Policy Recommendations for Business Continuity and Governance in the Financial Sector

Gregorio Caraballo, CaixaBank
Martí Fabregat, CaixaBank Tech
Ramon Martín de Pozuelo, CaixaBank
Thomas Selegny, RESALLIENCE

July 2025

ATLANTIS

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe Research and Innovation Programme under the Grant Agreement No. 101073909.

Policy Recommendations for Business Continuity and Governance in the Financial Sector

Martí Fabregat and Ramon Martín de Pozuelo (CaixaBank), Thomas Selegny (RESALLIENCE)

Overview

As part of the ATLANTIS project, the Large-Scale Pilot 3 (LSP3), plays a pivotal role in advancing the resilience of European Critical Infrastructure (CI), especially in the financial sector. Bringing together a variety of service operators, LSP3 addresses escalating risks related to cyber incidents, natural hazards, and systemic failures, while emphasizing the need of a robust approach to continuity planning and operational governance.

This white paper provides a practical roadmap based on three key policy recommendations aimed at enhancing the capacity of CI operators to anticipate, withstand, and recover from disruptive events effectively.

Recommendation 1: Establish Minimum Business Continuity Objectives (MBCO) for Essential Functions

CI operators, working in coordination with business unit leaders and IT continuity teams, should establish and formalize Minimum Business Continuity Objectives (MBCOs) for each essential function. These MBCOs serve as benchmarks for designing realistic recovery strategies and setting achievable goals for IT restoration efforts.

When MBCOs are not defined, IT teams may either overestimate or underestimate the recovery requirements of critical operations, which they can lead to inefficiencies, prolonged outages and resources misallocation. Therefore, defining clear MBCOs enables targeted, risk-informed targeted recovery planning, reduces downtime and ensures better alignment between business priorities and tech capabilities.

This approach is consistent with legal obligations under the CER Directive [1]. Specifically, Article 12 requires Member States to ensure that critical entities conduct regular risk assessments to identify all relevant threats to their operations, while Article 13 mandates that those entities implement appropriate and proportionate technical, security, and organizational measures — such as business continuity planning — to ensure operational resilience.

In parallel, the NIS2 Directive [2] reinforces these expectations. Article 21 obliges Member States to ensure that essential and important entities adopt suitable technical, operational, and organizational measures to manage risks to network and information systems, and to prevent or minimize the impact of incidents on the continuity of their services.

Together, these regulatory frameworks underscore the importance of defining MBCOs as a foundational step in both resilience and compliance.

Recommendation 2: Implement Tiered Continuity Levels and Recover Plans

Continuity should incorporate tiered levels of recovery, allowing phased restoration of services based on their criticality. Jointly developed by continuity planners, IT disaster recovery experts, and sector-specific operational leads, these plans should prioritize the most critical functions first and outline sequential steps for broader recovery.

Gradual recovery reduces the risk of systemic collapse and mitigates cascading effects across interdependent systems. It enables organizations to maintain partial functionality during crises while providing structured visibility into the full restoration process.

This approach aligns with Article 13 of the CER Directive, which mandates that Member States ensure critical entities implement appropriate and proportionate technical, security, and organizational measures — based on risk assessments — to ensure operational resilience and manage disruptions. Article 14 further supports this by requiring personnel security measures, such as background checks, for roles critical to the continuity of essential services.

Moreover, the European Programme for Critical Infrastructure Protection (EPCIP) [3] encourages strategic, phased continuity planning as part of a broader risk-based framework for protecting vital systems across the EU.

Recommendation 3: Establish Resilience Committees within CI Operators

CI Executive leadership should define and institute dedicated Resilience Committees composed of decision-makers from key departments e.g., operations, IT, risk management. These bodies should be empowered to align business objectives with recovery capabilities oversee the implementation of continuity strategies, and address identified gaps to oversee the implementation and continuous improvement of continuity strategies.

In case of a dedicated governance structure vacuum, recovery efforts often lack coordination and accountability. Resilience Committees ensure coherent decision-making, foster a culture of preparedness, and continuously assess and refine continuity plans help bridge gaps between strategic planning and operational response.

This aligns with Articles 10, 11, and 12 of the CER Directive, which assign responsibilities to national competent authorities and emphasize the importance of governance structures within critical entities to ensure effective risk assessment, coordination, and resilience planning.

Furthermore, Chapter IV of the NIS2 Directive, particularly Article 20, underlines the need for clear accountability and governance in cybersecurity risk management. It requires executive management to oversee, approve, and monitor the implementation of security measures — further supporting the establishment of formal internal bodies like Resilience Committees to govern and guide resilience efforts.

Conclusions

The core challenge addressed by these recommendations is the misalignment between organizational expectations for continuity and the actual technical capacity to meet them. By implementing MBCOs, CI operators gain clarity on essential service thresholds for recovery. Tiered continuity strategies ensure a structured, prioritized return to operations, Governance through Resilience Committees ensures accountability, coherence and ongoing refinement of preparedness plans between executive decisions and operational reactions.

Altogether, these actions, when implemented across LSP3 stakeholders, will significantly bolster the resilience, reliability and governance of Europe's critical infrastructure services.

While the CER and NIS2 Directives provide the core legal requirements for resilience and continuity governance, it is equally important to recognize the broader strategic context in which these instruments operate. The establishment of internal governance mechanisms—such as Resilience Committees and structured risk management processes—should be viewed not only as compliance measures but as contributions to the European Union's wider policy ambitions.

In particular, the EU Security Union Strategy (2020–2025) underscores the need for a coordinated and forward-looking approach to safeguarding critical infrastructure, promoting resilience against both physical and hybrid threats. It highlights the role of cross-sectoral preparedness, public-private cooperation, and proactive risk governance — principles directly aligned with the governance structures discussed in this paper.

Furthermore, the EU Cybersecurity Strategy for the Digital Decade (2020) sets out a vision for a resilient digital Europe, underpinned by robust cyber governance across essential sectors. This strategy provides the political and strategic foundation for legislative measures such as NIS2 and encourages entities to adopt proactive, risk-based approaches to digital resilience.

Finally, in the context of long-term sustainability and systemic risk, the European Green Deal, including its resilience annex, calls attention to the urgent need to adapt critical infrastructure to the realities of climate change. This includes planning for extreme weather events, energy system shocks, and environmental disruptions. Integrating climate resilience into continuity planning not only supports operational stability but also contributes to the Union's climate adaptation and sustainability goals.

By embedding these broader policy priorities into internal governance and continuity planning, critical entities can demonstrate leadership, enhance cross-sector resilience, and align with the EU's strategic direction for a secure, digital, and climate-resilient future.

References

[1] **CER Directive**, "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC".
https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[2] **NIS2 Directive**, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148."
https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27

[3] European Programme for Critical Infrastructure Protection (EPCIP).
https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html

Front cover image by Microsoft Stock Images.