Skadden

The Standard Formula: A Guide to Solvency II

August 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Sebastian J. Barling
Partner / London
44.20.7519.7195
sebastian.barling@skadden.com

Robert A. Chaplin
Partner / London
44.20.7519.7030
robert.chaplin@skadden.com

David Y. Wang
Associate / London
44.20.7519.7149
david.y.wang@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

22 Bishopsgate
London EC2N 4BQ
44.20.7519.7000

Chapter 10

Governance Models

Introduction

Solvency II is organised around three core pillars of prudential regulation, which ensure the safety and soundness of (re)insurers, in line with the scale, nature and complexity of their business:

- **Pillar One** focuses on quantitative measures and regulatory capital requirements, detailed through the Solvency Capital Requirement, and the Minimum Capital Requirement, technical provisions, the matching adjustment and internal models.[299]
- **Pillar Two** addresses governance and risk management. It obligates (re)insurers to conduct a thorough Own Risk and Solvency Assessment (ORSA) and mandates the establishment of robust internal governance frameworks.[300]
- **Pillar Three** sets out transparency requirements for(re)insurers to regularly disclose pertinent financial information to both regulators and the public.

This chapter focuses on Pillar Two, which sets out a system of governance requirements for (re)insurers under the Solvency II framework. This governance framework must integrate sound management practices, effective risk management strategies and clearly defined lines of responsibility. The Solvency II Directive requires the governance system to not only be comprehensive but also dynamic, including regular evaluations to address any significant shifts in the (re)insurer's risk profile or operating conditions.

The European Insurance and Occupational Pensions Authority (EIOPA) has supplemented such requirements with detailed guidance, emphasising the necessity of a well-integrated system that aligns with the broader organisational structure.[301] (Re)insurers are expected to ensure that governance practices are not only robust but also adaptive to changes, ensuring that they remain compliant with regulatory expectations.

Central to this governance system are the requirements for regular and systematic reviews. These reviews must be conducted at least annually or whenever there are material changes in the (re)insurer's risk environment. The aim is to ensure that governance structures remain effective and relevant in the face of evolving risks and operational challenges.

[299] These are detailed in our prior publications as follows: Chapter 1 (Own Funds), Chapter 2 (Reinsurance and Risk Transfer), Chapter 5 (Matching Adjustment), Chapter 7 (Technical Provisions), Chapter 8 (Capital Requirements) and Chapter 9 (Internal Models).

[300] Articles 40 to 49 Solvency II Directive, as implemented in the UK by the Conditions Governing Business Part of the *PRA Rulebook* and the Insurance Part of the *PRA Rulebook*.

[301] EIOPA, *Final Report on Consultation Paper No. 14/017 on Guidelines on Own Risk and Solvency Assessment* (2015).

In the context of UK (re)insurers, under the Senior Managers and Certification Regime (SMCR) the Prudential Regulation Authority (PRA) supplements the governance requirements under Solvency II.[302] Although the SMCR operates independently from Solvency II, it is designed with Solvency II in mind, enhancing and completing the governance standards set out therein.

Own Risk and Solvency Assessment (ORSA)

The Own Risk and Solvency Assessment (ORSA) is a fundamental aspect of the Solvency II framework, representing a (re)insurer's own perspective on its risk profile, and the capital and other resources needed to address these risks.[303] This assessment must cover each part of a (re)insurer's business and operations. EIOPA suggests that such processes should be tailored to and independently developed by a (re)insurer, tailored to its organisational structure, risk management framework and proportionate to its business.[304] According to the ORSA Guidelines, each (re)insurer must develop its own processes tailored to its organisational structure and risk management system, reflecting the nature, scale and complexity of the risks inherent in its business.

The ORSA must be comprehensive, involving input from across the organisation and going beyond merely producing a report or completing a template. The assessment should:

- Reflect all material risks, including those arising from assets, liabilities and intragroup and off-balance sheet arrangements.
- Incorporate the firm's management practices, systems and controls, including risk mitigation techniques.
- Evaluate the quality of processes and inputs, particularly the adequacy of the governance system.
- Connect business planning with solvency needs, factoring in the specific risk profile, approved risk tolerance and strategic business objectives of the firm.
- Identify possible future scenarios.
- Address external stress factors.
- Use a consistent valuation basis throughout the solvency needs assessment.

