Autorité
des marchés
financiers

December 2024

Report on the financial institution operational resilience survey

Legal deposit – Bibliothèque et Archives nationales du Québec, 2025
ISBN 978-2-555-00326-2

Table of contents

Preamble

The Autorité des marchés financiers (AMF) wishes to help further develop the resilience of Québec's financial system and financial system stakeholders, which are facing emerging issues and operating in an ever-changing environment.

In recent years, the AMF has been engaging in dialogue with financial institutions with a view to raising awareness and sharing information about practices that may enhance operational resilience.

A virtual seminar in February 2023 (in French only) provided an opportunity to hear the opinions of innovative financial institutions on the selection, implementation and testing of key operational resilience practices enabling them to manage the disruptions affecting their critical operations.

Subsequently, in the fall of 2023, the AMF, in order to maintain open dialogue, sent the *Survey of Good Operational Resilience Practices* to all authorized financial institutions operating in Québec. The purpose of the exercise was to develop a current portrait of operational resilience practices that institutions operating in Québec are following to address the many disruptions.

The survey covered a range of themes that directly contribute to enhanced operational resilience, such as the identification of important business services, tolerance for disruption, business continuity and third-party management.

The results of the survey will enable the AMF to work with the industry to identify and prioritize efforts to strengthen the existing frameworks, in accordance with standards observed at the international level, with the aim of reducing compliance burden. In addition, the survey will allow institutions to compare their operational resilience initiatives with those of their peers.

This report presents an anonymized compilation of operational resilience practices within financial institutions, some takeaways regarding those practices, and some of the comments made by institutions during this awareness exercise.

The AMF thanks the institutions for their participation and hopes that they will be able to draw inspiration from the results of this exercise in developing and implementing their operational resilience strategies.

Introduction

For this awareness exercise, the AMF developed a questionnaire covering the key themes brought into regulations by foreign regulators in recent years to address operational resilience.

The exercise ran from September 25 to November 10, 2023, and involved all authorized financial institutions operating in Québec. The results were compiled from the responses provided in the 254 completed questionnaires received by the AMF.

Four main themes addressed

Theme 1
Operational resilience

The objective of this first theme was to gain insight into how the concept of operational resilience and the concepts of organizational resilience and business continuity are distinguished within the institutions' day-to-day operations and how important operational resilience is for them compared to other business priorities. This theme also sought to identify the scope of implemented operational resilience initiatives and the challenges faced in implementing them.

Theme 2
Governance

The theme sought to obtain knowledge about the planning, development and implementation, and assessment of the effectiveness, of operational resilience objectives and strategies and the division and assignment of roles and responsibilities. Investments devoted to these initiatives were also addressed.

Theme 3
Important business service design and mapping

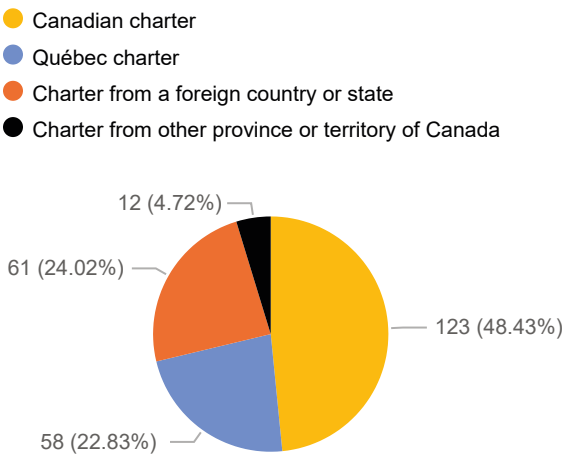
This theme sought insight into how institutions determine which business services are important business services in their organization and the extent to which important business services have been duly identified. In addition, this theme sought knowledge about how institutions ensure that all important business services have been identified and that all required resources and interdependencies between important business services have been documented.

Theme 4
Business continuity and third-party management

The objective of this theme was to identify plans in place to address operational disruptions and to understand established testing approaches and strategies, including by mapping important business services or collaborating with critical third parties.

Breakdown of respondents

Respondents by charter type



Theme 1
Operational resilience

Some of the questions submitted to the financial institutions:

- How do you define operational resilience?
- How are business continuity (BC) and operational resilience (Op Res) distinguished within your organization?
- Is there a distinction between operational resilience and organizational resilience in your institution?
- Compared to other business/strategic priorities how important is operational resilience within your organization?
- Does your organization have an operational resilience program or project?

Some takeaways from the responses received

The definitions of operational resilience vary widely and, in some cases, draw from definitions proposed by standard-setting bodies or other regulators, such those in the United Kingdom and the United States.

Operational resilience is regarded as a complement to business continuity and the management of, in particular, operational risks.

It is also regarded as an introduction of new concepts or as merely an overlap with business continuity activities.

Most of the institutions have an operational resilience program in place. Those that have not integrated the key elements leading to operational resilience are aware they are "lagging" and will need to ensure that such a program is implemented.

To do this, they intend to use upcoming clarifications in the regulatory frameworks as an opportunity to step up their efforts.

The challenges encountered by financial institutions when implementing an operational resilience program mainly stem from constraints related to the competence, knowledge, training and experience required of resources.

Excerpts of comments received from financial institutions

"Operational resilience is an absolute priority, because it will improve our capacity to withstand and recover from disruptive events and maintain client confidence. (...) with robust operational resilience measures, we can minimize downtime, mitigate risks and maintain our operations in adverse situations. (...) Operational resilience helps safeguard our reputation and client and stakeholder interests."

"We are continuing to invest in the implementation of an operational resilience program (...) it will take some time for the organization to mature enough to undergo the change in culture and mindset needed to improve our resilience."

"A certain lack of awareness and understanding of operational resilience within the organization is making it difficult to set priorities (...) Developments in the regulatory landscape are presenting interpretation challenges in constructing programs."

Theme 2
Governance

Some of the questions sent to financial institutions:

- What is your opinion of establishing a board level appointment who is responsible for assessing resilience at all levels and ensuring all resilience building efforts within the institution are aligned and co-ordinated?
- How do you ensure effective oversight and challenge is provided by the board and senior management?
- How do you assess the effectiveness of your operational resilience governance structure?
- What level of knowledge and skills exists at the senior executive level for operational resilience?

Some takeaways from the responses received

- Opinions aligned that there is no need to specifically task a board member with assessing the institution's maturity with regard to operational resilience.
- The responses revealed that senior executives, including board members, have a sufficiently developed and, at times, even specialized understanding that enables them to oversee the implementation of a resilient business model.
  - — Some institutions, however, believe that more training and workshops, including tabletop exercises, would be useful in more precisely determining the roles and responsibilities of stakeholders within the institution.
- Most institutions indicated that a documented governance structure is in place and that senior management's roles and responsibilities have been defined for the implementation of an effective operational resilience approach.

Excerpts of comments received from financial institutions

- *"Operational resilience is being developed. The governance structure will be aligned with the organization's strategic and operational resilience objectives."*
- *"We consider it important for board members to have the required competence, knowledge and experience in managing risks related to technology, cybersecurity, third parties and business disruption in order to provide the necessary operational resilience oversight."*
- *"A board member has been given responsibility for the operational resilience program, with governance arrangements in place to ensure oversight of the broader/related risk frameworks."*
- *"Management, not board members, should be responsible for assessing resilience across all levels and ensuring that all efforts are aligned and co-ordinated. The board should provide constructive challenge and oversight of these activities, as it does for other business activities."*

Theme 3
Important business services

Some of the questions sent to financial institutions:

- Has your financial institution identified and documented important business services that if disrupted could cause harm to consumers or market integrity?
- To what extent have you completed the inventory of your important business services and its interdependencies?
- How frequently are you testing your response and recovery capabilities for different disruptive scenarios?
- How do you intend to use important business service mapping in your testing approach?

Some takeaways from the responses received

- Many institutions have implemented a governance structure for the identification of important business services.
  - — The interpretation of what constitutes an important business service, like completion of the exercise, varies.
  - — The distinction between the concepts of critical activity and important business service is often difficult to establish.
- Resiliency requirements for important business services and the interdependencies between them are frequently documented and kept current by consolidating everything in a single list to ensure integrity.
  - — This list is subject to independent review, in some cases.
- There is a good understanding of the data used to map important business services.
  - — The inclusion of this data in testing approaches is being considered and this could even be extended to critical third parties.

Excerpts of comments received from financial institutions

- *"We have completed a number of pilot operational resilience assessments of important business services identified within several of our business lines. The lessons learned from these pilot projects have been integrated and we are now developing a business operational resilience program and a comprehensive program roadmap."*
- *"(...) intend to develop an operational resilience strategy, while conducting an analysis of deficiencies in important business systems (...) prioritize critical business services (...) improve the effectiveness of our business continuity management system."*
- *"(...) recognize the importance of strengthening buy-in across the organization and developing resilience strategies, including that of third parties."*
- *"We use extensive mapping of important business services to help us develop and carry out exercises involving severe but plausible disruption scenarios. We will continue to build on our exercises in order to make them more complex and reflect emerging disruptions."*

Theme 4
Business continuity and third-party management

Some of the questions sent to financial institutions:

- In the event of an operational disruption, how do you prepare and prioritize your resources and actions in order to ensure continuity of your business services and minimize harm to consumers/clients?
- Do you have a list of all the services provided by third parties and their suppliers within your institution?
- What third-party or outsourcing issues has your financial institution experienced, if any?
- How do you identify your dependency on services provided by 3rd parties (including intra affiliates) for the delivery of important business services which could result in customer harm?

Some takeaways from the responses received

- Institutions have a formal continuity framework in place and a well-defined approach to testing continuity plans.
  - — Their ability to respond and recover from various disruptive scenarios is tested on an annual basis.
  - — Recovery plans take into account services provided by third parties.
- The challenges encountered with third parties relate mainly to data security, IT issues and service interruptions.
  - — Most of the institutions periodically conduct due diligence on new and existing third parties to assess and manage the risks and vulnerabilities that are likely to be brought into the operating environment.
- Institutions conduct periodic independent reviews of their processes and controls and report third-party results to senior management or the board.
  - — Their third-party registers are updated periodically and are also independently reviewed.

Excerpts of comments received from financial institutions

- *"Prioritization is based on the criticality and resilience requirements specific to critical activities or IT systems, depending on the scenario considered. Security teams have visibility and reports from multiple sources to proactively address disruptions of any kind."*
- *"We have proven third-party risk management and business continuity management programs and are building on existing programs to more explicitly integrate testing exercises for important business services."*
- *"A formal post-incident analysis process is in place, with analyses focused on severe outages (…) The analysis takes into account data collected both during and after the incident. The lessons learned are incorporated into the appropriate business processes."*
- *"Identification of concentration risk has been in place for 10 years (…) Although important business services have been identified and dependencies on third parties have been mapped, these are not currently included in our third-party risk register."*

Conclusion

"Resilience has become non-negotiable in a world of ever-increasing disruptions. Now is the time for action. We need to move from "talking the talk" to "walking the walk". The present time must be recognized as an opportunity to build (...) a new leadership model for the future. To do so, organizations need to recognize where they stand on their resilience journey and leaders need opportunities to share experiences, learn from best practices and build partnerships to develop joint solutions."

World Economic Forum Resilience Consortium

The International Organization for Standardization (ISO), a global federation of national standards bodies, has defined organizational resilience as the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.

According to ISO, organizational resilience is supported by several management disciplines and strategies, including those that are generally addressed under the theme of operational resilience around the world (...), including business continuity management and information security and cybersecurity management.

Operational resilience is a growing concern in the financial services industry. Concerns about the consequences and potential consequences of multiple operational disruptions have spawned the rapid development of regulatory initiatives to respond to the growing challenges of financial institutions related to their reliance on technology, interconnections and evolving threats.

Among other things, control of third-party relationships and management of the associated risks have been increased, reflecting concerns about concentration and other risks associated with the outsourcing of critical functions to potentially unregulated entities.

Operational disruptions are having a significant impact on financial institutions and consumers of financial products and services. According to the institutions that participated in the survey, these disruptions are being caused by an increasing number of technological breakdowns, cyber attacks, climate events and, sometimes, even a simultaneous combination of various factors.

The results show that the institutions are aware of the consequences of the rising number of such disruptions, although they report that, so far, the consequences they have suffered as of result of recent years' disruptions have been limited.

"Resilience is the ability to deal with adversity, withstand shocks and continuously adapt and accelerate as disruptions and crises arise over time."

World Economic Forum Resilience Consortium

The survey results show that financial institutions are rolling out operational resilience initiatives but that they are at varying degrees of maturity. From definition of the concept and the roles and responsibilities assigned within the organization to the work implemented to identify important business services and the consideration of impacts of disruptions on the institution and its clients, shifts in culture are taking place in different ways.

The collected responses confirm the need for the AMF to enhances certain frameworks to support the financial institutions in their transition to a more resilient business model.

The results of the survey revealed a need to harmonize the practices within institutions. The AMF could address this need by aligning its prudential framework with new international operational resilience standards, as the institutions themselves have recommended it do.

"A key differentiator is the critical operations lens, in conjunction with the end-to-end view, the focus on impact, the use of the tolerance for disruption to drive decisions about resilience investment, and the consideration of third parties' resilience."

Bank for International Settlements

The cooperation of institutions participating in this survey has also helped identify a number of their needs for strengthening operational resilience.

The AMF, acknowledging from the outset that operational resilience risks are significant and systemic, will analyze the various avenues open to it to support the industry.

