, and do we manage them end-to-end?

Question 2

Where does friction in our service delivery destroy value or trust today, and do we understand its real cost?

Question 3

Are our CX and AI investments driven by a clear value ambition or primarily by technological opportunity?

Question 4

How intentionally are we preparing for agentic and ambient AI in customer service and case management?

Question 5

Do our employees have the autonomy, data, and support required to deliver the experience we promise?

Question 6

Who's accountable for experience outcomes at the executive level, and how is this reflected in our governance?

By

Xavier Roch Lhotellier
Partner, Technology Advisory and Alliance Leader, EU Institutions Market Leader
E: xavier.rochlhotellier@kpmg.lu

Julien Hugo
Director, Management Consulting
E: julien.hugo@kpmg.lu

Luxembourg investment tax credit: Strategic considerations for boards and Chief Financial Officers

Luxembourg offers an investment tax credit (ITC) designed to incentivize qualifying CapEx that drive competitiveness, innovation, and economic development. For corporate groups and boards, the ITC offers a powerful mechanism to reduce the effective tax costs of strategic investments.

The modernized regime, effective since 1 January 2024, increased rates and broadened eligibility to include certain operating expenses (OpEx) for qualifying digital transformation or ecological and energy transition initiatives.

Understanding the ITC framework

The ITC serves as a primary fiscal tool for organizations looking to optimize their Luxembourg footprint.

- It's a tax relief allowing qualifying companies to claim a credit against corporate income tax. This applies to certain investments in tangible and intangible assets.
- For specific projects, the credit also covers qualifying OpEx.
- Recent reforms increased the baseline rate for the global investment ITC to 12%. This single rate applies regardless of the amount invested.
- The new regime also creates more generous reliefs for projects tied to digital transformation or ecological and energy transition objectives.

Key rates and new features

The 2024 modernization simplified the rate structure while significantly expanding potential tax savings.

- 12% for global investment. The update increased the rate from 8% and removed the previous EUR150,000 threshold.
- 18% ITC for digital transformation or ecological and energy transition. This rate applies to projects meeting expanded definitions. Crucially, it can include qualifying OpEx, such as personnel costs and third-party costs, in addition to capital investments.
- 6% (or 18% otherwise) for investments in tangible depreciable assets and software. Where assets expect to benefit from the 12% global investment credit, a 6% rate may apply; otherwise, the 18% rate may be relevant.
- 14% for investments qualifying under Article 32bis of the Luxembourg income tax law (LITL). This applies to tangible depreciable assets with special amortization profiles. To qualify, these investments must deliver environmental improvements, such as reducing water consumption, waste, or pollution.

Eligible project types for the 18% ITC

To qualify for the enhanced rates, projects must demonstrate a clear link to the country's dual-transition goals.

- Digital transformation. Projects delivering process, organizational, or service delivery innovations. Examples include ERP implementation, cybersecurity enhancements, or adopting advanced analytics to redefine processes.
- Ecological and energy transition. Projects that reduce environmental impact or improve energy or material efficiency. This includes energy decarbonization, renewable self-consumption, energy storage, and circularity initiatives.

Interaction and exclusions

Navigating the boundaries between different tax regimes is essential for total compliance.

- The ITC cannot be combined with the intellectual property (IP) box regime under Article 50ter LITL.
- Project qualification dictates the specific treatment of the assets, such as software capitalization and the timing of expenses. Early analysis and documentation are essential.

Illustrative corporate income tax savings

For a project with a cost profile over the next three years consisting of EUR1,200,000 in OpEx and EUR2,600,000 in CapEx:

- ITC at 12%: EUR312,000 on CapEx
- ITC at 18%: EUR684,000 on combined CapEx and OpEx.

Compliance, documentation, and process

Securing these credits necessitates a high degree of administrative precision and proactive communication with authorities.

- The regime requires rigorous evidence of eligibility. This includes invoices, contracts, asset registers, and proof of operational use.
- For projects seeking the enhanced 18% rate or Article 32bis treatment, companies may need to file eligibility attestation requests with the Ministry of the Economy. KPMG's proposed approach includes:
  - » Eligibility review and quantification
  - » Drafting and filing of the attestation
  - » Annual follow-up and ad-hoc assistance.
- Timeline highlights: expenses incurred before submitting the eligibility attestation application are typically ineligible. After the project is closed, a certificate attesting the actual expenses must be requested within two months. The issuance of this certificate may take up to nine months.