The ORSA should be forward-looking, encompassing medium and long-term perspectives to capture all material risks adequately. The PRA expects firms to consider risks over the "ultimate time horizon" — the period until all obligations to policyholders have run off — as part of their ORSA.[305]

The ORSA must also ensure continuous compliance with the firm's Solvency Capital Requirement (SCR) and Minimum Capital Requirement (MCR). This includes assessing deviations from the assumptions underlying the SCR. While firms have some flexibility in conducting this assessment, the PRA has specific expectations regarding compliance with regulatory capital and technical provisions, as well as the assessment of any significant changes in the risk profile. The calculation of technical provisions must be validated annually, particularly through comparison against experience.

The board of a (re)insurer holds ultimate responsibility for the firm's compliance with applicable laws and regulations under Solvency II.[306] The board must interact effectively with any committees, senior management and key function holders, taking an active role in the ORSA process. This includes challenging the assumptions behind SCR calculations to ensure they align with the firm's risk profile. The board should leverage insights from the ORSA when approving the firm's short and long-term capital plans, and the ORSA should be a standing agenda item in relevant board and committee meetings, with discussions recorded in the minutes.

In addition to maintaining a formal ORSA policy, (re)insurers must keep a record of each ORSA, prepare internal and supervisory reports and assess any deviations from the assumptions underlying SCR calculations. The results and conclusions of the ORSA should be communicated to all relevant staff after board approval.

Firms must also document specific processes involved in the ORSA, such as data collection, quality analysis and the selection of assumptions used in technical provisions calculations.

The PRA states that the ORSA should be a dynamic, iterative process, continuously refined as the business environment and risk landscape evolve.[307] (Re)insurers are expected to establish a "feedback loop" where ORSA outcomes directly influence the firm's risk management framework, strategic decisions and capital planning. This ensures that the ORSA is iteratively improved and remains an integral part of risk management and strategic planning, rather than a mere annual compliance task.

Moreover, the PRA mandates that the board of a (re)insurer must actively engage in the ORSA process.[308] This involves setting the risk appetite, reviewing the ORSA outcomes and ensuring they are fully integrated within the broader risk management framework. The PRA emphasises that the ORSA should generate meaningful management information, supporting informed decision-making and fostering an organisation-wide culture of risk awareness and strategic alignment regarding the (re)insurer.

[302] Senior Management Functions Part of the *PRA Rulebook*.

[303] Article 45 Solvency II Directive.

[304] EIOPA, *Final Report on Consultation Paper No. 14/017 on Guidelines on Own Risk and Solvency Assessment* (2015).

[305] PRA, *Supervisory Statement SS26/15 – Own Risk and Solvency Assessment (ORSA)*, paragraph 3.6.

[306] Article 41 Solvency II Directive.

[307] PRA, *Supervisory Statement SS5/18 – Solvency II: The ORSA and the Role of the Board*, paragraph 2.4, 2018

[308] *Id* at paragraph 3.1, 2018.

Climate Change

In April 2021, EIOPA issued an opinion on the climate risk scenarios.[309] This opinion outlines EIOPA's expectations for how EU National Competent Authorities (NCAs) should oversee the integration of climate change risk scenarios by undertakings in their ORSA.

Key points from the opinion include that (a) firms should identify material climate change risks relevant to their business, or, if they conclude that climate change is not a material risk, they should provide a rationale for this conclusion; and (b) both physical and transition risks should be considered, mapping these to traditional prudential risk categories such as underwriting and market risk.

EIOPA expects firms to assess both short-term and long-term climate change risks and to adjust their time horizons for stress testing and scenario analysis accordingly.

Note that this opinion was published after the Brexit Transition Period and is not directly applicable to UK firms, however, it covers similar topics to those addressed in the PRA Supervisory Statement SS3/19.