The observations gleaned from this analysis will enable the AMF to continue discussions with the financial institutions, particularly regarding the opportunity to provide them with appropriate contemporary frameworks for the various facets of operational resilience and the sound management of the underlying risks.

Appendix

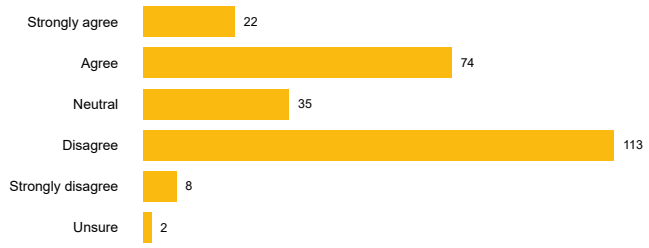
Detailed results

This appendix provides a detailed, anonymized summary of the responses, broken down by question, to the 254 completed questionnaires received by the AMF as part of this awareness exercise.

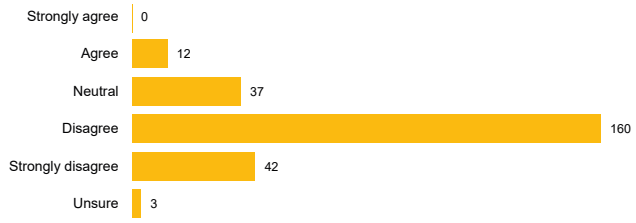
Various comments or observations that were provided by the participating institutions are also presented for each theme.

Q100-2 How are business continuity (BC) and operational resilience (Op Res) distinguished within your organization?

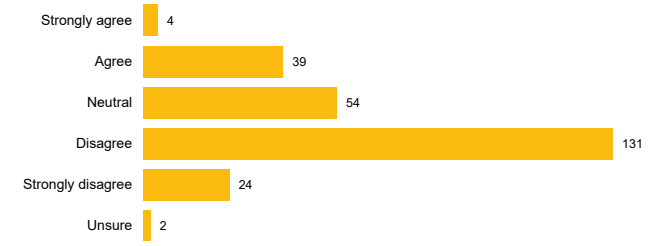
BC and Op Res are viewed as different functions with different purposes in our organization



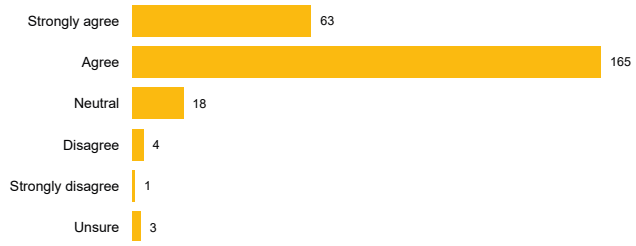
BC has been rebranded as Op Res in our organization, but no changes have been made to job responsibilities



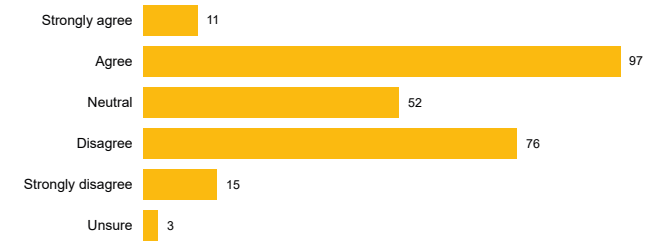
BC and Op Res are synonymous in our organization



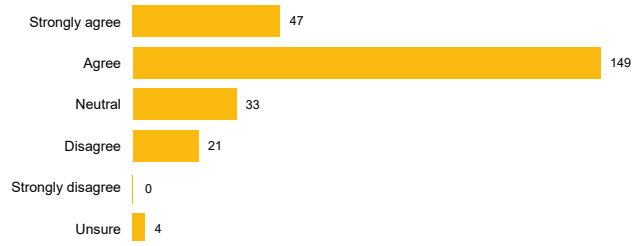
BC is part of Op Res, it supports resilience



There is an overlap between BC and Op Res, however we have not clearly defined the differences



BC is a tool/process to drive Op Res



Some of the comments made by institutions:

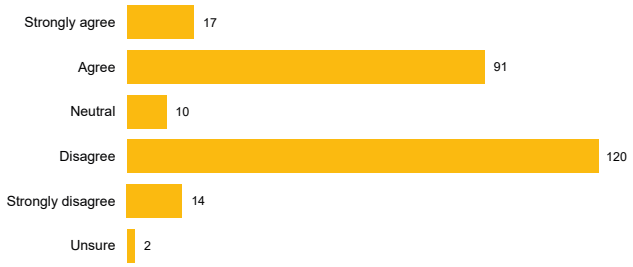
"Business continuity and operational resilience are two separate teams that work together regularly and share common objectives."

"Operational resilience is also a mindset they bring to everything they do in terms of crisis management, business disruption management, third-party risk management, travel risk management, pandemic preparedness, etc."

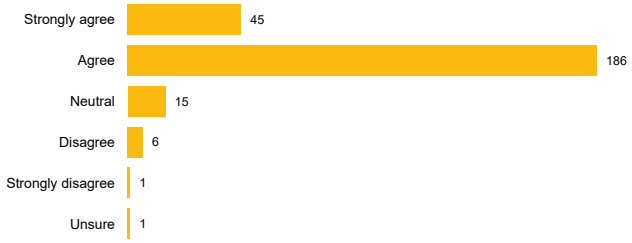
"The long-term objective of strengthening operational resilience is to protect an organization's reputation and viability over the long term, while the goal of business continuity management is to minimize the potential impact of a disruptive event."

Q100-3 To what extent do you agree with the following statements?

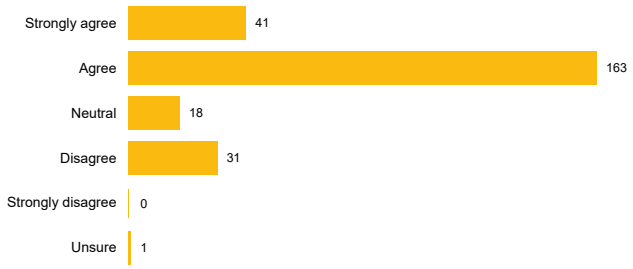
BC is reactive and focused on response and recovery



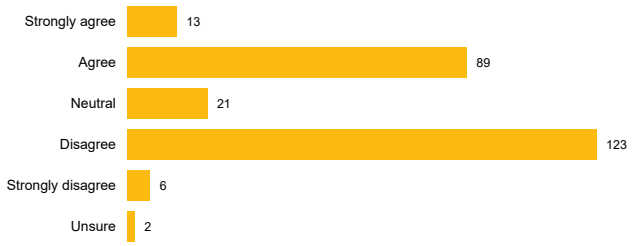
Op Res is proactive; it works to prevent disruption and deliver recovery capability



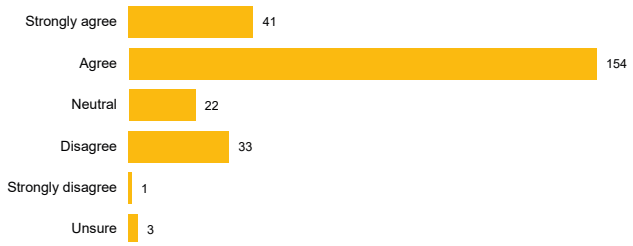
BC considers the likelihood of disruption



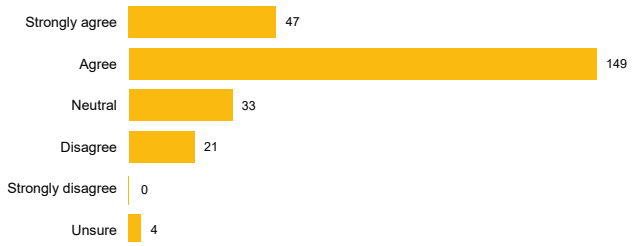
BC's primary focus is on the internal impact for the organization, when faced with a disruptive event



BC's focus is equally on the internal and external impact to the organization when faced with a disruptive event



BC is a tool/process to drive Op Res



Some of the comments made by institutions:

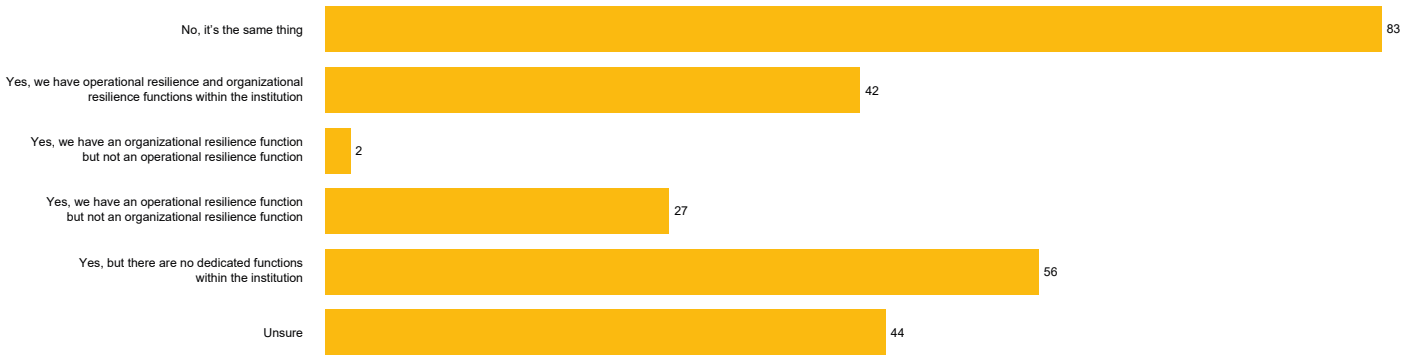
"Operational resilience also focuses on the internal and external consequences when institutions are faced with a disruptive event. Our approach to external consequences is focused on clients and market integrity."

"Consideration is given to the reputational, regulatory, financial and economic impacts that affect partners and clients."

"Operational resilience is a proactive approach that involves identifying critical operations and mapping the internal and external dependencies required to support them. (...) determining tolerances for disruption, conducting scenario testing and establishing a culture that promotes and reinforces behaviours that support operational resilience and proactively managing the culture and behavioural risks that may affect resilience."

"The operational resilience program focuses on the strategic approach to maintaining essential business services in the event of extreme but plausible events that could have an impact not only on the institution, but also on its clients and on the financial market in general."

Q100-4 Is there a distinction between operational resilience and organizational resilience in your institution?



Some of the comments made by institutions:

"We do not define any of these terms in our policies and (...) for the time being, these concepts are not reflected in dedicated functions within our organization. These concepts are therefore still vague."

"(...) Organizational resilience brings together financial resilience and operational resilience. A business can be resilient operationally but still fail owing to liquidity and capital problems, while another business that is financially resilient can suffer operational problems that harm it. Operational resilience refers to an organization's ability to withstand and adapt to various technological and/or human-caused disruptions in processes. It helps guarantee that critical business operations continue despite disruptions, by mitigating potential risks and by quickly adjusting for or recovering from disruptions. Operational resilience is essential so that organizations may build and maintain the trust of their clients, protect their clients and markets from harm and comply with regulatory requirements."

"Organizational resilience includes all main areas of the business: strategic, capital/financial, technological, operational, cultural and learning. Operational resilience is focused mainly on the operational model, with controls, policies, oversight and practices to strengthen operational integrity and consistency."

Q100-5 Compared to other business/strategic priorities how important is operational resilience within your organization?

Some of the comments made by institutions:

"Senior management puts operational resilience at the top of the list of priorities (...) linked to our strategic priorities (...) a fundamental element of all business and strategic initiatives."

"After the COVID-19 pandemic and in a world of increasing uncertainty, it is more important than ever to understand the risks to the organization (...)."

"Operational resilience is an absolute priority because it will improve our capacity to withstand and recover from disruptive events and maintain client confidence. (...) helps safeguard our reputation and client and stakeholder interests."

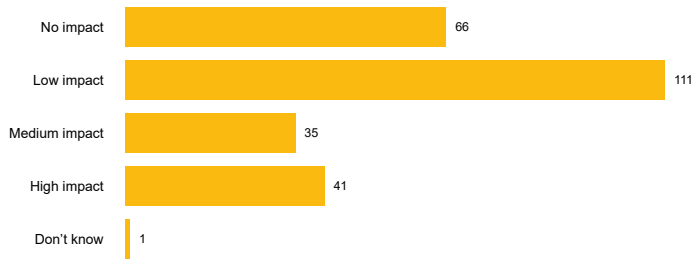
"This is a new concept for us. Now that we have been made aware of it, operational resilience appears to be rather important!"

"Operational resilience is a central aspect of the IT strategy (resilience by design)."

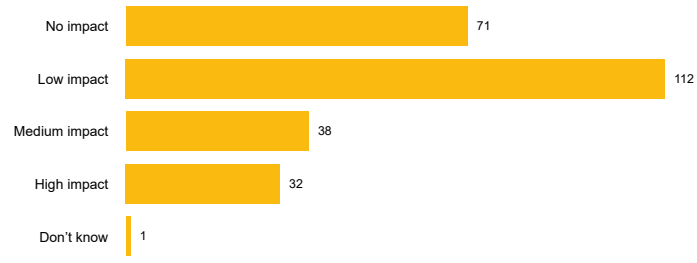
"We are starting work in this area and will step up our efforts as regulatory guidance clarifies things."

Q100-6 Aside from the pandemic, how much of an impact has the most severe operational disruption experienced in recent years had on the following aspects of your business?