Governance and board considerations

Beyond the technicalities, boards should focus on the strategic integrity of the claim.

- Strategic alignment: ensure the investment drives core business objectives beyond tax benefits.
- Controls and documentation: implement project-level tracking for CapEx and OpEx, maintain contemporaneous records, and retain evidence supporting eligibility.
- Audit readiness: prepare a structured file to support claims in the event of queries from the Ministry of the Economy or tax authorities.

Practical next steps

- Immediate (up to three months): map planned investments against ITC eligibility, run a preliminary quantification, and gather documentary evidence.
- Short term (three to six months): prepare and submit eligibility attestation requests where appropriate, and engage advisers for drafting and liaising with the Ministry.
- Ongoing: perform an annual validation of consumed budgets, obtain certificates to support corporate tax filings, and maintain a governance framework for future claims.

Conclusion

The modernized ITC presents meaningful opportunities to enhance the return on strategic CapEx and qualifying OpEx. Capturing these benefits requires early planning, precise project qualification, and robust documentation. Structured engagement with advisers and proactive governance will increase the probability of successfully securing and defending this tax credit.

Questions that may be raised

Question 1

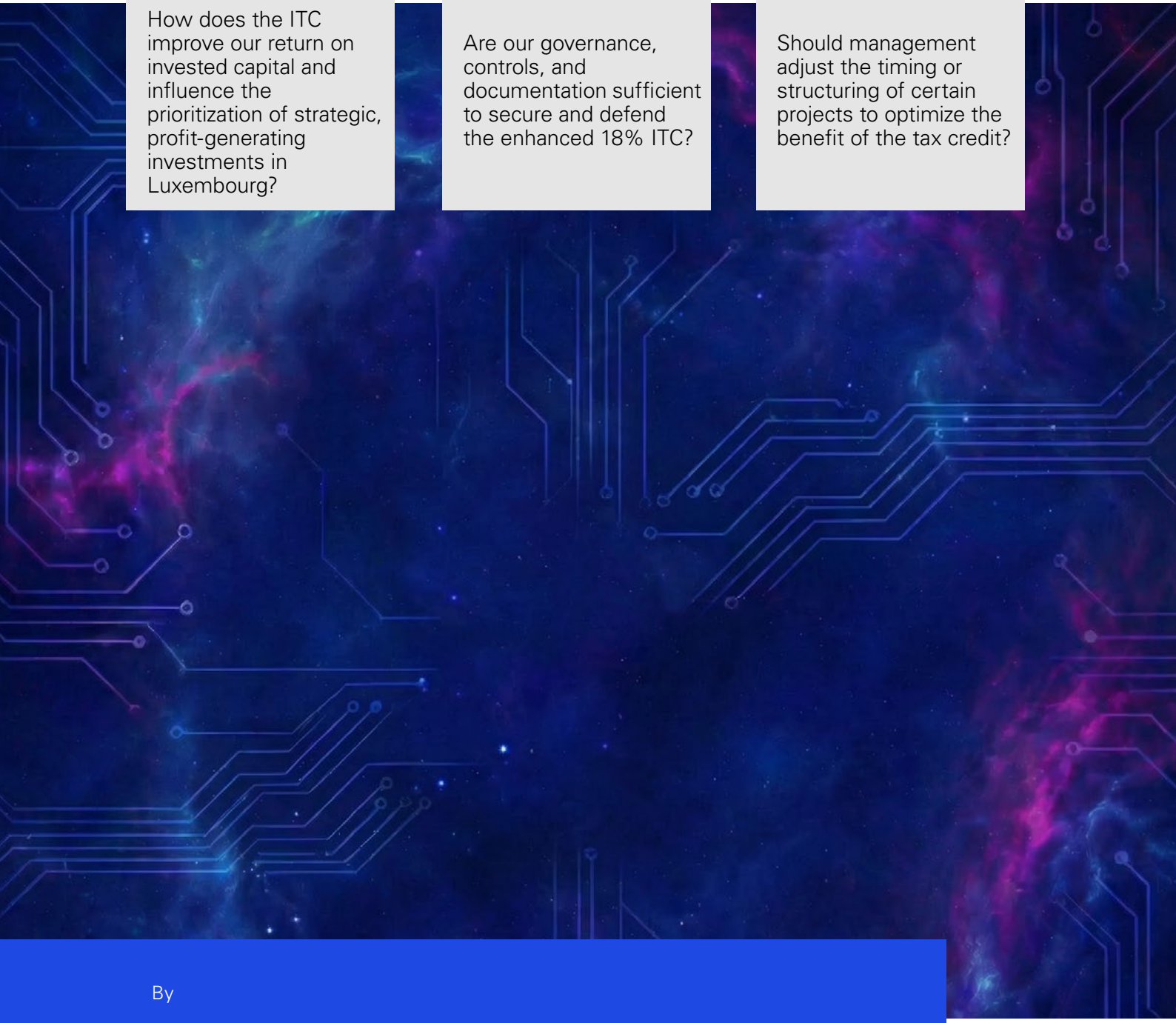
How does the ITC improve our return on invested capital and influence the prioritization of strategic, profit-generating investments in Luxembourg?