Risk Management, Compliance and Audit Functions

Solvency II mandates various key governance functions that are critical to ensuring robust risk management within (re)insurers. These functions include risk management, compliance, internal audit and actuarial, each with specific delineated roles and responsibilities defined by the Solvency II Directive:

- **Risk Management:** Solvency II requires (re)insurers to establish an effective risk management system. This system should include strategies, processes and reporting procedures designed to identify, measure, monitor, manage and report risks on a continuous basis. The scope of this function encompasses underwriting, asset-liability management, investment, liquidity, concentration risk, operational risk and reinsurance (or other risk mitigation techniques).[310]
- **Compliance Function:** The compliance function is responsible for ensuring that the (re)insurer adheres to applicable laws, regulations and administrative provisions. It must also assess the potential impact of legal and regulatory changes on the (re)insurer's operations, often referred to as "horizon scanning."[311] The function is also responsible for developing and updating internal compliance policies and ensuring that all staff receive adequate training on regulatory changes and compliance requirements.
- **Internal Audit Function:** Solvency II requires the internal audit function to be independent from operational activities within the (re)insurer. This function provides the board and senior management with assurance about the adequacy and effectiveness of the internal control system and other governance elements, and must report directly to the board without influence from operational management. The internal audit function must regularly evaluate the firm's governance practices, identify weaknesses and recommend necessary improvements. Its independence ensures objective insights into the firm's operations, free from undue influence.[312]
- **Actuarial Function:** The actuarial function is tasked with the accurate calculation of technical provisions, ensuring the appropriateness of methodologies, models and assumptions. It also assesses the sufficiency and quality of data, compares best estimates against actual experience and reports to the board on the reliability of these calculations. The actuarial function is critical for maintaining sufficient reserves to meet obligations, thereby securing the (re)insurer's solvency and protecting policyholders.[313]

Additional Key Functions

The PRA recognises that additional functions may be classified as key, depending on the specific nature of the (re)insurer's business. These may include the investment function, claims management, IT and reinsurance. The classification of these functions as key depends on their criticality to the firm's operations, the complexity and materiality of the risks they manage and the potential impact of their failure on the firm's solvency and policyholders.

SMCR

Overview

The PRA has introduced the principle of individual responsibility and accountability on the basis that regulation will be more effective if senior individuals at insurers are personally responsible for certain areas.

PRA Fundamental Rules and FCA Principles for Business

A number of high-level principles are imposed on UK (re)insurers, which they are expected to meet at all times, and the breach of which could give rise to enforcement action against the firm by the regulators — the PRA's high level principles are known as "Fundamental Rules," while the Financial Conduct Authority (FCA) has "Principles for Businesses." It is vital that the boards and senior management understand these rules and establish within their firms a culture that supports adherence to them.

[309] EIOPA, *Opinion on the Supervision of the Use of Climate Change Risk Scenarios in ORSA* (EIOPA-BoS-21-127, 2021); PRA Supervisory Statement SS3/19.

[310] Article 44 Solvency II Directive.

[311] Article 46 Solvency II Directive.

[312] Article 47 Solvency II Directive.

[313] Article 48 Solvency II Directive.

The PRA Fundamental Rules are:

- A firm must conduct its business with integrity (FR1).
- A firm must conduct its business with due skill, care and diligence (FR2).
- A firm must act in a prudent manner (FR3).
- A firm must at all times maintain adequate financial resources (FR4).
- A firm must have effective risk strategies and risk management systems (FR5).
- A firm must organise and control its affairs responsibly and effectively (FR6).
- A firm must deal with its regulators in an open and cooperative way and must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice (FR7).
- A firm must prepare for resolution so, if the need arises, it can be resolved in an orderly manner with a minimum disruption of critical services (FR8).

The FCA's Principles for Business are:

- A firm must observe proper standards of market conduct (PRIN 5).
- A firm must pay due regard to the interests of its customers and treat them fairly (PRIN 6).
- A firm must pay due regard to the information needs of its clients, and communicate information to them in a way that is clear, fair and not misleading (PRIN 7).
- A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client (PRIN 8).
- A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely upon its judgment (PRIN 9).
- A firm must arrange adequate protection for clients' assets when it is responsible for them (PRIN 10).
- A firm must act to deliver good outcomes for retail customers (PRIN 12).

Note also that the FCA has rules under its Principles for Business overlapping with the PRA's Fundamental Rules set out above — PRIN 1 to 4 and PRIN 11.

Senior Management Functions

Officers, directors and persons who exercise senior management functions (known as SMFs) or "controlled functions" under FSMA (for example, the director function, chief executive function, actuary function or systems and controls function) must be approved by the FCA or the PRA (or both) before performing such functions.[314]

Once approved to perform such functions, the person in question becomes subject to the SMCR and accompanying conduct rules that impose several significant responsibilities on the individual, including a duty to comply with regulatory requirements, general principles and expectations on an ongoing basis.