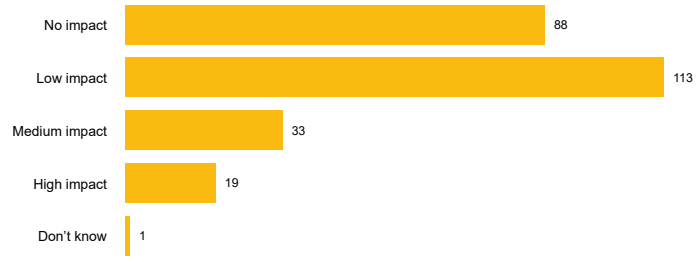
Technology



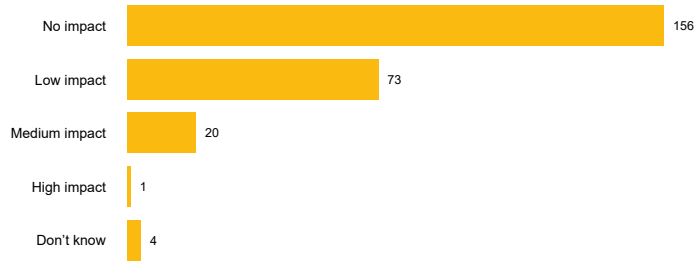
Operations (disruption of essential processes/services, etc.)



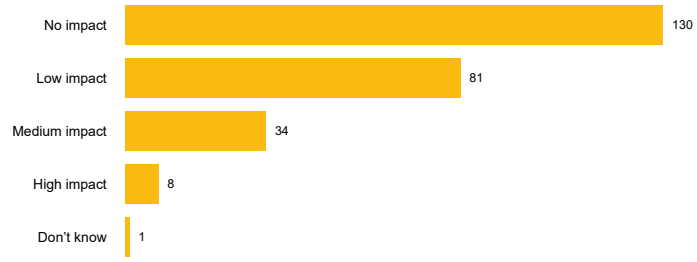
Workforce



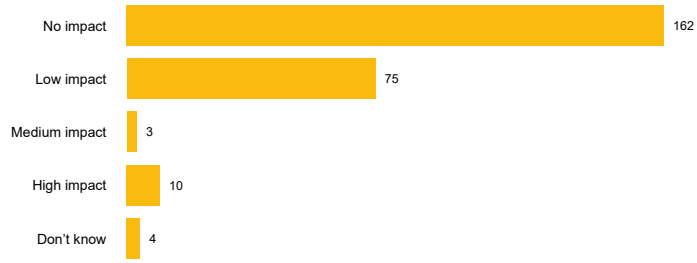
Financial situation



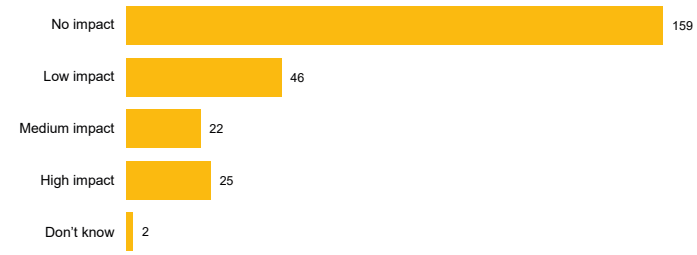
Relations with customers and business partners



Brand reputation/strength



Business strategy



Some of the comments made by institutions:

"We experienced several problems that suggested a cyber attack may be in progress. While it turned out not to be a cyber incident, il was a good "test" of our cybersecurity and crisis management protocols, providing an opportunity to learn important lessons."

"We managed the event in accordance with our business continuity procedures and further improved redundancy by seeking and implementing improvements based on the lessons learned."

Q100-7 In order of importance, which areas (max 3) presented the most challenges for your organization in your response to the most severe disruption experienced in recent years (apart from the pandemic)?

Énoncés	Priority 1	Priority 2	Priority 3	Total
Ability to communicate effectively with internal stakeholders	14	14	7	35
Ability to gather appropriate information quickly and efficiently	32	16	20	68
Ability to make timely and informed decisions	2	7	5	14
Clarity on responsibilities for response	4	9	6	19
Determination of roles and responsibilities and decision-making power for all response teams	8	7	6	21
Ability to use appropriate technologies/tools to increase response capacity	18	20	25	63
Ability to prioritize actions, including recovery and recovery, as appropriate	4	4	12	20
Ability to recognize that the incident constituted a crisis and therefore required escalation and mobilization of the appropriate management team	8	6	2	16
Visibility into organization-wide impact	13	15	22	50
Usefulness of the response plan (e.g., crisis management, business continuity, disaster recovery, etc.)	10	8	8	26
Ability to recover/restore essential business services and processes for normal operations	35	12	5	52
Ability to maintain critical business services and processes through continuity measures	10	33	12	55
Ability to communicate effectively with external stakeholders	1	23	15	39
Ability to influence media coverage	4	1	5	10
No area in particular	74	1	10	85

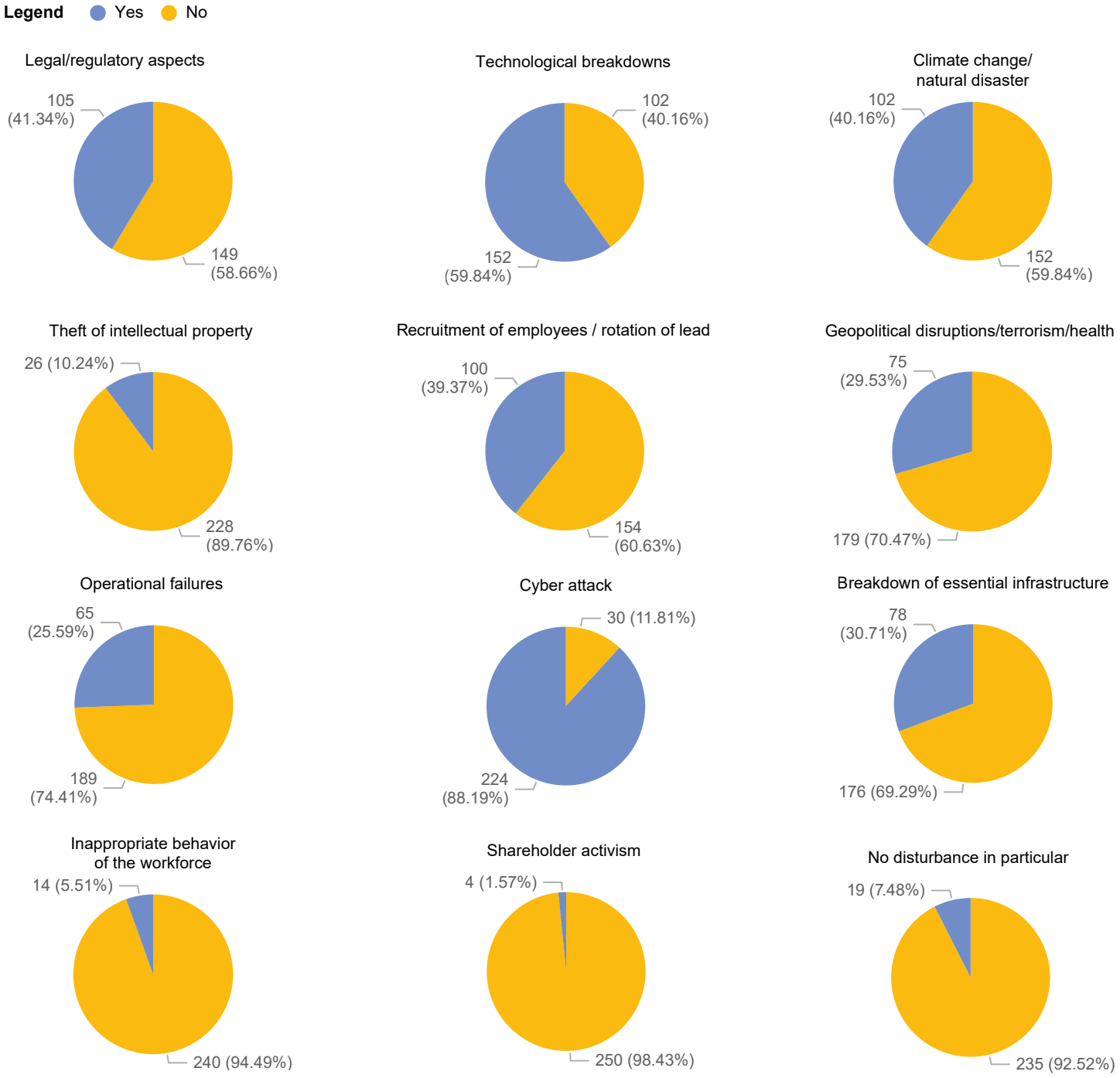
Some of the comments made by institutions:

"Continually engage key stakeholders to strengthen engagement and interconnectivity and improve running processes. Understanding external impacts on suppliers via events is important and guarantees two-way communication."

"In the past, the most notable disruptions were dealt with quickly and transparently with all affected stakeholders to avoid major negative impacts. (...) as business and operational models continue to evolve, we are ensuring that internal communication capabilities, controls and protocols are kept current and relevant."

"(...) Communicating and directing third parties is more difficult owing to the lack of insight into their operations and resilience (...) the ability to gather information quickly and efficiently was hampered, as the disruption was part of a third-party incident affecting multiple entities. This in turn hindered the capacity to communicate effectively with external stakeholders."

Q100-8 What types of disruptions do you fear your organization will face, or continue to face, over the next two years?



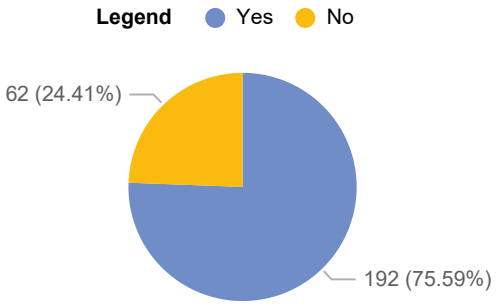
Some of the comments made by institutions:

"The failure of a critical/key supplier (supply chain) or the major outage at a third party and also concentration risk with suppliers, technological infrastructure."

"Strategic competition when faced with open banking, fintech and the regulatory changes that these evolving forces will bring about."

"Additional regulatory requirements as standards and governance models evolve and require increased oversight and responsiveness."

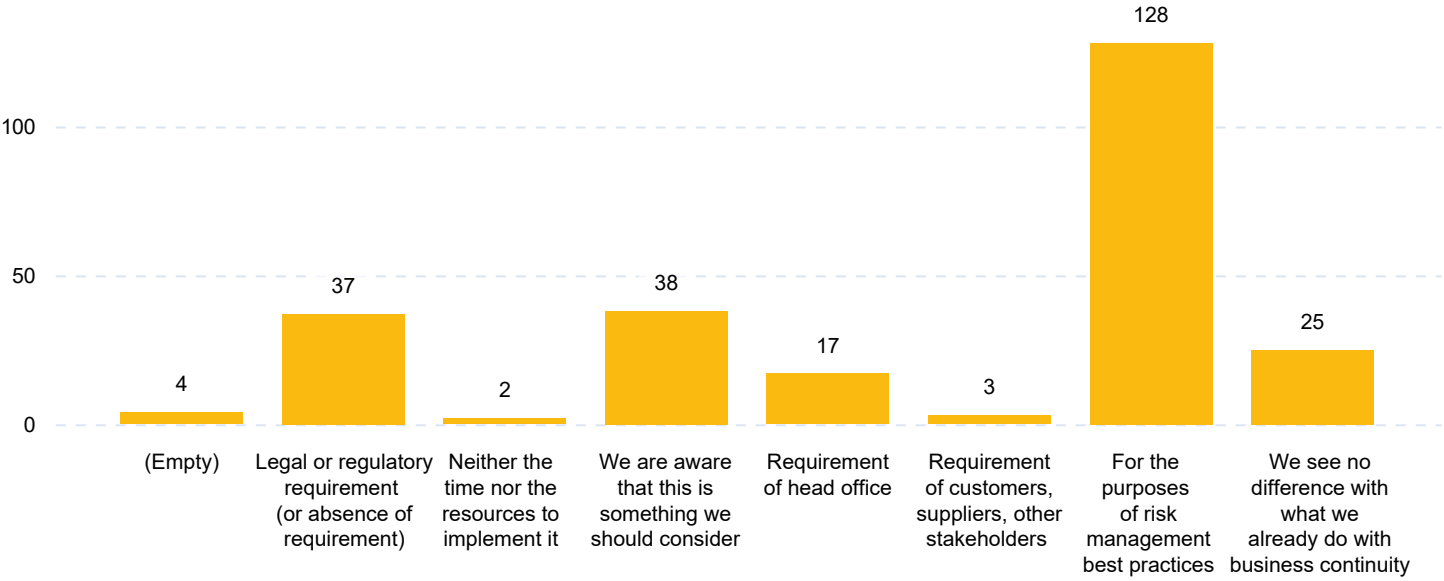
Q100-9 Does your organization have an operational resilience programme or project?



Overall, nearly 76% of institutions report having an operational resilience program or project in place. This rate is 88% for institutions with a charter from a foreign country or state, 77% for institutions with a Canadian charter and 64% for Québec-chartered institutions.

Q100-10 Explain why you have (or don't have) an operational resilience program or project.