Question 2

Are our governance, controls, and documentation sufficient to secure and defend the enhanced 18% ITC?

Question 3

Should management adjust the timing or structuring of certain projects to optimize the benefit of the tax credit?



By

Henri Prijot
Partner, Commerce and Industry Tax
E: henri.prijot@kpmg.lu

Anne-Marie Folquet
Partner, Commerce and Industry Tax
E: anne-marie.folquet@kpmg.lu

Pillar 2 and the global minimum tax

The Pillar 2 Directive aims to ensure large multinational enterprises (MNEs) pay a minimum level of tax on the income generated in each jurisdiction where they operate. For boards and executive teams, understanding these rules is no longer a future compliance task; it's a current strategic necessity.

What's Pillar 2 about?

Pillar 2 is part of the OECD's Base Erosion and Profit Shifting (BEPS) initiative. It was adopted at the EU level on 14 December 2022 and transposed in Luxembourg on 22 December 2023.

It introduces a 15% global minimum tax on certain groups with consolidated revenue of EUR750 million or more in at least two of the four preceding years. If a jurisdiction's effective tax rate (ETR) falls below 15%, top-up tax provisions apply. To levy this tax, two interlocking rules have been introduced:

- Income Inclusion Rule (IIR)
- Undertaxed Profits Rule (UTPR)

Additionally, jurisdictions may implement a Qualified Domestic Minimum Top-up Tax (QDMTT), which imposes the top-up tax domestically if the ETR is below the 15% threshold.

The Pillar 2 Directive applies for fiscal years starting on or after 31 December 2023.

What's the Side-by-Side package?

On 5 January 2026, the OECD/G20 Inclusive Framework on BEPS published the Side-by-Side (SbS) package, which modifies key aspects of the Pillar 2 framework. The package introduces a dual-component system consisting of two primary safe harbors, both effective from 1 January 2026:

- SbS Safe Harbor: This suspends IIR and UTPR application for MNEs with an Ultimate Parent Entity (UPE) in a jurisdiction that imposes minimum taxation on both domestic and foreign income, and provides a foreign tax credit for QDMTT. The OECD Central Record of Qualified SbS regimes currently lists the US as the only qualifying regime.
- UPE Safe Harbor: This replaces the existing transitional UTPR Safe Harbor. It exempts UPE jurisdictions from the UTPR if they impose minimum taxation requirements on domestic income. The official OECD Central Record of eligible jurisdictions is currently pending publication.

What's at stake for CIPS?

Unless specific exclusions apply, MNE groups in CIPS that meet the EUR750 million threshold fall under the scope of these rules. With the release of the Pillar 2 forms in online and XML formats, the Luxembourg tax authorities have made the compliance process fully operational. Organizations must now navigate three procedures via the MyGuichet platform to maintain compliance:

- Registration: every Luxembourg-based constituent entity, joint venture, and joint venture affiliate must complete an individual registration. This form may also be used to notify the authorities of any group changes or to deregister an entity.
- GloBE Information Return (GIR): Luxembourg constituent entities must submit the GIR, unless it's filed in another jurisdiction and exchanged with Luxembourg. If filed elsewhere, a notification must be submitted to the Luxembourg tax authorities.
- Local tax return: this covers IIR, UTPR and QDMTT. For UTPR and QDMTT, a Luxembourg designated entity may be elected to file and pay on behalf of all Luxembourg constituent entities. The form is relatively short and only requires general information and a declaration of the tax payable.

