GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

IAIS Operational Resilience Working Group meeting in Washington DC – 19 March 2025

Operational Resilience Working Group Stakeholder Engagement Questions

Operational Resilience Frameworks

As technology is evolving, threats are evolving too, what are the key characteristics that an operational resilience framework should have in order to keep pace with innovation and be a tool used by undertakings to proactively monitor their risks?

Frameworks should be tailored to the specific entity's risk profile, which will be a function of multiple variables including size, portfolio, attack surface, etc. An effective framework should include elements of all the following, scaled up or down as appropriate to the organisation:

- Adaptable and flexible – a framework should be capable of evolving alongside technological advancements and emerging threats.
- Risk-based approach – should prioritise critical functions and assets, ensuring that risk mitigation is focused on high-impact areas. (For some organisations, this may include adopting real-time threat intelligence services/sharing)
- Scenario-based stress testing
- Align with established industry standards and applicable regulation – a framework should align with legal and industry-specific regulations (e.g., NIST, ISO 27001, DORA).
- Robust incident response & recovery plan that defines procedures for identifying, responding to, and recovering from disruptions.
- Cross-functional coordination to ensure collaboration between cybersecurity, IT, risk management, and business continuity teams.
- Third-party & supply chain risk management to assess and manage risks associated with external vendors and service providers.
- Training
- Comprehensive risk management
- Board oversight and engagement
- Proportional approach, continuous improvement and adaptation

As a global industry operating across multiple jurisdictions, what specific aspects of operational resilience supervision would benefit most from international harmonization via this Application Paper, and where would you prefer to maintain jurisdictional flexibility to account for regional differences?

With the understanding all of this is nonbinding, aspects of operational resilience supervision benefiting from international harmonisation:

- Common definitions & terminology – Having a shared language for operational resilience concepts to ensure consistency across jurisdictions would be helpful, relying on existing international definitions where possible.
- Minimum resilience goals – Setting baseline thresholds for risk management, business continuity, and incident response frameworks.
- Cross-border incident reporting & response protocols – Harmonising requirements for timely reporting, information sharing, and coordinated responses to global disruptions.
- Stress testing & scenario analysis – Having minimum guidelines for assessing resilience under different disruptive scenarios, fostering systemic stability.
- Alignment of standards and information-sharing protocols
- Data protection & privacy standards – Aligning with global best practices (e.g., GDPR, ISO 27001) to reduce compliance complexity for multinational entities.

Harmonisation may be too much, and flexibility is necessary in the following areas:

- Local regulatory & legal compliance – National laws, especially regarding data sovereignty, consumer protection, and financial regulations will require some flexibility.
- Regulatory expectations for cyber resilience – Notwithstanding the bullet about having minimum resilience goals above, standardising cybersecurity best practices, such as threat intelligence sharing, penetration testing, and disaster recovery plans may benefit from some general guidelines, but they must also be flexible.
- Proportionality in implementation and governance structures

Critical Services

Our draft Application Paper emphasizes the importance of setting impact tolerances to critical services. What practical challenges has your organization faced in establishing and maintaining these tolerances across different types of critical services, and how have you addressed the trade-offs between operational resilience investment and business efficiency?

Challenges in setting and maintaining impact tolerances:

- Define critical services clearly – It's hard to decide which services are "critical" across different teams and regions.
  - Possible solution: Create a common framework to encourage consistency where possible while recognising that there will be jurisdictional differences. We recommend that any common framework be aligned with and provide allowances for existing regulatory frameworks.
- Measure tolerances accurately – Setting clear limits on acceptable downtime is difficult.
  - Possible solution: Use past incidents and industry data to set realistic tolerance levels.
- Balancing strictness vs. practicality – Stricter limits mean higher costs and more resources.
  - Solution: Focused investments on the most critical services first.
- Dependencies on third-party vendors – Suppliers may not meet our resilience expectations.

