# FINEOS Assists the Delivery of Operational Resilience

When insurers make the decision to take advantage of cloud services today, operational resilience must be to the fore. Across the globe this topic is being given increasing prominence through a growing body of regulation[1].

Regulation calls out wide-ranging requirements including:

- the identification and monitoring of critical third-party relationships,
- requirements to strengthen risk governance and management, and
- guidance around business continuity and exit planning.

FINEOS helps its regulated insurance customers and users address and strengthen their operational resilience to manage operational risk at the enterprise level in a way that is consistent with regulatory guidelines. The FINEOS Platform offers the highest levels of resilience through state-of-the-art design such as secure and resilient cloud operations, use of automation, and implementation of zero trust.

A common feature across the various regional regulations is that they encourage insurers to take a principled, risk-based, and technology neutral approach to addressing operational risk. The majority of such regulation recognises that these risks also exist in an on-premises environment.

Beyond operational aspects, regulations also highlight non-operational risks in relation to outsourcing, in particular financial insolvency risks and resolution approaches. Non-operational risks can't be managed through technological measures but instead are addressed with legal measures during the contracting phase and by invoking the exit strategy.

## FINEOS recommends a five-step approach for managing operational risk in the insurance sector

There are several elements that must be considered before making critical choices on how to manage operational risks, which is why FINEOS recommends a five-step approach to strengthening operational resilience:

**Step 1**
Update cloud risk governance

**Step 2**
Assess alternatives to provider dependency

**Step 3**
Plan legacy modernisation

**Step 4**
Test business continuity plan

**Step 5**
Prepare exit plans

## Step 1
## Update cloud risk governance

Cloud technology in financial services regulation has historically been achieved through third-party outsourcing guidelines that apply specifically in this context, with different sets of regulation applying to the on-premises ICT environment.

More recent regulation, such as DORA, take a holistic approach when it comes to strengthening operational resilience, making little or no distinction between on-premises systems and cloud-based ones. In addition, DORA determines that an insurer's intra-group IT department should be seen as a 3rd party provider, governed by the same terms as an outside vendor.

FINEOS recommends that insurers revisit internal risk governance frameworks and holistically incorporate these new operational resilience measures.

Risk governance frameworks must also be updated annually to ensure continued compliance in a rapidly evolving regulatory landscape.

*"While intra-group provision of ICT services entails specific risks and benefits, it should not be automatically considered less risky than the provision of ICT services by providers outside of a financial group and should therefore be subject to the same regulatory framework."*

**Recital (31) of the EU Digital Operational Resilience Act (DORA)**

## Step 2
## Assess alternatives to provider dependency

Third-party provider dependency is commonplace today across many critical institutional services, and it may not be feasible to eliminate it.

For instance, consider the pervasive nature of financial information networks like Bloomberg or Thomson Reuters and large software vendors like Microsoft, IBM and Oracle. Complete substitution of any of these would be challenging. A financial services institution can devise an exit plan for a specific third-party service, but it becomes difficult to discontinue all use of a third-party solution. Therefore, the focus should be on reducing concentration risk so that it stays within an organization's risk tolerances.

The strategic imperative to minimise concentration risk also makes a strong case for selecting modular, component-based, solutions from vendors rather than end-to-end or turnkey solutions where replacing one service can be tricky.

When assessing such concentration risks, financial services institutions must evaluate each of the underlying threat scenarios, leading in turn to a more nuanced view that includes both benefits and drawbacks associated with concentration of services. Threat factors to consider include data centre disasters, hardware failures, network outages, cyber-attacks, faulty changes and upgrades, human errors etc. For each of these appropriate mitigating measures should be carefully considered. Firms must also consider mitigation costs, complexity, and availability of in-house skills when considering their preferred approach to deliver operational resilience.


Copyright 2024 © FINEOS Corporation Ltd

## Step 2
Assess alternatives to provider dependency (continued)

Enhancing operational resilience often involves managing concentration risk rather than entirely eliminating third-party dependencies, which may not always be feasible or desirable. To strengthen resilience, firms can focus on mitigating underlying threat scenarios associated with concentration risk, such as regional data center disasters.

This can be achieved by:

- Lowering the probability of threat events through robust resilience measures in solution design. FINEOS, in partnership with our insurance customers, implements rigorous risk management procedures, including state-of-the-art infrastructure, a zero-trust security model, regular system updates, validated business continuity plans, and modular technologies. Each of these measures contributes to creating a highly resilient environment.
- Limiting the impact of threats by reducing risk at lower levels through the design of services that operate across multiple availability zones, ensuring adequate redundancies and recovery mechanisms (e.g., highly available architecture with automated failover), and leveraging geo-redundant designs. FINEOS works closely with our infrastructure partner AWS to deliver this capability to our customers. Such configurations not only result in higher resilience and better SLAs, but also help to mitigate against threats such as the loss of a single data centre or even an entire region due to their distributed nature. This approach surpasses what is typically achievable in on-premises or hybrid scenarios.

## Step 3
Plan legacy modernisation

Many Operational Resilience regulations place particular focus on legacy systems. DORA defines them as follows:

*"'Legacy ICT system' means an ICT system that has reached the end of its lifecycle (end-of-life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity."*

The simplest and easiest scenario to address is when a solution licensed or purchased from a vendor years ago can no longer be supported by the vendor.

More difficult to identify, and to deal with, are legacy in-house systems where the knowledge and skill that was present at their inception is no longer within the firm. DORA does distinguish between the obligation placed on systems sourced from outside vendors and those provided and maintained by in-house IT teams.

Another characteristic of aged legacy systems, particularly those deployed on mainframes, is that they were designed in an era where single service, or monolith, software was the norm. These legacy systems require special attention and careful phase-out plans.


Copyright 2024 © FINEOS Corporation Ltd

## Step 4
Test business continuity plan

Testing a business continuity plan is essential for ensuring its effectiveness, identifying and addressing weaknesses, complying with regulations, maintaining stakeholder confidence, and continuously improving resilience capabilities.

## Step 5
Prepare exit plan

Some threat scenarios can't be managed with business continuity plans or technical resiliency measures, such as the risk of bankruptcy or resolution of the third-party provider, or their underlying infrastructure partner. An exit plan has the benefit of dealing with such catastrophic scenarios and should be seen as complimentary to having tested business continuity plans.

This is why every organization should develop a comprehensive exit strategy along with individual exit plans for its critical use cases, as these are essential for compliance with various regulations and future guidelines.

The regulatory demands on the insurance industry are constantly evolving and maintaining compliance grows harder every day – at the same time, the costs of non-compliance grow at an even faster rate.

FINEOS collaborates closely with our insurance clients to bolster their operational resilience and compliance efforts. We have a specialized team of compliance experts embedded within our product organization, dedicated to providing ongoing support. Led by the FINEOS Chief Information Security Officer (CISO), our team spearheads the advancement, implementation, and integration of both existing and novel cybersecurity frameworks, strategies, policies, and processes. These initiatives are meticulously aligned with industry standards and best practices, ensuring the highest levels of security and regulatory adherence.

1 Including, but not limited to:
- Financial Stability Board (FSB) consultation on enhancing third-party risk management and oversight (22 June 2023 FSB Consultation)
- The EU Digital Operational Resilience Act (DORA)
- Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 230 Operational Risk Management
- UK PRA Discussion Paper 'Operational resilience: critical third parties to the finance sector' (UK DP3/22)
- Canada Third Party Risk Guidelines
- Monetary Authority of Singapore's establishment of a Cloud Resilience Forum


Copyright 2024 © FINEOS Corporation Ltd