The deadline for these filing obligations is 15 months after the end of the fiscal year (18 months for the transitional year). Accordingly, calendar-year taxpayers face their first filing obligation by 30 June 2026 in respect of the 2024 fiscal year.

Strategic recommendations

MNE groups should perform a comprehensive perimeter assessment to confirm if Pillar 2's rules apply and document the findings for tax governance purposes. We recommend addressing the following:

1. Exemptions: does the group or specific entities fall under any exemptions, such as the excluded entity status?

2. Classifications: are the group's entities properly assessed (e.g. constituent entities, intermediate parent entities, partially owner parent entities, joint ventures, etc.)?

3. Safe harbors: can the group benefit from transitional, permanent, or the new SbS safe harbors?

4. Elections: are any specific elections needed, such as the Equity Investment Inclusion Election or the QDMTT Safe Harbor election?

The priority now is to confirm entity classifications, ensure full registration by the required deadlines, and assign clear internal ownership for the calculation and filing process.

M&A considerations

Pillar 2 impacts require continuous oversight through the M&A lifecycle. Typical triggers include:

- Revenue thresholds: acquisitions or disposals can impact whether a group remains above the EUR750 million threshold.

- Consolidation rules: differences in accounting consolidation between buyer and seller can lead to different Pillar 2 outcomes.

- Pricing deviations: a transaction can trigger pricing deviations for the same target when modeling Pillar 2 for buyers and sellers with different Pillar 2 profiles.

M&A transactions may also require discussions regarding the relevant information a buyer should obtain from the seller to fully onboard the target into Pillar 2's scope. Similarly, a specific contractual protection should be negotiated in the share purchase agreement (SPA) regarding the Pillar 2 tax risk. These considerations should not be underestimated and must be closely monitored.

And finally, what about data?

With Pillar 2 now in force, fund managers should already have identified the data they need from all jurisdictions where they operate, and set up processes to collect it. The priority now is to ensure data quality, and make any adjustments before the first filing deadline.

Digital tools, such as the KPMG BEPS 2.0 Automation Technology (KBAT), empower groups to streamline this reporting, automate calculations, and ensure data integrity.

Questions that may be raised

Question 1

Do we have Pillar 2 oversight in-house, and are we considering local Pillar 2 positions at the entity level?

Question 2

Is our scoping and entity classification reviewed and validated by a third party?

Question 3

Do we have Pillar 2 oversight in-house, and are we considering local Pillar 2 positions at the entity level?

Question 4

Can we effectively manage the Pillar 2's data collection and processing requirements?

Question 5

Have we assigned clear ownership for the registration and filing of our first returns?

Question 6

How are we mitigating Pillar 2 tax risks in our current M&A pipeline and SPA negotiations?

By

Emilien Lebas
Partner, Commerce and Industry Tax
E: emilien.lebas@kpmg.lu

The talent imperative: Navigating Luxembourg's evolving labor landscape

Luxembourg is widely recognized as a stable, efficient, and attractive economic hub at the heart of Europe. Its political stability, transparent regulatory environment, and favorable tax framework establish it as a premier hub for companies and institutions seeking to innovate and operate across borders.

A defining strength of the country lies in its highly international and multilingual workforce. Organizations benefit from a pool of professionals who bring adaptability and cross-cultural expertise, key assets in a globalized economy.

However, this environment presents distinct challenges. Competition for specialized talent is intense, particularly in digital transformation, sustainability, compliance, and risk management. High living costs and limited housing availability can also hinder recruitment and retention.

Winning the talent race: Luxembourg's strategic approach

Key figures

Luxembourg's labor market stands out in Europe for its exceptional degree of internationalization. The following figures from the National Institute of Statistics and Economic Studies (STATEC) highlight the market's unique structure:

- Total workforce: approximately 489,000 employees
- Cross-border workers: 47% of the workforce, mainly from France (126,000), Belgium (52,000), and Germany (52,000)
- Citizenship: only 25% of employees hold Luxembourgish nationality.[15]

These figures reveal a dual reality: a large daily cross-border commuter population alongside a growing community of resident international professionals. This structure underpins Luxembourg's economic dynamism but also creates a heavy dependence on continued appeal as a top-tier employment destination.