In connection with the Risk Management, Compliance and Audit Functions required under Solvency II, the SMCR assigns the responsibility for key governance functions to senior management of (re)insurers, in alignment with Solvency II's broader regulatory framework, reinforcing individual accountability at the highest levels.

These SMFs are the (a) chief compliance officer, (b) chief risk officer, (c) chief internal auditor and (d) chief actuary.

As stated above, SMFs must be approved by the PRA before assuming their roles. The PRA expects firms only to put forward suitable individuals for SMF appointments, assessing their fitness and propriety, experience and qualifications. The PRA will not merely accept any appointments and will challenge appointments that it considers inappropriate or unsuitable, particularly for (re)insurers of certain sizes and systemic importance to the UK (or global) financial system.

The Conduct Rules

A number of more detailed requirements are imposed on both firms and individuals in relation to particular areas, including governance.

Further, the conduct rules for Senior Managers include (in both the *FCA Handbook* and the *PRA Rulebook*):

- Individual Conduct Rule 1: You must act with integrity.
- Individual Conduct Rule 2: You must act with due skill, care and diligence.
- Senior Manager Conduct Standard 1: You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively.
- Senior Manager Conduct Standard 2: You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with relevant requirements and standards of the regulatory system.

[314] Senior Management Functions Part of the *PRA Rulebook*.

- Senior Manager Conduct Standard 3: You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively.
- Senior Manager Conduct Standard 4: You must disclose appropriately any information of which the FCA or PRA would reasonably expect notice.
- Senior Manager Conduct Standard 5: When exercising your responsibilities, you must pay due regard to the interests of current and potential future policyholders in ensuring the provision by the firm of an appropriate degree of protection for their insured benefits.

Management Responsibilities Map

Further, (re)insurers are required to put in place a management responsibilities map.[315] The responsibilities map must provide a comprehensive overview of the firm's management and governance arrangements, detailing how responsibilities are allocated among senior managers, and indicating whether these responsibilities are shared or divided.

The map must clearly delineate the roles and responsibilities of each SMF holder. It should specify the individual accountabilities for key areas of the business, ensuring that there is no ambiguity about who is responsible for what.

The map must outline the firm's overall governance structure, including the reporting lines and the interaction between different governance functions. This should encompass the roles of the board, senior management and key functions such as risk management, compliance, internal audit and actuarial. The map should also detail any committees established by the board, including their membership and how they relate to the broader governance framework.

The responsibilities map must be documented comprehensively and kept up to date. It should be readily accessible to the PRA upon request, demonstrating the firm's commitment to transparency and regulatory compliance. Regular updates are necessary to reflect any changes in the governance structure, such as new appointments, reassignments or changes in responsibilities. The map must also integrate with the firm's risk management framework, ensuring that all key risks are appropriately managed by designated individuals or functions.

Ultimately, the board holds responsibility for ensuring that the management responsibilities map is accurate and effective. The board must review the map regularly, particularly when there are significant changes to the firm's structure or operations. The map should be used as a tool to facilitate board oversight, enabling the board to ensure that all responsibilities are appropriately allocated and that senior managers are held accountable for their areas of responsibility.

Outsourcing

Outsourcing is a critical consideration for global financial groups and regulators, including (re)insurers operating across multiple jurisdictions with dependencies outside their home state. Outsourcing encompasses any function that a (re)insurer could perform internally, such as claims administration, claims management and investment management.

Solvency II mandates that outsourcing must not compromise the quality of a (re)insurer's governance system.[316] (Re)insurers are required to maintain ultimate responsibility for outsourced functions and ensure effective oversight. This involves rigorous due diligence, clear contractual arrangements with robust enforcement and monitoring mechanisms and continuous monitoring of outsourced activities.

EBA Outsourcing Guidelines

In addition to the rules under Solvency II, (re)insurers are also subject to certain guidelines from the European Banking Authority (EBA) on outsourcing.[317] Note that these apply broadly across the financial services sector (and not just to (re)insurers), including to banks, investment firms, payment institutions and electronic money institutions. The EBA Outsourcing Guidelines set out detailed expectations for how financial institutions should manage outsourcing arrangements, particularly for critical or important functions. The principles established by the EBA are designed to ensure that outsourcing does not compromise the firm's operational resilience, governance or regulatory compliance, making them highly relevant for (re)insurers operating under Solvency II.