    - Solution: Add resilience requirements into contracts and actively monitor vendors.
- A one size fits all approach is not appropriate for all third-party providers. Risks associated with a third party will vary depending on the relationship. Whatever requirements are put into contracts should reflect the risk profile of the relationship with the third party.

Should there be more regulatory guidance on handling prolonged IT outages (e.g. lasting more than 48 hours)?

- Not sure this is necessary, and unclear what value it would add absent aligning expectations. Most large organisations will be in the best position to navigate prolonged outages if they prepare (and larger organisations generally have shown they do.)
- If guidance is provided, it should emphasise the importance of aligning operational resilience standards across global regulators and enhancing information-sharing protocols and cross-border cooperation.

Third-Party Risks

Given the increasing reliance on third-party service providers, what specific contractual provisions or monitoring practices have proven to be most effective in managing operational resilience across your supply chain, particularly with regard to nth-party dependencies that may not be immediately visible?

- Insurers have found it important to adopt a comprehensive and robust approach to operational resilience, including aligning resilience strategies with existing regulatory definitions and standards to ensure uniformity across supervisory authorities.
- Some of the specific third-party contractual provisions that individual insurers have used effectively include:
    - Clear service level agreements with performance metrics.
    - A right to audit under certain circumstances the services being provided by third-party and nth party providers.
    - Incident reporting and response obligations with predefined escalation procedures based on jurisdictional requirements.
    - Data security and compliance requirements aligned with regulatory obligations.
- It is very important to keep in mind the importance of proportionality, particularly because insurers may have more leverage over smaller third-party data providers focused on insurance services, but many servicers are unwilling to allow auditing or other individualised risk controls

What practical steps do you take to assess and address nth-party risks?

- Critical role of board oversight and a holistic approach to operational resilience.
- Continuous monitoring tools, regular third-party risk assessments and (as appropriate) audits, risk-mapping to identify nth-party risk.

GFIA
GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

Cyber Risks

From your perspective, what specific supervisory practices would be the most effectively to drive improvements in technology and cyber risk management while accommodating differences in insurers' size, complexity, and business models?

- It is very important that supervisory practices be proportional and take into account regional and jurisdictional circumstances rather than imposing uniform requirements.
- Proportionality should be risk-based. Regulators should consider a tiered supervisory approach that adjusts scrutiny based on insurers size, complexity, and risk exposure, and "customised" compliance requirements to align with an insurers business model while still aligning with core cybersecurity principles.
- Clear guidance can be helpful on the expected level of board involvement at the holistic level to ensure operational resilience.
- To support consistency across supervisory authorities, it is important that supervisors align their definitions and expectations with existing regulatory frameworks.
- It is very important to have enhanced supervisory engagement & collaboration in the form of an ongoing dialogue and partnership between regulators and insurers to discuss emerging threats and best practices, to update each other, and ensure both parties are aligned in expectations/understandings.

Incident Reporting

How has your organization's approach to testing operational resilience scenarios evolved in recent years, and what metrics have you found most useful for evaluating whether your critical services can withstand disruption within your defined impact tolerances?

- A shift from periodic to continuous testing – we've moved away from annual or quarterly resilience exercises to ongoing, scenario-based testing which streamlines into our operational management process.
- We are putting greater emphasis on understanding supply chain vulnerabilities and exposure, with more attention to n-th degree risks.
- Our metrics for evaluating operational resilience evolve – far more attention to understand things like the mean time to detect an intrusion, minimum tolerable downtime, and time to recover critical services.
- Example: US NAIC Insurance Data Security Model Law, which mandates that boards receive annual reports detailing risk assessments, risk management decisions, third-party service provider arrangements, testing results, cybersecurity events, and recommendations for programme changes.

What are your views on the FSB's Format for Incident Reporting Exchange (FIRE)?

- A common reporting framework, agreed upon by the global financial sector and all supervisors, would streamline processes for global organisations.