Luxembourg's administrative structure is further defined by significant public expenditure. As of 31 December 2024, the state employed nearly 37,000 public servants.[16] These substantial budgetary allocations reflect a strategic priority for high-quality services and long-term preparedness, particularly in defense, security, digital transformation, and climate policy.

These commitments demonstrate the Grand Duchy's resolve to invest in its future. However, they also underline the importance of maintaining sustainable fiscal revenue in an increasingly competitive landscape. Sustaining this model requires consistent economic growth and, crucially, a persistent ability to attract and retain talent.

Luxembourg's threefold strategy

The government has made talent a central pillar of its 2023–2028 coalition agreement. This strategy is supported by institutional initiatives and targeted tax reforms.

Supporting young professionals

Fiscal packages introduced in 2024 and 2025 aim to facilitate entry into the labor market:

- Housing allowance, designed to help young employees cope with high rental costs
- Young employee bonus, designed to foster loyalty from the first job and promote long-term engagement.

[15] STATEC, Regards 01/25 – Panorama of the Luxembourg labour market on May 1st, 2024.
[16] Ministry of the Civil Service, 2024 Activity Report of the Ministry of the Civil Service, 2025.

Attracting experienced professionals

To draw highly skilled profiles, Luxembourg relies on targeted reforms, including:

- Modernization of the impatriate tax regime, strengthening its appeal to international experts
- Revision of the carried interest tax framework, expanding eligibility and providing legal clarity, particularly for the financial sector
- European Blue Card, streamlining immigration for highly qualified workers.

Retaining existing talent

Retention is supported through enhanced fiscal and social instruments:

- Modernized participation bonus, reinforcing performance-related incentives
- Interest subsidies, serving as a valuable retention tool
- Supplementary pension schemes, supporting long-term financial security and loyalty.

Boosting young and innovative start-ups

From the 2026 tax year, Luxembourg has introduced a 20% start-up investment tax credit for individual investors. This measure aims to channel private capital into innovative companies while ensuring robust governance and eligibility safeguards.

Rewards: Balancing motivation, equity, cost, and performance

Luxembourg's diverse workforce fuels innovation, but also increases complexity for employers. Reward strategies are evolving toward a more holistic approach. Today's professionals seek purpose, flexibility, fairness, personalized benefits, and strong career development opportunities alongside competitive pay.

Shifting trends in executive compensation

According to a KPMG EMEA survey on executive compensation and long-term incentive plans, based on responses from 271 organizations, executive pay structures are undergoing a significant shift toward performance-driven models.

While base salaries remain aligned with market benchmarks, variable pay — especially at senior levels — has increased in response to inflation, geopolitical uncertainty, regulatory pressure, and the intensifying competition for leadership talent. Compensation strategies are increasingly designed to reward specific outcomes over tenure, reinforcing both individual accountability and corporate cost discipline.

Short-term versus long-term incentives: a vital distinction

The distinction between short-term incentives (STIs) and long-term incentives (LTIs) is now fundamental to modern reward philosophy.

- STIs support organizational agility and annual execution. In Luxembourg, some firms use favorable tax mechanisms like the participation bonus to optimize these payouts.
- LTIs, employed by nearly 70% of surveyed organizations, align executive interests with multi-year strategic goals, shareholder expectations, and sustainable value creation.

LTIs are particularly vital in volatile environments. They help counter short-termism, reinforce ownership behaviors, and secure executive retention. Increasingly, they incorporate ESG-related metrics, reflecting broader expectations around responsible governance.

From a cost-management perspective, LTIs allow organizations to tie compensation to realized value rather than fixed commitments. In many organizations, base salary now represents less than 60% of total compensation, with the remainder linked to performance over annual and multi-year horizons.