PART A (All institutions)



Some of the comments made by institutions

Most of the institutions that have implemented an operational resilience program or project have done so primarily for best management practice purposes. Some of them have also expressed that the implementation was required by their head office or to comply with a current or upcoming regulatory requirement. In particular, they indicated that:

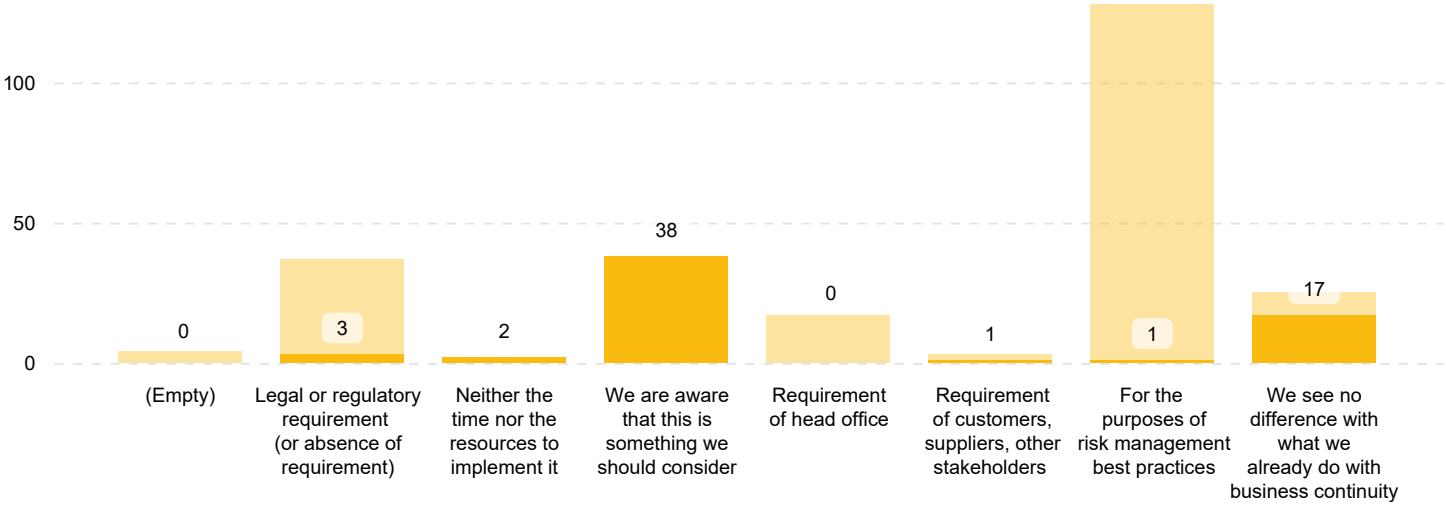
"The exercise is being driven by regulatory requirements, but the goal of the program is to make the organization resilient by design."

"In addition to the requirements set out above, the organization recognizes the importance of an operational resilience program regardless of external requirements or influences."

"The main goal is risk management, even if some timeframes and deliverables are aligned with regulatory expectations."

"We are convinced that the operational resilience program is beneficial and in line with the expectations of our clients, suppliers and stakeholders."

PART B (Institutions that don't have a program)



Some of the comments made by institutions:

"Developing a framework to incorporate various regulatory requirements, including third-party risk and cyber and technology risk."

"Although we have not specifically identified a resilience program or project, we have built resilience through organic changes and lessons learned from disruptions."

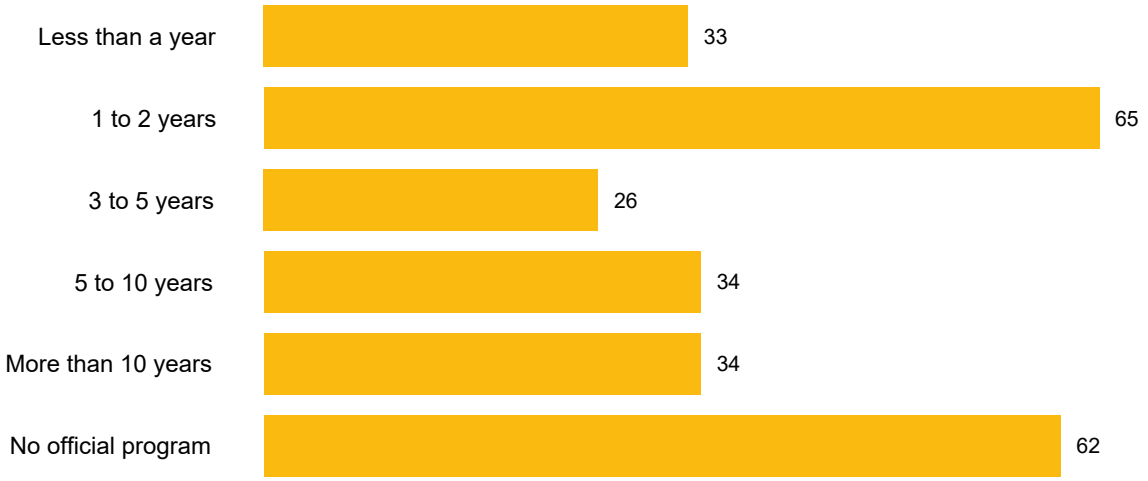
"Our business continuity and disaster recovery programs as well as our programs covering technological resilience, cyber resilience, business resilience (business risk management) and supplier resilience address and document many aspects of operational resilience."

"We are in the early planning stages and are awaiting guidance on this topic (...). No official project at this time."

"We are working with our industry peers to review best practices. Operational resilience is a topic that has started to gain traction (...), a path forward along which we will integrate some concepts into our existing program."

"This is a recent concept. We are a small organization (...), we currently do not have the resources to undertake this project."

Q100-11 How long has your operational resilience program been around?



Some of the comments made by institutions:

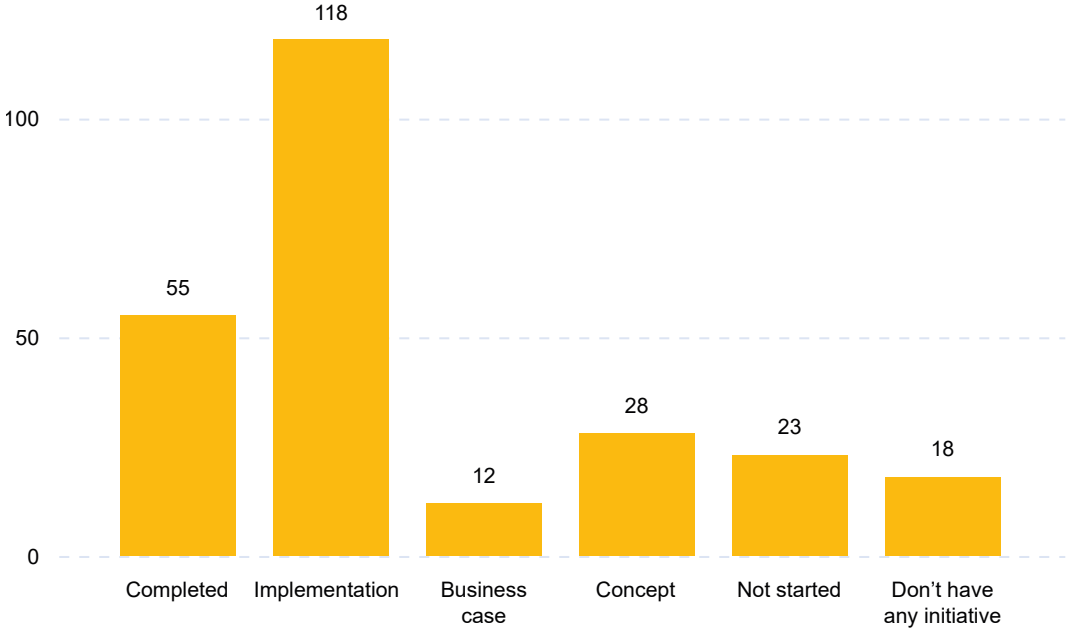
"We have been actively integrating operational resilience into our ORM program since 2022. However, key operational risk practices related to operational resilience have existed within the institution for the past several years."

"A formal operational resilience program was created two years ago to link operational risk management programs and provide us with additional capacity to assess resilience."

"The program in a broad sense began several years ago with the concept of 'disaster recovery'. Then it evolved into the concept of business continuity, and finally into a concept of operational resilience for each business line. The operational resilience program (draft) began at the end of 2020 for the ransomware portion (design phase and first step of patching in tactical mode). The succession portion began in late 2021. For the past year and a half, the program (draft), consolidated and structured under the umbrella of operational resilience, has been addressing all issues in tactical and strategic mode in order to reduce the organization's risk."

"The program has been rebranded as Operational Resilience in recent years, but it previously existed as Business Continuity Management and has been in place for over 10 years."

Q100-12 What stage is your initiative or project on operational resilience?



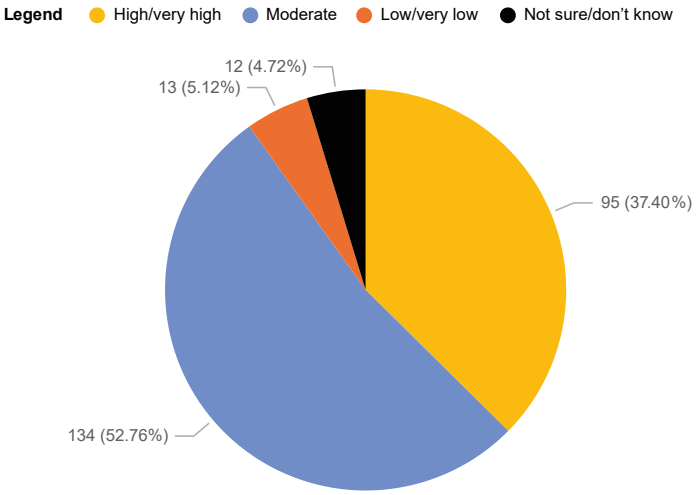
Some of the comments made by institutions:

Most of the institutions indicated that their operational resilience project has been completed or is in an implementation phase. In particular, they indicated that they are in continuous improvement mode or are currently implementing a multi-annual operational resilience program. Some institutions, at the design stage, also indicated that:

"They are in the process of reviewing their operational resilience requirements to determine the needs and requirements of the program. This will be done in accordance with OSFI E-21 guidance and timeframes."

"We are shifting our focus to business continuity practices and plan design in order to begin considering a more holistic approach to operational resilience."

Q100-13 Thinking about your organization's overall approach, resources, and processes, how do you rate its capability in operational resilience?



Some of the comments made by institutions:

"Operational resilience is not a project that is coming to an end; it is a program that is constantly evolving and maturing, integrating the principles of business continuity across the organization."

"Small organization = ability to support processes quickly."

"Operational resilience is in 'business as usual' mode. (…) resilience is a moving target as our threat landscape continues to evolve (…) we are focused on continuous improvement and raising the bar in terms of our resilience capabilities."

"As an organization, we are constantly testing and refining processes using various practices, such as tabletop exercises."

"The operational resilience program is in construction mode; full capacity has not yet been implemented."

"End-to-end operational resilience pilot assessments have been conducted for several critical business services within some business lines. The lessons learned from these pilot assessments have been incorporated into the overall roadmap and assessment plan for the remaining critical business services."

"While we have an existing business continuity/operational resilience program, we recognize that it needs to be updated to better reflect changing business models (e.g., hybrid work and increasing use of technology)."

"Continuously improving, but it requires substantial human and financial resources."

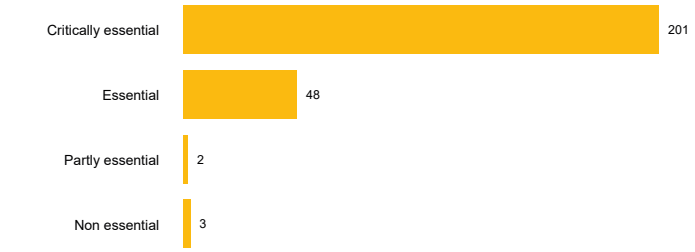
"(…) It will take some time for the organization to mature enough to undergo the change in culture and mindset needed to improve our resilience."

"We are shifting our focus to business continuity practices and plan design in order to begin considering a more holistic approach to operational resilience."

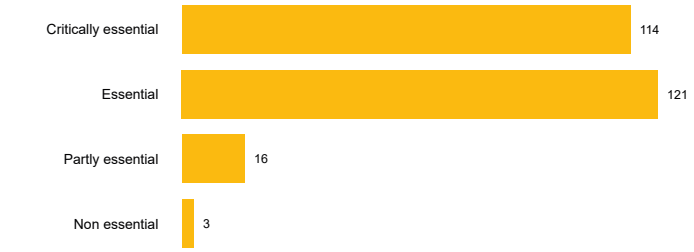
"The business is experiencing significant growth and changes, and resilience is tasked with alignment and deployment to protect those changes and that expansion."

Q100-14 What processes/activities do you consider essential to operational resilience?