The requirements are:

- **Critical and Important Functions:** The EBA guidelines place significant emphasis on the identification and management of critical or important functions. (Re)insurers must ensure that any outsourced activities deemed critical or important do not adversely affect their overall risk management capabilities or their ability to comply with regulatory obligations. This includes comprehensive risk assessments prior to outsourcing, ensuring that the service provider has the necessary ability and capacity to deliver the services effectively without compromising the (re)insurer's governance or operational resilience.

[315] Senior Managers and Certification Regime: Management Responsibilities Map Part of the *PRA Rulebook*.

[316] Article 49 Solvency II Directive.

[317] EBA, *Guidelines on Outsourcing* (EBA/GL/2019/02, 2019) (EBA Outsourcing Guidelines).

- **Risk Management and Operational Resilience:** The guidelines stress that outsourcing arrangements should not diminish a firm's control over critical operations. (Re)insurers must establish robust mechanisms to manage outsourcing risks and maintain operational resilience. This includes the implementation of contingency plans and exit strategies to mitigate the risk of service disruptions. Continuous oversight is essential, with (re)insurers required regularly to review and test their resilience against various risk scenarios, particularly those related to critical outsourced functions.
- **Sub-outsourcing and Oversight:** The EBA guidelines introduce specific considerations for sub-outsourcing, where a service provider may further outsource a portion of the services it is contracted to deliver. (Re)insurers must ensure that they retain adequate oversight and control over the entire outsourcing chain, including sub-outsourcing arrangements. This involves ensuring that the original service provider remains accountable and that all sub-outsourcing agreements meet the same rigorous standards of governance, risk management and operational resilience as the primary outsourcing agreement.
- **Data Security and Confidentiality:** Another key aspect of the EBA guidelines is the protection of data. (Re)insurers must ensure that outsourced services, particularly those involving the processing of sensitive or personal data, adhere to stringent data security and confidentiality standards. This includes ensuring compliance with relevant data protection regulations, such as the General Data Protection Regulation (GDPR), and establishing clear protocols for data access storage, and transfer within the outsourcing arrangements.
- **Governance and Board Accountability:** The EBA guidelines reinforce the need for governance structures that ensure senior management and the board retain full accountability for outsourced activities. This aligns closely with Solvency II's requirements, where the board must oversee outsourcing arrangements, ensuring they do not dilute the firm's governance framework. Boards are required to approve outsourcing policies, oversee the selection of service providers and ensure that any outsourcing arrangement does not impede the firm's ability to meet its regulatory obligations.[318]
- **Documentation and Reporting:** Comprehensive documentation is crucial under the EBA guidelines. (Re)insurers must maintain detailed records of all outsourcing arrangements, including the rationale for outsourcing, due diligence processes, risk assessments and ongoing monitoring activities. These records must be readily available for regulatory review, demonstrating that the (re)insurer maintains effective oversight of all outsourced functions. Regular reporting to the board on the performance and risks associated with outsourcing arrangements is also essential, ensuring that the board remains informed and engaged in overseeing these critical aspects of the firm's operations.

[318] Article 49 Solvency II Directive.

In the UK, these requirements remain applicable post-Brexit, by way of PRA Supervisory Statement 2/21.[319] Importantly, the PRA and the FCA take the view that an intragroup outsourcing is still considered outsourcing (notably, even within the same entity, *e.g.*, a (re)insurance branch and its head office), and requires such outsourcing to be subject to the same requirements as outsourcing to third-party providers. The regulators caution against assuming that intragroup arrangements carry less risk. Therefore, (re)insurers must approach intragroup outsourcing with the same level of scrutiny and control as external outsourcing. The PRA acknowledges that compliance can be proportional, depending on the level of control and influence the (re)insurer has over the entity providing the outsourced service.

Connection With the SMCR

Importantly, boards and senior management, especially those in Senior Management Functions (SMFs), cannot delegate their accountability. They remain responsible for the monitoring and supervision of outsourced functions, ensuring that the (re)insurer's governance framework remains robust.

