Canadian Institute of Actuaries | Institut canadien des actuaires

February 5, 2024

OSFI
resilience@osfi-bsif.gc.ca

Subject: CIA Response to Draft Guideline E-21 – Operational Resilience and Operational Risk Management

The Canadian Institute of Actuaries (CIA) is pleased to provide our comments on this important draft guideline.

The CIA supports OSFI's expansion of the existing Guideline E-21 to focus on operational resilience in addition to operational risk management. We encourage OSFI to enhance the wording throughout to reinforce that the guidance is principles-based. We also suggest that OSFI explicitly acknowledge that the application of the guideline should be risk-based, allowing federally regulated financial institutions (FRFIs) to adopt the application to their specific circumstances.

A. Overview

We are pleased to see a focus on critical operations but have noted that at times the expectations are expanded to operations more broadly. The notion of risk-based application should be added and complement a principles-based approach to allow for recognition of critical and/or high-risk operations, including that there may be functions within critical operations that are not themselves critical.

A.3 Application and proportionality

We are pleased to see the concept of proportionality; however, it is unclear as to the expectations for smaller institutions offering unique services/offerings. Current wording in the draft suggests there are instances when products or services offered by a smaller institution are so key that disruption to that institution could lead to the failure of the financial system or economy. OSFI could consider providing an example of such a situation, as it is not initially apparent what scenario could give rise to this outcome.

The draft guideline provides wording related to interconnectedness but does not provide examples. We recognize that banking services, such as Interac and other payment processes, are critical to the financial system, economy and to other FRFIs, but OSFI could consider including an example of insurance-specific services that would be deemed as critical to the financial system and/or economy.

A.4 Definitions

The definition of “operational resilience” includes explicit reference to technology and cyber risks. Operational resilience requires **all** operational elements (people, processes, etc.) to be functioning to support the delivery of products and services, including those deemed critical. It is not clear why technology and cyber risks are called out explicitly whereas other categories of operational risk are not, and this may lead to other operational elements being deemed less important.

The draft guideline defines “operational risk” as the risk of loss resulting from people, inadequate or failed internal processes and systems, or from external events. While we understand this is a standard definition (used by, for example, the International Association of Insurance Supervisors), our preferred approach would be to allow each FRFI to use its own definition that reflects their culture and communication approach, while still reflecting the key elements of the OSFI definition. As an example, we have seen a slightly modified definition, as follows: "Operational risk is broadly defined as the risk of loss resulting from human error, decisions, actions or failure to act, inadequate or failed internal processes and systems, or from external events that affect business operations."

The definition of data risk, as written, suggests you can have "inadequate or failed people" as well as process and systems. We are unclear as to the intention and would recommend that OSFI review and rewrite this definition.

We are pleased to see that the definition of “scenario testing” aligns with that outlined in Guideline E-18 and suggest that a cross reference to E-18 would be helpful.

We recommend including a definition for “severe but plausible scenarios.” Alternatively, OSFI may wish to consider refreshing Guideline E-18 to capture elements of scenario testing and then referencing E-18 where appropriate.

We recommend adding a definition for “central functions,” although we note that organizational structures in FRFIs can vary widely.

Finally, we note that while the definitions noted include data risk, they do not include other risks that are referenced throughout the draft guidelines and also covered in other OSFI guidelines.

A.6 Related guidance

We recommend this list be expanded to include Bulletin E-5 *“*Retention/Destruction of Records,” the new “Integrity and Security - Guideline” and possibly “Draft Guideline E-23 – Model Risk Management” although we do acknowledge this latter guideline is in the early stages of consultation. We also suggest reference to Guideline B-3 “Sound Reinsurance Practices and Procedures.*”* While Guideline B-3 is largely focused on financial risk, there are operational risk elements associated with reinsurance and it would be helpful to highlight the connection.

1.1 Senior management is responsible for operational resilience and managing operational risks

While we agree that there should be clear ownership and accountabilities for operational resilience and management of operational risk, we are unclear as to how OSFI defines "central functions."

1.2 Operational resilience and management of operational risks are integrated into the FRFI's enterprise risk management program and reporting

The draft guideline notes "…fully integrated with its enterprise risk management program, which includes operational risk, technology and cyber risk, third-party risk, and data risk,…" We recommend removing all of the references to categories of operational risk in this statement. The guideline includes a definition of operational risk. Inclusion and exclusion of some categories may create confusion and could suggest that other elements of operational risk are less important. The assessment of the categories should be specific to each FRFI based on the nature of their operations.

1.3 Business lines and central functions manage risk and are subject to independent oversight and 1.3.2 Independent risk and compliance oversight of operational resilience and managing operational risks

In this section, there is reference to "central functions," and separately, the "risk and compliance oversight function" making it appear that they are not deemed to be part of central functions. It may be helpful to define central functions and to refer to OSFI's "Corporate Governance Guideline" for the reference to risk and compliance as oversight functions. Our interpretation is that risk and compliance oversight functions are second line whereas central functions are first line. It may be helpful to clarify this in this section.

In addition, the wording suggests risk and compliance are one function – in practical terms, they generally are not.

1.3.3 Independent assurance is provided

The guideline notes that independent assurance should be provided by internal audit or a similar function. Can OSFI provide an example of a similar function?

2. Operational resilience

We agree with the outcome statement in this section but suggest that it should be acknowledged that not all functions within critical operations will themselves be critical.