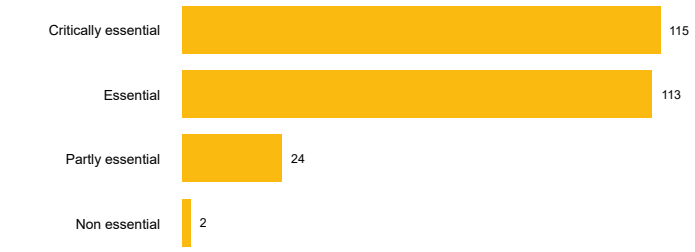
Identifying important business services



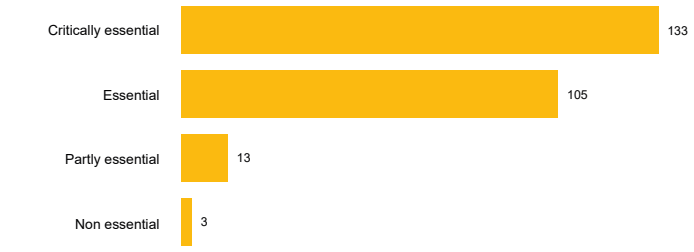
Establishing impact tolerances



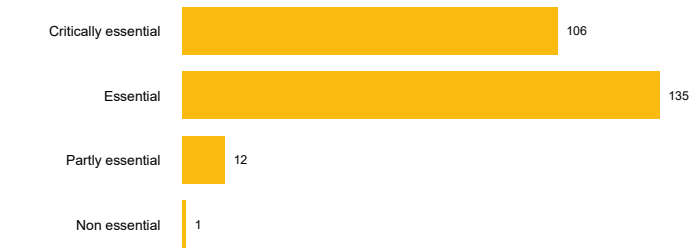
Mapping interconnections and interdependencies



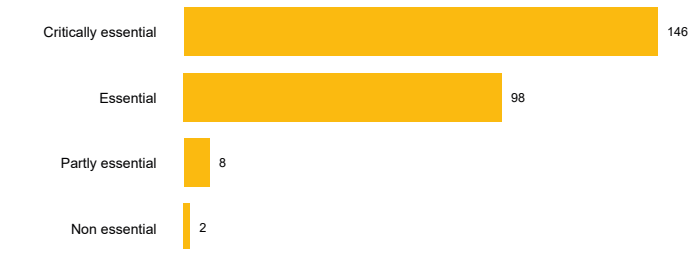
Governance



Operational risk management

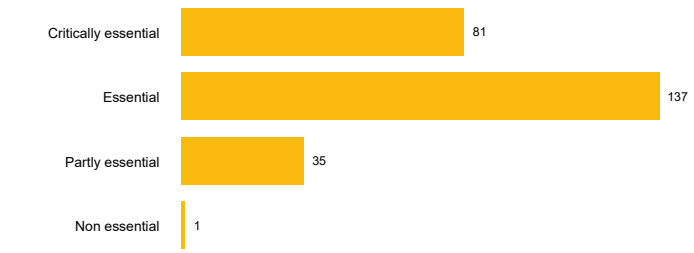


Managing third-party dependencies



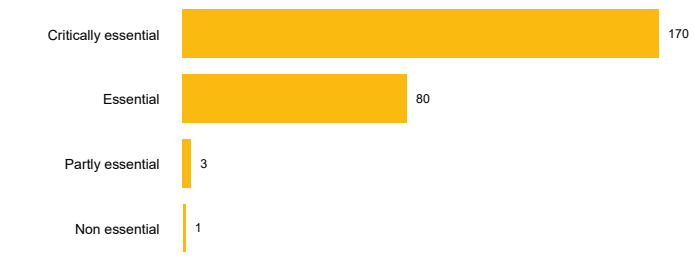
Planning business continuity

Identifying and using plausible scenarios

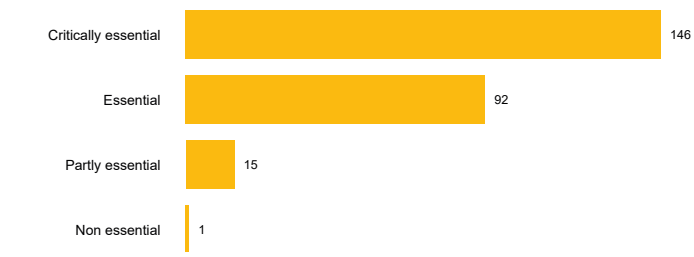


Q100-14 What processes/activities do you consider essential to operational resilience? (continued)

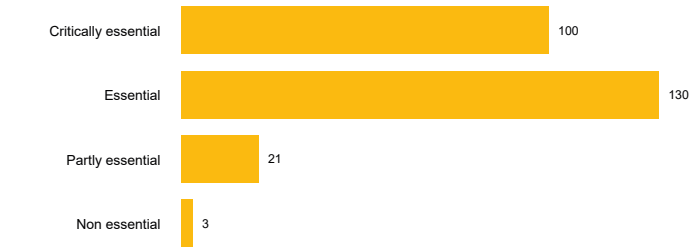
Managing ICT / cybersecurity



Incident management



Prioritizing and working vulnerabilities



Some of the comments made by institutions:

"Establishing a culture that fosters and reinforces behaviours that support operational resilience, including senior management responsibility for operational resilience and management of the operational risks associated with their critical operations."

"Having the financial and human capabilities to do the planning but also during the event. Maintaining greater financial reserves to deal with them."

"Internal and external communications plans, compliance, established crisis management plan and program, change management and data risk management."

Q100-15 What challenges has your organization faced in establishing an operational resilience program?

Statements	Number of responses
We do not have an operational resilience program	50
Establishing a program (how to start)	23
Proof of return on investment	12
Initial program design and implementation	38
Competency constraints (resources with the necessary resilience knowledge, training and experience)	78
Constraints related to the team (dedicated resources)	102
Alignment with a target operating model	38
Program facilitation using technology	45
Achieving tangible change/desired results	26
Maintaining and advancing the program (optimization/continuous investment)	44
No problems so far	63

Some of the comments made by institutions:

"Speed of change in client and industry expectations, resulting in rapid organizational changes to meet those needs."

"Despite the implementation of the management and governance framework (...) the expectations for the Operational Resilience Program do not seem to be clearly set out in the various guidelines."

"In recent years, regulatory and client requirements have made it easier to justify the outlay and effort (...). Strategic investments in technology as the practice of operational resilience is maturing."

"When hiring, we found that Canada is an immature market for qualified and experienced operational resilience resources."

"Prioritization of the program by stakeholders with other, competing priorities."

Q100-16 How do you rate the priority of operational resilience for your organization over the next 12 months?

Some of the comments made by institutions:

"Operational resilience is being developed in tandem with the company's changing business strategy and risk appetite. Resilience lies at the intersection of many areas and will therefore continue to be a very high priority in order to ensure short-medium- and long-term sustainability."

"Given the importance of the topic owing to the potential external risks facing our organization and the industry (...) a phased approach with milestones that must be achieved according to a particular timetable."

"In addition to the recent hiring of a new head of operational risk and resilience, there are still challenges to be addressed in order to maintain and increase OR as a high priority."

Q100-17 How integrated is your organization's approach to operational resilience?

Some of the comments made by institutions:

"We have several different functions that work together to contribute to operational resilience, namely our business continuity, business and technology resilience, disaster recovery, information security, third-party risk management and third-party cyber risk teams."

"Teams dedicated to the operational resilience mission are in place, along with centralized funding enabling us to deliver our resilience strategies. The objective is also integrated into all our strategies related to IT and business continuity, such as modernization of our IT systems. The teams and decision-making bodies of the three lines of defence are also involved in the resilience enhancement program. In addition, discussions are underway to continue our integration efforts."

"Management outsources operational management of operations, including operational resilience, to a third party, and the response reflects that third party's approach."

Q100-18 What is your institution doing to bring together operational resilience and other related functions/disciplines such as third-party management, IT/cyber risk, business continuity?

Statements	Number of responses
We all report to the same person	65
Dual/cross reporting	89
Collaboration through an internal working committee/structure	214
Unsure/unaware	5
Nothing	6

Some of the comments made by institutions:

"In connection with risk management, there are specific groups dedicated to managing various functions and disciplines, such as third-party management, IT/cyber risk, business continuity, all of which report to the compliance committee."

"The business continuity and resilience program is reviewed and revisited through a work structure within the IT team that also includes input from the chief executive, financial and legal officers. Any major changes or revisions to the Policy are also informed by the Audit and Risk Committee and the Board."

"Consultants hired to help assess and make recommendations while integrating operational resilience considerations into other functions (TPRM, technology, BCM). Operational resilience, TPRM and BCM come under the same officer, operational resilience jointly owned with technology and cyber resilience."

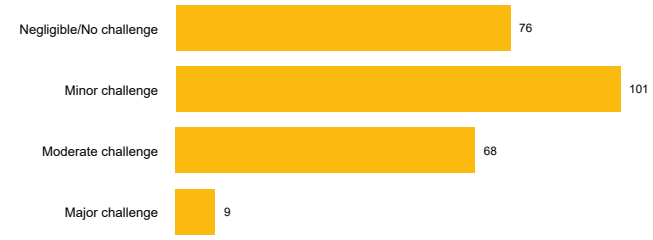
"Collaboration with these functions is critical to the success of the Operational Resilience Program. We organize monthly working and steering committee meetings that all the parties participate in."

"Business units and business functions must require all critical third-party suppliers to maintain their own business continuity capabilities as well as sufficient service levels to meet our critical requirements. A third-party business partner's capacity to respond must be validated through exercises with us and/or through the provision of sufficient evidence of exercises and tests (...)."

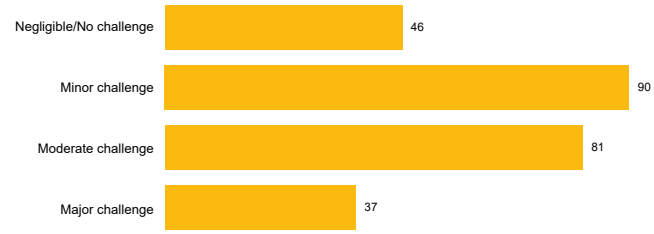
"The entire management team reports to our CEO, and operational resilience issues are discussed at bi-weekly executive scrums and monthly ERM risk committee meetings."

Q100-19 What do you perceive as the major challenges to implementing operational resilience within your own organization?

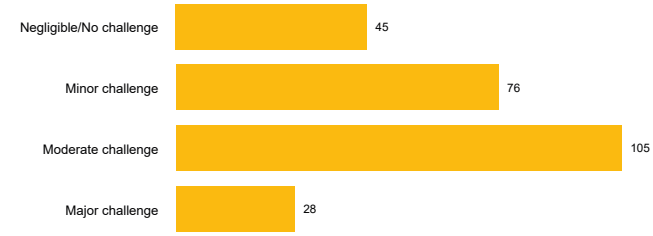
Inconsistent stakeholder understanding



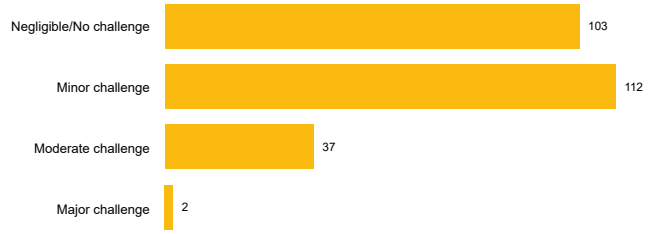
Addressing legacy infrastructure



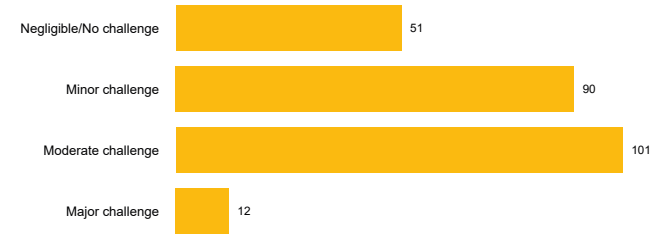
Not having the headcount and/or staff time



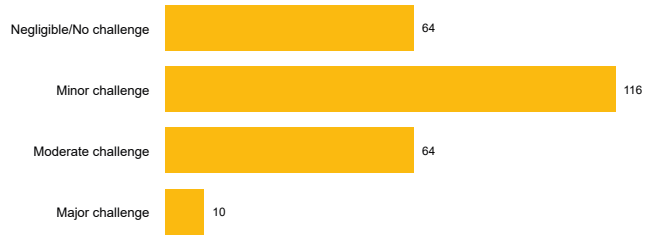
Governance and accountability: having the right people



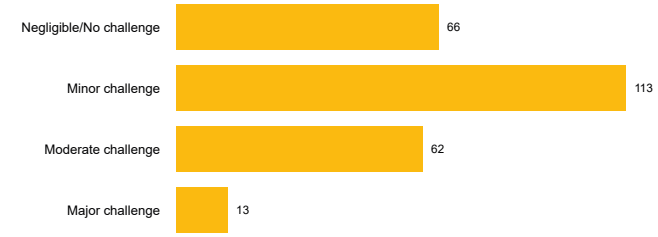
Understanding, monitoring and managing supply chain risks



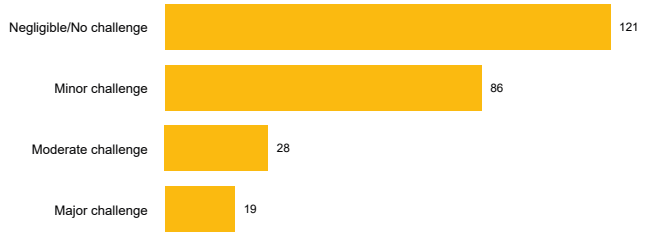
Defining correct and/or realistic impact tolerances



Mapping important business services at a sufficient level to identify vulnerabilities