Board and Governance Structures

Responsibility for the aforementioned requirements is with the board of a Solvency II (re)insurer, which is ultimately responsible for ensuring that the company adheres to all regulatory requirements, including the establishment and maintenance of robust governance structures. The board must set the tone at the top, ensuring a culture of risk awareness and regulatory compliance permeates throughout the organisation.[320]

The board must oversee key governance functions set out above (including risk management, compliance, internal audit and actuarial functions), ensuring that these areas operate independently and effectively.

The board must ensure that the governance framework remains effective and is regularly reviewed to adapt to changes in the business environment or regulatory landscape, including setting up appropriate committees, such as audit, risk and compliance committees, to focus on specific areas of governance and provide detailed oversight.

The board is also responsible for ensuring that the firm's governance framework includes measures to ensure operational resilience, particularly in the face of external shocks or disruptions. This involves overseeing the implementation of business continuity plans and ensuring that critical functions can continue to operate effectively under stress conditions.

[319] PRA, *Supervisory Statement SS2/21 – Outsourcing and Third-Party Risk Management*.

[320] PRA, *Supervisory Statement SS5/18 – Solvency II: The ORSA and the Role of the Board*, 2018.

Operational Resilience

Overview

Lastly, operational resilience is a critical component of a (re)insurer's governance framework under Solvency II and the PRA's supervisory expectations. It is also an area of increasing regulatory scrutiny across all financial services sectors. It encompasses a range of strategies and measures designed to ensure that a firm can continue to operate and serve its policyholders, even in the face of significant disruptions.[321]

A foundational element of operational resilience is the identification of critical business services that, if disrupted, could have severe consequences for policyholders and the broader market. This step requires a thorough analysis of the services most essential to the firm's operations and their potential impact if disrupted.

(Re)insurers must develop tailored mitigation and recovery plans that address specific operational risks. These plans should be robust and adaptable, designed to manage and recover from disruptions swiftly, and should include establishing comprehensive business continuity plans, incident response strategies and frameworks to manage risks associated with outsourcing critical functions.

To assess a firm's ability to withstand various risks, (re)insurers must conduct scenario analysis and stress testing. These exercises help identify vulnerabilities and gauge the firm's preparedness to respond to and recover from different types of disruptions, ensuring resilience in adverse conditions.

Governance is central to ensuring that operational resilience measures are effective and regularly reviewed. Senior management and the board must be actively involved in overseeing the firm's resilience strategies, ensuring they are continuously updated to reflect changes in the risk environment and operational landscape. This active oversight aligns with the broader governance requirements under Solvency II and is crucial for maintaining the firm's stability and compliance.

[321] PRA, *Supervisory Statement SS1/21 – Operational Resilience: Impact Tolerances for Important Business Services*, 2021.

Digital Operational Resilience Act (DORA)

The EU's Digital Operational Resilience Act (DORA), coming into effect on 17 January 2025, introduces additional requirements that (re)insurers in the EU must adhere to, some of which extend beyond the existing Solvency II framework and the under the EBA Outsourcing Guidelines.[322] While some of the requirements overlap, DORA goes beyond in many measures, bringing into scope all information and communication technology (ICT) risks so as to ensure digital resilience and ensuring continuity of operations in a rapidly evolving digital environment.

In-scope (re)insurers are required to:

- Establish and maintain a comprehensive ICT risk management framework that addresses the specific risks associated with digital operations.[323]
- Implement continuous monitoring and control of ICT systems to ensure their resilience against potential threats.[324]
- Conduct advanced digital operational resilience testing, including threat-led penetration testing, to identify and address vulnerabilities.[325]
- Develop a robust third-party risk management function to oversee and mitigate risks associated with outsourcing digital services.[326]
- Establish an incident classification and reporting framework to ensure timely and accurate reporting of ICT-related incidents to regulatory authorities.[327]
- Develop and maintain business continuity and IT service continuity plans, including secure and segregated backup systems to ensure operations can continue during disruptions.[328]
- Define clear governance structures that hold top management accountable for ICT risk management, ensuring that resilience is embedded at the highest levels of the organisation.[329]

[322] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (DORA).

[323] Article 10 DORA

[324] Article 11 DORA.

[325] Article 23 DORA.

[326] Article 25 DORA.

[327] Article 17 DORA.

[328] Article 13 DORA.

[329] Article 5 DORA.