Pay transparency: a strategic and regulatory priority

The EU Pay Transparency Directive (the "Directive") is a major focus for Luxembourg HR departments. It aims to promote pay equity and fairness, and must be transposed into national law by 7 June 2026

Objectivity as a foundation

To ensure non-discriminatory pay practices, organizations must rely on gender-neutral criteria. Work of equal value is now assessed based on education, skills (including soft skills), effort, responsibility, and working conditions.

Reinforced employee rights

The Directive strengthens transparency throughout the employee lifecycle:

- Recruitment: candidates must be informed of salary ranges before accepting an offer; employers are prohibited from requesting pay history.
- Internal transparency: employees may request information about their own pay and average levels for equivalent roles. Employers must respond within two months.

Mandatory reporting on gender pay gaps

Reports must provide granular data, including gender pay gaps by worker category, variable pay distribution, and gender representation across pay quartiles.

The frequency of mandatory reporting is staggered based on the company's size:

- For fewer than 100 employees: reporting remains voluntary.
- Between 100 and 149 employees: the first report is due in 2031, then required every three years.
- Between 150 and 249 employees: the first report is due in 2027, then required every three years.
- For more than 250 employees: the first report is due in 2027, then required annually.

These new obligations supplement existing reporting duties to the staff delegation.

Managing the risks of non-compliance

If a gap of at least 5% cannot be objectively justified and remedied within six months, corrective action with employee representatives is required. Failure to comply exposes employers to financial penalties, reputational damage, and operational risks such as internal friction and talent attrition.

Pay transparency statistics: EU and national perspectives

According to Eurostat, the average gender pay gap in the EU stood at 11.1% in 2024. Luxembourg stands out as the only EU country to have achieved pay parity, reporting a -0.8% gap in favor of women.[17]

Data from STATEC shows a dramatic improvement from a 10.7% gap in 2006. However, hourly pay parity doesn't fully translate into annual income equality. Men remain overrepresented in high-bonus roles, while women are more likely to work part-time.[18]

The Committee on the Elimination of Discrimination against Women (CEDAW) has noted persistent poverty among working women in Luxembourg, particularly single-parent households, despite the country's high GDP per capita.[19]

Preparing for transparency

While awareness of the Directive is high, implementation remains challenging. Typical preparatory steps include gender pay gap analyses, job classification reviews, HR and management training, and the establishment of transparent salary bands.

Pay transparency is more than a compliance obligation; it's a strategic opportunity to strengthen fairness, attract talent, and enhance organizational credibility.

As emphasized by KPMG Luxembourg, effective total rewards strategies can transform regulatory requirements into a competitive advantage.

The road ahead

Luxembourg's ability to attract international talent has long underpinned its economic success. Today, evolving jobseeker expectations and intensified competition require a more forward-looking approach.

By combining targeted fiscal measures with a focus on quality of life and fairness, Luxembourg is well-positioned to strengthen its role as a leading European destination for talent in an increasingly interconnected world.

[17] Eurostat, Gender pay gap statistics, February 2027.
[18] United Nations, Gender equality: smaller pay gaps in Belgium, Italy and Luxembourg, 7 March 2025.
[19] Ibid

Questions that may be raised

Question 1

Which levers are most effective to retain our critical and hard-to-replace talent?

Question 2

Have we benchmarked our remuneration frameworks against our peers?

Question 3

Are existing tax incentives delivering measurable returns in attraction and retention?

Question 4

Does our reward mix properly balance short-term performance and long-term value creation?

Question 5

Are we ready for the EU Pay Transparency Directive, and how can compliance become a strategic advantage?

Question 6

What legal, financial, and reputational risks do we face if pay transparency requirements are not fully met by 2026?

By

Sacha Thill
Partner, Executive Compensation & Personal Tax
E: sacha.thill@kpmg.lu

Sabrina Bonnet
Director, People and Change
E: sabrina.bonnet@kpmg.lu

KPMG Luxembourg

39, Avenue John. F. Kennedy
L-1855 Luxembourg

T: +352 22 51 51 1
F: +352 22 51 71

Yves Thorn
Partner,
Corporate & Public Sector
Market Leader
E: yves.thorn@kpmg.lu

Xavier Roch Lhotellier
Partner,
Technology Advisory and Alliance Leader,
EU Institutions Market Leader
E: xavier.rochlhotelier@kpmg.lu

www.kpmg.com

home.kpmg/socialmedia