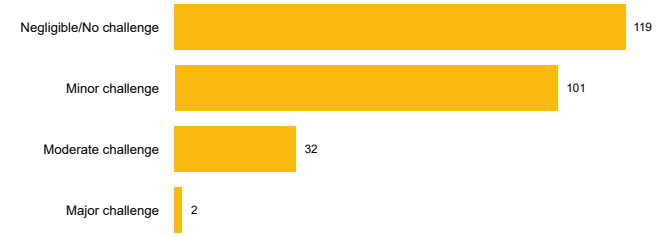


Lack of guidance from regulators and/or governments

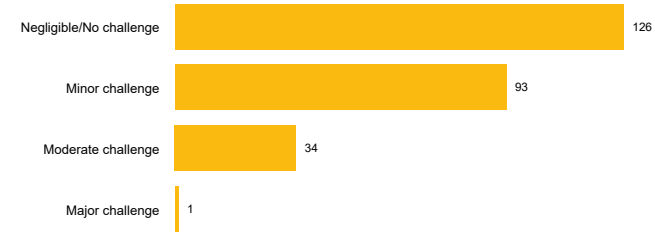


Q100-19 What do you perceive as the major challenges to implementing operational resilience within your own organization? (continued)

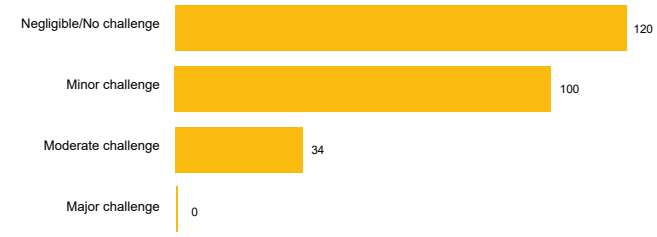
Choosing "severe" but "plausible" scenarios for testing



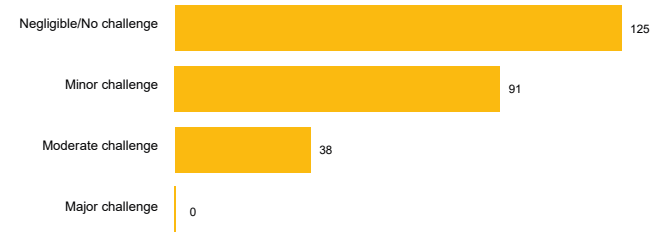
Reporting and learning from disruptions and near misses



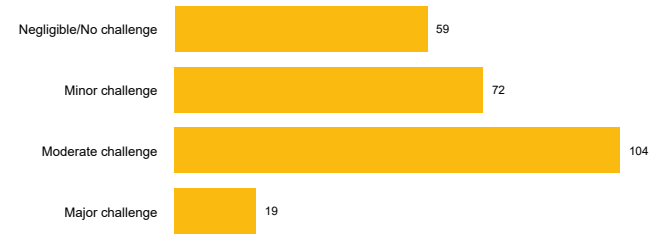
Identifying and agreeing important business services



No requirement to be operationally resilient in the sector



Embedding operational resilience into the fabric of the organization



Some of the comments made by institutions:

"A certain lack of awareness and understanding of operational resilience within the organization is making it difficult to set priorities for other implementation commitments."

"A potential lack of consistency in the various regulators' approach could present a moderate challenge for an international organization and reduce the overall effectiveness of operational resilience programs."

"(...) To embed operational resilience within the organization, fundamental governance documents must be in place, GRC and reporting tools must be in place, and the organization must be mature."

"Finding the right balance between implementing operational resilience, on the one side, and maintaining flexibility and efficiency in the way activities are conducted, on the other."

"Part of the challenge will lie in our reliance on and the number of third parties."

Q100-20 How do you see your organization using operational resilience outputs (top 5 priorities)?

Statements	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Total
Board/exec decision making	37	15	9	9	20	90
Investment planning	10	21	21	19	30	101
Provide board/exec assurance	11	13	15	9	29	77
Help recovery plans/business continuity	34	30	23	33	21	141
Satisfy regulatory requirements	19	12	23	36	36	126
Addressing customer harm when disrupted	60	29	31	26	17	163
Co-ordinating with other risk disciplines actively and regularly	4	4	12	20	13	53
Identifying vulnerabilities that could lead to an increased frequency of disruptions	37	49	45	43	22	196
Planning for the disruption of business services and measuring the capability to recover	50	64	29	33	12	188
Assessing and mitigating the effects of supply chain disruption	3	11	34	12	40	100
Don't know	2	1				3

Some of the comments made by institutions:

"While we have identified our top 5, we recognize that operational resilience outputs will support most of the elements listed above."

"We interpreted operational resilience outputs as meaning the top 5 objectives of the BC/Op Res program. We do not see Op Res as a separate program/area but, rather. as the goal of well-designed and integrated programs for business continuity, third-party risk management, cybersecurity, etc."

"All of these elements are a priority for our organization and are considered part of our Op Res roadmap."

"The results of risk assessments and financial, operational, cultural and technological monitoring are direct inputs to the resilience framework."

Q200-1 Is the operational resilience strategy documented/formalized within your organization?

Statements	Number of responses
A documented comprehensive operational resilience strategy exists. The strategy is reviewed and updated on a periodic basis and includes embedding operational resilience into the wider culture of the firm.	55
A documented operational resilience strategy exists, it is in line with business requirements and is approved at Exco/board level.	63
A documented strategy exists which considers operational resilience at a high level. The strategy is not formalized but there is a general consensus in relation to the overall objective and desired outcome.	90
No documented operational resilience strategy in place. Operational resilience is not fully understood and strategy is currently under development.	46

Some of the comments made by institutions:

"To be effective, we believe there needs to be a consistent group-wide understanding and approach to operational resilience. (...), the implementation of our operational resilience strategy and associated governance arrangements has been managed at group level (rather than entity level)."

"We have an operational resilience framework that is reviewed and approved by the board's risk management committee on a prescribed basis."

"Operational resilience is made up of several frameworks, policies, and more, as opposed to being a stand-alone program, strategy, document or policy."

"It is not formalized insofar as it exists piecemeal across various practices (continuity, succession, security). The risk management team is working to consolidate all the pieces in order to develop an overall view."

"The operational resilience strategy is the equivalent of IRM for us."

"We do not have a separate operational resilience strategy, but it is taken into account in business and technology strategies, which are designed to generate resilient outcomes for clients, the markets in which we operate and our stakeholders."

"Operational resilience is understood, but formalized documentation is limited."

Q200-2 How is the operational resilience planned, implemented and managed within the firm?

Statements	Number of responses
There is a clearly defined implementation plan, which includes timely execution. Plans include provision for operational resilience including investment and improvements required for the important business services in order to meet the (agreed) risk appetite. Plans are being reviewed on a periodic basis to address any gaps identified.	74
Plans to execute the operational resilience strategy have been approved (i.e., resources, funds and other necessities are or will be made available as required within the envisaged timeframes).	65
Prioritized the business services for operational resilience that have the potential to threaten viability, but it is still work in progress. Plans for implementing the operational resilience strategy is in the initial stages and incorporates a dialogue with the different business areas.	77
There are no documented plans to deliver the operational resilience strategy. Operational resilience is ad hoc and primarily reactive in response to a disruption to business services.	38

Some of the comments made by institutions:

"Continuity management is fully implemented within the Group. Operational resilience is a new concept that is being studied, particularly through DORA and other, similar regulatory developments."

"Operational resilience is a priority in various components of our risk management framework; it is not a separate program with a separate implementation plan. (...) It is an ongoing process integrated into the overall business and strategic planning processes."

"The operational resilience plan is designed to align with the critical business processes, services, products and technologies that execute and operate the organization's critical operations. Owing to the inventory of priority services, resilience scenarios and stress testing measures and activities will be prioritized, executed and reported."

"We are in the process of implementing our operational resilience program."

"Operational resilience is a work in progress."

"Plans are built and managed between matrix departments."

"We established the corporate operational resilience standard in December 2021 describing our framework for managing non-financial operational risks with an impact on operational resilience, as well as a multi-year supporting implementation program that is overseen by the operational resilience steering committee (bi-monthly meeting)."

Q200-3 Has the institution aligned its governance structure with its strategic and operational resilience goals?

Statements	Number of responses
There are formal governance committees that review Operational resilience related business decisions and exceptions are periodically reported to the board. The governance structure is subject to independent assurance review by internal audit and/or external parties. The board is effective in providing governance and leadership for the resilience agenda, and in developing the necessary capabilities. Risk, compliance and internal audit independently report into the board via risk and audit committees on technology and operational resilience.	49
The governance structure has been designed to support the firm's business model, risk appetite and is aligned to its strategic operational resilience objectives. The board and senior management are fully aware of their responsibilities for maintaining effective oversight. Risk, compliance and internal audit independently report into the board.	110
There is a documented governance structure in place, but it requires further alignment with the firm's strategic and operational resilience objectives. Senior management roles and responsibilities for overseeing the firm and its activities have been defined. Independent assurance on operational resilience matters has been provided by external party but the outcomes need to be embedded internally across the 3 lines of defence.	69
No documented organizational structure currently in place. Roles and responsibilities are determined on an ad hoc basis.	26

Some of the comments made by institutions:

"At the enterprise level, the board's risk committee has been provided with regular status reports on resilience program developments, which describe the key activities and timetables for assessing the resilience of our most critical services."

"There is a business continuity committee, which reports on its activities, including resilience issues, to the board."

"No independent assurance has been provided by an external party."

"Although no specific structure has been documented, the governance and organizational structure supporting operational risk management activities are largely adequate and sufficient to support an operational resilience framework."

"Operational resilience is currently being developed. The governance structure will be aligned with the organization's strategic and operational resilience objectives."

"Since operational resilience is currently embedded in the operational risk management program, management has taken advantage of the existing governance structure at the management and board levels."

"Operational resilience governance is aligned with operational risk management governance as defined in the AMF's 2016 Operational Risk Management Guideline, Section 1 – Governance of financial institutions."

Q200-4 How do you assess the effectiveness of your operational resilience governance structure?

Statements	Number of responses
The operational resilience governance structure is well established and subject to an independent assurance by internal audit/external parties. Accountable executives (including the board) provide effective leadership from a challenge and oversight perspective.	56
The operational resilience governance structure supports the firm's business model and is being embedded across the organization to align with its strategic objectives. Senior management provide effective challenge and oversight where necessary.	105
Operational resilience governance structure with defined roles and responsibilities in place. The governance structure would benefit from further alignment with the firm's strategic objectives.	33
No formal assessment undertaken to assess if the operational resilience structure is fit for purpose.	60

Some of the comments made by institutions:

"The effectiveness of our BC/Op Res program is regularly assessed by our internal audit team and was recently assessed by an external third party."

"The BC plan is revised annually as part of SOC 2; tabletop exercises are conducted each year with external support; External assessments of our BC plan are conducted periodically."

"The effectiveness assessment will be monitored and measured through the establishment of a set of key resilience indicators. These will be reported through the operational risk committee to the board's risk committee on a quarterly basis. We are in compliance with Section 2.2 Monitoring and reporting of the AMF's 2016 Operational Risk Management Guideline. The effectiveness of the operational resilience governance structure will also be consistent with this guideline."

Q200-5 What level of knowledge and skills exists at the senior executive level for operational resilience?

Statements	Number of responses
All senior executives (including members of the board) have sufficient understanding to provide effective oversight of the firm's operational resilience strategy. At least one senior executive has specialist knowledge and skills which the other executives can draw on.	122
At least one senior executive (including members of the board) has sufficient understanding to provide oversight of the firm's operational resilience strategy. Training is scheduled to develop other senior executives' capabilities in the next 12 months.	91
Senior executives have limited skills within the operational resilience areas. There is a dependency on external knowledge and skills to address gaps and provide effective oversight of the firm's operational resilience strategy. There is a plan to upskill / appoint senior executive with relevant experience in the next 12 months.	14
No senior executives currently have the relevant knowledge and skills to provide effective challenge and oversight of the firm's operational resilience strategy. There are no plans in place to address this.	27

Some of the comments made by institutions:

"All senior executives and board members have a good understanding of operational resilience. (...) leaders at all levels understand the roles and responsibilities and have the knowledge they need to develop and maintain effective operational recovery plans based on the firm's priorities."

"We are not in a position to give you a specific answer on this question, since it has never been assessed directly."

"Now that the concept of organizational resilience has been brought to our attention, a proficiency training plan will be put in place."

"Senior executives and the board are literate in the areas of operational risk management, business continuity and disaster recovery, and their knowledge of the aspects of operational resilience needs to be improved with the support of appropriate communication/training, if necessary."

"Senior management and the board have different levels of knowledge of operational resilience. However, the CRO continues to champion the principles of operational resilience (...) formal training is still being developed."

Q200-6 How do you ensure effective oversight and challenge is provided by the board and senior management?

Statements	Number of responses
The board, committees and senior management have all the appropriate metrics available, enabling them to provide effective oversight and challenge. The 2LOD and 3LOD perform their challenge and oversight responsibilities effectively. The management information produced enables governance-related decision making.	77
The oversight being exercised by the board, committees and senior management is structured, documented and normalized. Management information is used to inform senior management and as input into most decision making. 3rd LOD reviews the management information and provides independent assurance.	92
The oversight being exercised by the board, committees and senior management is high level and ad hoc. Management information is used to inform senior management and as input into some decision making.	84
There is no evidence that the board, committees, and senior management are providing oversight. Independent assessments have highlighted a poor decision making/judgement environment.	1

Some of the comments made by institutions:

"The firm's board, committees and senior management oversee the operational resilience strategy for important business services. We are in our first life cycle and are currently establishing a formal Op Res structure."

"We recently started to report to the Board and, since then, have been expecting guidance to be strengthened in the coming quarters. We plan to report to and update the Board on a quarterly basis, enabling it to provide effective challenge and oversight."

"Oversight is being strengthened as part of the improvements identified in the program. The 2LOD and 3LOD are fulfilling their challenge and oversight responsibilities effectively."