2.2.1 Tolerances for disruption should be established for each of the identified critical operations

The draft introduces the concept of "tolerances for disruption" and suggests evaluating the FRFI's ability to operate within the "tolerance" in the scenario analysis. We note that the definitions provided in the draft are different than established enterprise risk management practices. For example, the CIA has published a practice resource document that

includes definitions for these concepts. We suggest including the following definitions[1] from that publication to provide readers with further context:

> **Risk appetite** is the level and type of risk that an organization is willing to accept in order to achieve its objectives. It is expressed as a series of qualitative and quantitative risk appetite statements articulating risk appetite relative to earnings, capital, liquidity, and/or other measures as appropriate.
>
> **Risk capacity** is the maximum level of risk an organization can accept before breaching risk constraints. These constraints are determined by regulatory capital and liquidity needs, the operational environment (e.g., technical infrastructure, risk management capabilities, expertise), and obligations to stakeholders (e.g., depositors, policyholders, shareholders, fixed income investors, and regulators). Risk appetite is constrained by risk capacity.
>
> **Risk tolerance** is the maximum level of risk that an organization is willing and able to accept. It is the practical application of risk appetite and operationalizes the risk appetite statements with qualitative and/or quantitative measures that can be monitored and reviewed.
>
> **Risk limits** consist of qualitative and quantitative measures that allocate an organization's risk tolerance to business lines, subsidiaries, risk categories, concentrations and other levels as appropriate. Risk limits translate risk tolerance into boundaries on risk monitoring measures. Some risk limits are hard limits; exceeding them represents an unacceptable level of risk and immediate corrective action is required. Some are soft limits that provide an early warning signal as risk profile approaches risk limits. Exceeding a soft limit prompts management to evaluate whether corrective action is necessary.

We note that measuring disruption as a duration or unit of time is prescriptive and limiting. FRFIs should be able to establish a measure that is appropriate for the critical operation and related risks.

2.3.3 Frequency and intensity of testing is proportionate to risk and criticality

We agree that frequency and intensity of testing should be proportionate to the risk and criticality but would recommend flexibility as to the frequency. As testing is to consider a range of severe but plausible threats, hazards and operational risk events, it should also acknowledge that not all of these events will result in the same level of risk. In these cases, testing less frequently than annually may be appropriate.

3.2.1 Operational risk appetite articulates types of risk and sets quantifiable limits for risk acceptance

We find it unusual that the definition of risk appetite in this section is referencing "business as usual" – please see our comments above under 2.2.1. This is not aligned with general accepted practice.

[1] These definitions are from the CIA's practice resource document, *Risk Appetite*.

3.3.1.1 Tools are applied to determine a FRFI's risk profile

While we acknowledge that the identified tools are commonly used, providing a list and including detailed descriptions is prescriptive. We recommend amending the wording to note that these tools are examples only and that the FRFI should determine the tools appropriate to the nature of the operational risks being reviewed and assessed.

While we are pleased to see the following statement "The size, nature, complexity of operations, strategy, risk profile and risk environment of the FRFI should be taken into account when determining the appropriate tools to apply" inclusion of details related to the tools suggests they are required. That level of detail should be included in an appendix as examples of tools.

4. Operational risk management subject areas that strengthen operational resilience

We recommend that the list of subject areas be noted as "including but not limited to" as the list provided is not exhaustive.

4.1.3 BCP testing

In this section, we note that reference is made to "a range of adverse circumstances." Should this be "adverse but plausible"? Also, a definition of "adverse circumstances" may be helpful. As noted earlier, refreshing Guideline E-18 to capture the types of scenarios would also be helpful.

4.4 Change management

Within the bulleted list in this section, it states, "considering risks related to human resources, risk management, and technology." Can OSFI provide clarity on what is meant by risks related to risk management? Furthermore, we would like to understand why a few categories of operational risk are included and not others. We would recommend that the bullet be changed to be: "considering risks related to the various categories of operational risk."

We also recommend that the reference to "initiating significant change" be amended. It may not be necessarily true that significant change impacts critical operations. The focus should be on the impact of change to critical operations and/or functions/activities deemed higher risk. The change may or may not be significant, but if it impacts a critical process then heightened due diligence would be prudent.

4.7 Data risk management

We agree that managing data risk is important. Federal and provincial privacy laws outline detailed expectations. We recommend including a reference to privacy legislation to avoid duplication and/or conflicting expectations.

We question the need for a separate and distinct risk appetite for data risk rather than managing it within operational risk tolerances. Consideration of data, specifically the type, nature and use, should be an input to other risk assessments.

The CIA appreciates the opportunity to provide feedback on these issues, and we would welcome further discussion with you throughout this process.

If you have any questions, please contact Chris Fievoli, FCIA, Actuary, Communications and Public Affairs, at 613-236-8196 ext. 119 or chris.fievoli@cia-ica.ca.

Sincerely,

Steve Prince, FCIA
President, Canadian Institute of Actuaries

The Canadian Institute of Actuaries (CIA) is the qualifying and governing body of the actuarial profession in Canada. We develop and uphold rigorous standards, share our risk management expertise and advance actuarial science to improve lives in Canada and around the world. Our more than 6,000 members apply their knowledge of math, statistics, data analytics and business in providing services and advice of the highest quality to help Canadian people and organizations face the future with confidence.