"The Op Res framework is in the early stages of implementation, and oversight up to this point has been high level. Implementation progress reporting is in place, but the measures have not yet been communicated."

Q200-7 Have all responsibilities been assigned at the appropriate level and signed off by relevant stakeholders?

Statements	Number of responses
Roles and responsibilities are integrated into job specifications and performance management. Roles and responsibilities have been signed off and been communicated to key stakeholders, including regulators. Matters such as conflicts, duplication and shared responsibilities have been clearly identified, documented and the risks mitigated.	37
Structure in place with operational expertise available at board/senior management level. Key roles and responsibilities for operational resilience are documented with ownership clearly defined and understood.	117
Individuals responsible for operational resilience have been identified with reliance on external advisers to supplement and address knowledge and/or skills gaps (where necessary).	66
Ownership/roles and responsibilities not fully determined and understood. Roles and responsibilities are allocated on a reactive basis.	34

Some of the comments made by institutions:

"Governance is in place for the various components of an operational resilience program (e.g., third-party, technology, data and information security risks)."

"We also do business with external firms (breach coach, forensics and communications)."

"Roles and responsibilities are currently being reviewed and updated as part of identified program improvements."

"Governance and risk frameworks and practices have been in place at the enterprise level and within IT and claims operations for many years now, but they are not qualified as 'operational resilience.'"

Q200-8 Do your staff and senior staff members understand about the strategic objectives of the firm and how the operational resilience capabilities enable these?

Statements	Number of responses
All staff are aware of the strategic objective to have an operationally resilient firm. Discussion of operational resilience is evidence at board level and considered in all business-as-usual activity. The culture of the firm is designed to promote operational resilience, and this is exhibited in the behaviour of personnel at all levels. Operation resilience education and awareness is considered in business decisions.	42
Most staff are aware of the strategic objective to have an operationally resilient firm. Training sessions and seminars etc. are being held to improve staff knowledge of operational resilience including security training and awareness. There is some evidence of operational resilience being embedded in the culture of some parts of the firm.	88
Some staff (including senior staff) are aware of the strategic objectives and have an awareness of operational resilience. Basic high-level training is provided including security training and awareness.	103
The operational resilience strategy has not been cascaded to staff. Staff do not appear to be aware of operational resilience and no formal training is in place to address the gap.	21

Some of the comments made by institutions:

"Several programs supporting operational resilience have rolled out training elements, including mandatory organization-wide training for all employees."

"The company is aware of the importance of further developing a culture of operational resilience. The main challenge is closely related to the staff movements experienced by all employers."

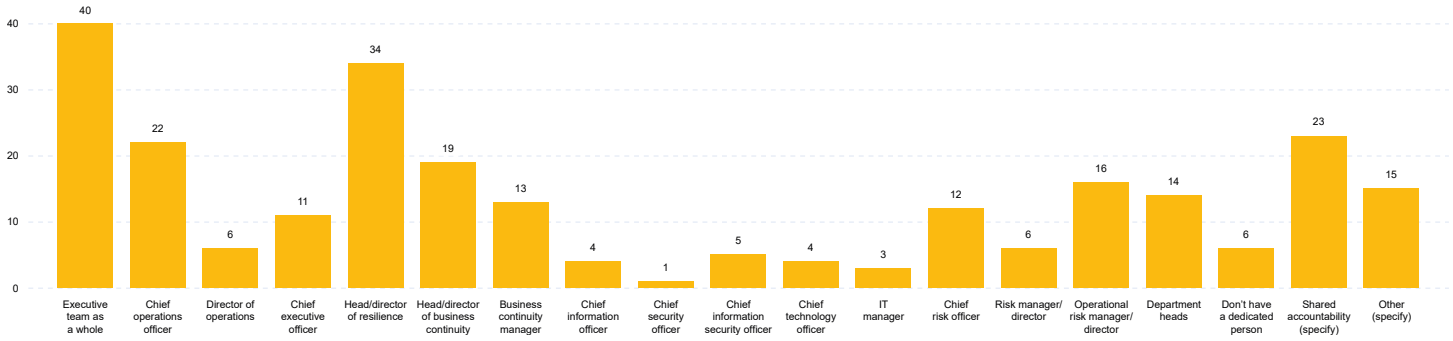
"We have enterprise-wide business continuity and awareness training requirements and an annual compliance management training program."

"Most leaders are aware of the importance of operational resilience. More training, including tabletop exercises, is needed to ensure clarity of roles and responsibilities."

"The structure is in place, but it requires expanded opportunities for operational resilience."

"Emergency preparedness has been cascaded down, as an element of operational resilience, to all trained staff."

Q200-9 Person taking the day-to-day lead for operational resilience within the organization?



Some of the comments made by institutions:

"This element has not yet been made official. The responsibility will potentially lie with the owners of identified vital operations. The CRO will also have responsibility as an executive owner."

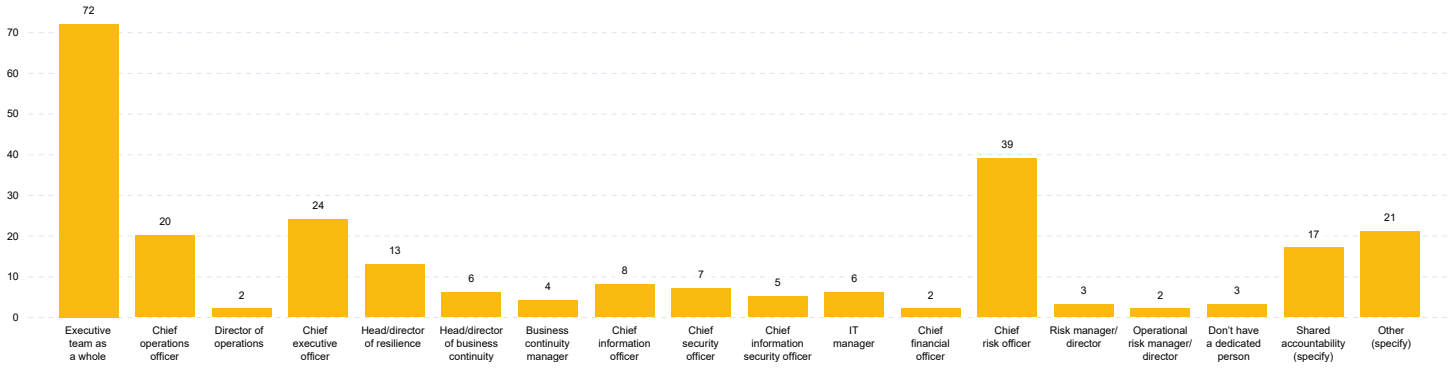
"Operational resilience is not the responsibility of one person. There is a shared responsibility at the group level between: the global head of enterprise resilience, the chief information security officer (CISO), the third-party risk manager (TPRM), the operational risk manager, the IT manager and those responsible for all the relevant activities. This responsibility is largely assumed at the entity level by the chief commercial officer."

"The business continuity manager is responsible for maintaining BC tools and processes. Risk management staff ensure that other risk management frameworks (e.g., cybersecurity, third parties) appropriately reflect operational priorities in terms of resilience."

"Management is entrusting management of its operations, including operational resilience, to a third party."

"We also recently hired a new chief operational risk and resilience officer, who will also be involved in this activity."

Q200-10 Person with overall responsibility for operational resilience within the organization?



Some of the comments made by institutions:

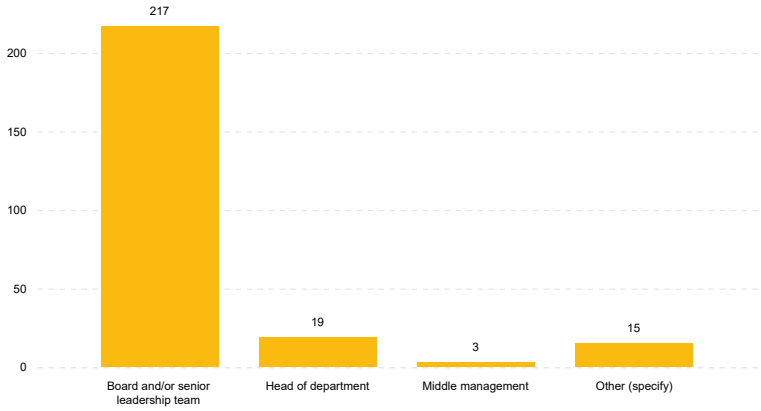
"Risk will be owned by the first line – probably a member of the executive, if not the CEO."

"The most developed component of operational resilience is currently found within the IT department. As such, the CIO is the closest to this function. (...) structure will be further clarified as we develop our operational resilience program."

"The CIO is responsible for the BC and cybersecurity frameworks, as well as some of the third-party risk management. The CRO is responsible for ensuring that operational resilience is reflected in all applicable frameworks."

"Responsibility shared between the Business Resilience Office, Risk Management, Information Security, Incident Management and Disaster Recovery."

Q200-11 What level is the person with overall accountability for operational resilience within your organization?



Q200-12 What is your opinion of establishing a board level appointment who is responsible for assessing resilience at all levels and ensuring all resilience building efforts within the institution are aligned and co-ordinated?

Some of the comments made by institutions:

"A sub-committee of the board will oversee all the organization's risks."

"Operational resilience is the responsibility of senior management. (...) There is no advantage to centralizing this matter with one person during a board meeting."

"Must be under the responsibility of the risk management committee. The chair of this committee is already on the board."

"We will consider the appropriate structure as we continue to implement our operational resilience program."

"We respectfully believe that the board should be informed of the steps taken, but that such a function (assessing operational resilience) should be the responsibility of management."

"We don't think it is necessary. The role of the board is to oversee the organization's key risks, including operational resilience."

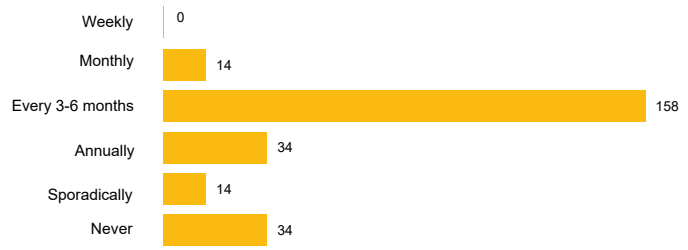
"The board should provide constructive challenge and oversight of these activities, as it does for other business activities."

"The board challenges aspects of operational resilience without there being a dedicated position."

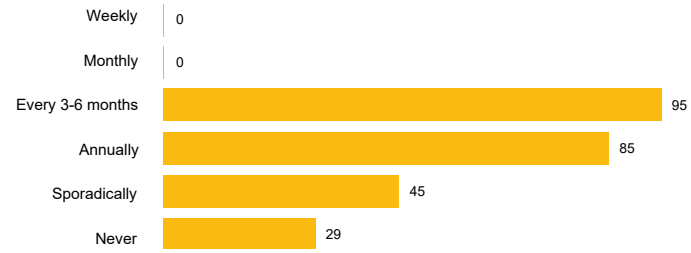
"A board member of the board has been given responsibility for the operational resilience program, with governance arrangements in place to ensure oversight of the broader/related risk frameworks."

Q200-13 How often is operational resilience on the agenda of the following committees or their nearest equivalent in your organization?

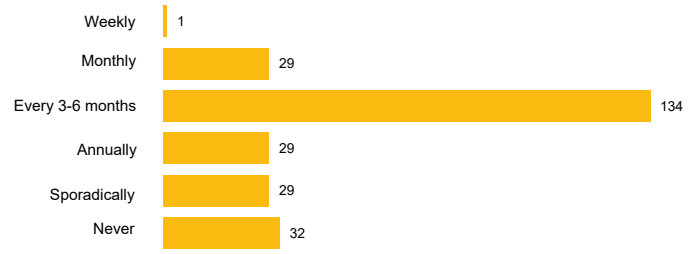
Risk committee



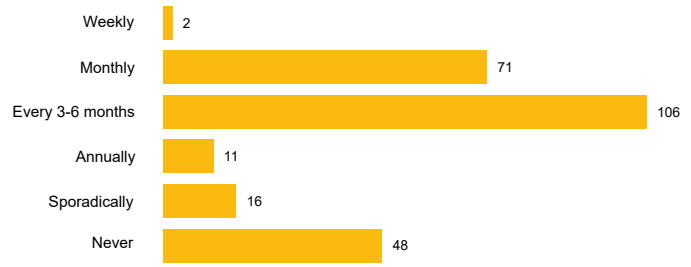
Board



Executive committee



Technology risk committee



Some of the comments made by institutions:

"We will start reporting on the operational resilience program to the board. (...) Currently, such reporting is on an ad hoc basis to the operating committee and monthly updates are provided to the operational risk committee."

"Our CRO reports quarterly to our compliance, risk and risk management review committee, which includes business continuity and other operational resilience risks."

"Currently, operational resilience is a regular item on the agenda of the board."

"Because of the importance of this initiative, it is presented to all members of the Board. We do not have a technology risk committee."

"Management is entrusting management of its operations, including operational resilience, to a third party. The third party does not have a dedicated risk committee or a technology risk committee. (...) The third-party executive committee discusses business continuity, if necessary, at least once a year."

"Locally, we do not have a dedicated risk committee or a technology risk committee. Our board discusses business continuity at least once a year, but the transition to operational resilience has not yet taken place. (...) Globally, our operational risk committee reviews various elements of our Op Res program an average of 2 to 3 times per year."

"There is no set frequency for including operational resilience on the agenda – matters related to operational resilience are addressed as needed. On average, option 3 (every 3 to 6 months) would be the most appropriate response. However, there are times when operational resilience may appear more frequently on the agenda. In addition, we have a business resiliency council that meets every three weeks."

Q200-14 How would you characterize your annual budget designated for your operational resilience contingency?

Some of the comments made by institutions:

"Since we don't have a program, no budget is allocated. It's included in our operating expenses."

"We have an emergency budget for cybersecurity. Other operational resilience contingencies would be funded from available capital."

"Priority has been given to funding operational resilience. We have approved funding for the next 15 months and will seek additional funding thereafter."

"We have specific operational budgets for the teams responsible for various aspects of our enterprise-wide operational resilience program."

"There is currently no budget dedicated specifically to operational resilience, but where there are separate initiatives in support of operational resilience elements, the contingency reserve would follow project management practices."

"A budget is in place for business continuity management, including technology and a dedicated resource, but it needs to be expanded to cover operational resilience."

"The Board recognizes that additional financial resources are needed to address this growing need."

Q200-15 How do you characterize your annual budget for operational resilience as changing over the next 12 months?

Some of the comments made by institutions:

"We do not intend to substantially adjust our current operational budgets. Our firm's surplus is currently sufficient to withstand a wide range of operationally disruptive events."

"There is currently no budget dedicated specifically to operational resilience, but there are separate initiatives to support the strengthening of operational resilience elements included in the operational risk, technology and business budgets."

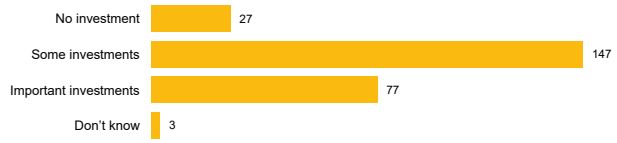
"We anticipate that our financial needs will increase as we develop the program."

"As regulatory guidance becomes clearer with a definite date of entry into force, we would also consider allocating more resources to operational resilience."

"As we continue to grow and invest in the organization, resilience plans and goals will be factored into this process to avoid having to play 'catch up.'"

Q200-16 Level of investments made in the last two years by your organization in the following areas.

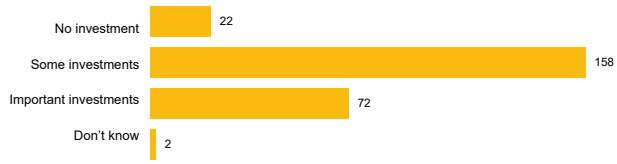
Mapping of critical processes



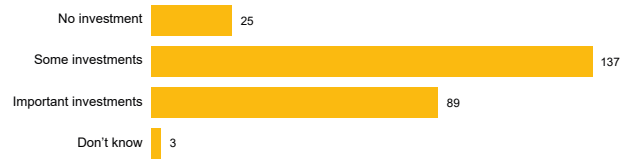
Identification and management of threats and vulnerabilities of critical operations

Business continuity planning and testing

Identification of interconnections and interdependencies

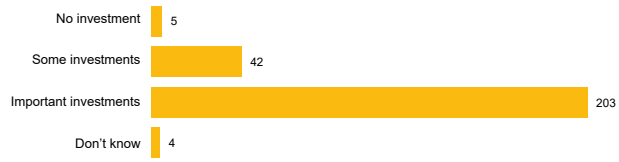


Third-party dependency management for the delivery of critical operations



Incident management

Protection, detection, response and recovery programs for ICT and cybersecurity resilience



Q200-17 Level of planned investments over the next two years by your organization in the following areas.

Mapping of critical processes

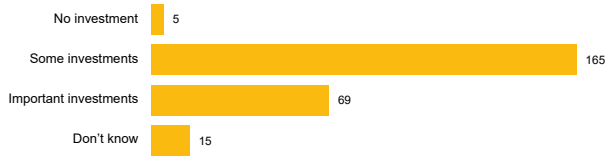
Identification and management of threats and vulnerabilities of critical operations

Business continuity planning and testing

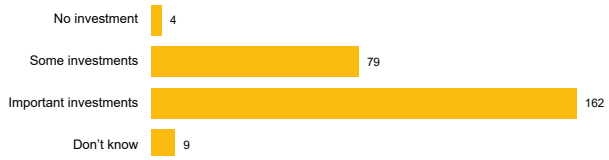
Identification of interconnections and interdependencies

Third-party dependency management for the delivery of critical operations

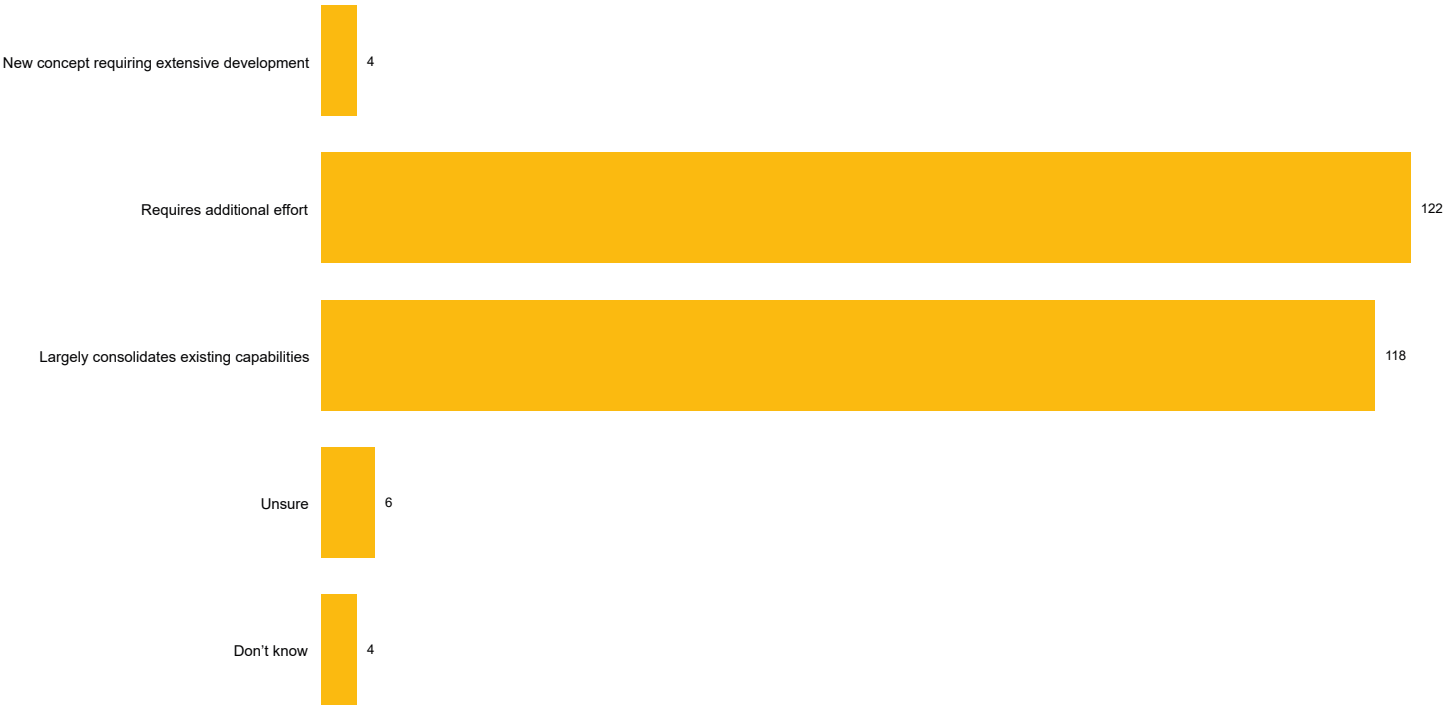
Incident management



Protection, detection, response and recovery programs for ICT and cybersecurity resilience



Q200-18 What impact does operational resilience have on your existing risk management capabilities?



Some of the comments made by institutions:

"Our risk management framework is fairly mature, but we need to more explicitly embed reflection on operational resilience into it."

"Resilience is an integral part of our operational risk management practices. However, we are currently reinforcing the systemization of this approach, particularly at project level."

"This is a new concept for us, and it will require additional efforts."

"We are reviewing our existing processes and procedures to ensure that we correctly identify critical risks and adjust the way we address them."

"Consideration of operational resilience must be embedded into existing risk management capabilities."

"We have not yet been able to measure the extent of the additional efforts that will be necessary because we have not completed the plan."

"Our risk management capabilities are sufficient to support the ongoing integration of operational resilience into the organization. However, (...) amending our practices requires the involvement of several established governance mechanisms."

Q200-19 Do you have an established organizational structure and governance process for managing the operational resilience risk and does it outline the responsibilities and accountabilities?

Statements	Number of responses
Operational resilience risk management function has been established and fully embedded across the organization with clear articulation of roles and responsibilities. Governance structure and process have been independently reviewed with documented evidence. The board is aware of key risks including the ones that have exceed risk appetite and/or need approval.	39
Organogram outlining the operational resilience risk management structure is in place. Governance structure and framework has been established outlining the overall approach and is aligned to the strategic objectives. Relevant committees and reporting structures in place with senior individual nominated. This individual is the accountable executive and has oversight of the operational resilience risk. Management information is produced and shared with senior management on a periodic basis.	103
Operational resilience governance structure and framework has been established but not fully embedded. Roles and responsibilities have been outlined and assigned to key individuals. Accountable executive will be assigned in due course. Management information is produced on an ad hoc basis and shared with senior management.	59
Operational resilience governance structure does not exist. We are in the process of establishing the governance process to manage operational resilience risk.	53

Some of the comments made by institutions:

"Resilience is part of technology risk governance and management, the roles and responsibilities for which have been enhanced in recent years. The risk appetite frameworks are also applied to resilience risks."

"There is no organization chart outlining the operational resilience risk management structure."

"An inquiry is underway, with the aim of building on the existing governance structure for business continuity management."

"We will seek to assess and build on our existing business resilience governance framework."

"Once implemented, we will formalize a governance structure to enable effective reporting and create visibility."

"A governance model with roles and responsibilities is currently under consideration. (...) Operational resilience governance is aligned with the operational risk management governance as defined in the 2016 AMF Operational Risk Management Guideline, Section 1 – Governance of financial institutions."

Q200-20 To what extent is management information, including key risk indicators, used to inform decision makers on the performance of operational resilience controls?

Statements	Number of responses
Senior executives periodically review management information on operational resilience controls. Management information is also used to inform senior management on key issues related to operational resilience and for relevant decision making. Key risk indicators are reviewed after every significant event. This management information in conjunction with the risk and controls self-assessment is used to assess the effectiveness of the control environment and for relevant decision making.	67
2nd line of defence staff, such as operational risk leads, periodically review management information on operational resilience controls in conjunction with risk and control self-assessment to assess the effectiveness of the internal control processes.	80
Risk control framework developed and implemented across the organization. 1st line staff, such as technology or operational leads, periodically review management information on operational resilience controls to make informed decisions.	49
Management information for operational resilience controls is captured in an ad hoc manner and not periodically reviewed.	58

Some of the comments made by institutions:

"Specific controls for operational resilience, in addition to existing controls in technology, cybersecurity and third-party risk, are currently under development."

"KRIs are in place and reported quarterly."

"The considerations relating to formalized management information for controls will be integrated into the future construction of the program."

"It's a work in progress that needs to be improved for operational resilience."

"Key operational resilience risk indicators are integrated into the executive management committees, such as the IT management committee and the risk and compliance committee."

Q300-1 Has your financial institution identified and documented important business services that if disrupted could cause harm to consumers or market integrity?

Some of the comments made by institutions:

"The critical activities of all areas of the organization are identified, and tolerance for disruption is established based, among other things, on the impact on business relationships and client satisfaction."

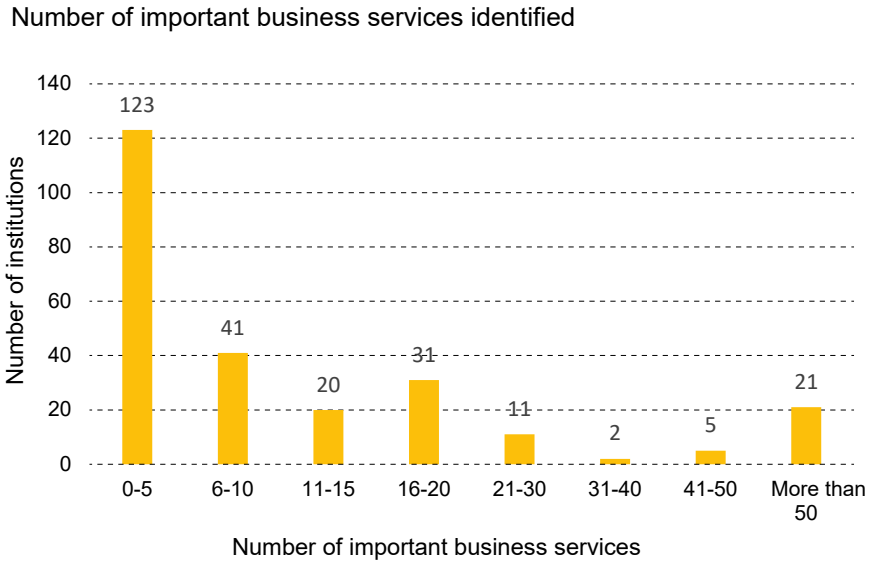
"We have identified 20 essential services within the global business that, if disrupted, would cause intolerable levels of harm to clients, market integrity and financial stability and/or threaten the safety and soundness of the institution."

"Even if critical processes are identified, they relate to the firm's operations and not to the harm caused to consumers or market integrity."

"This question is difficult to answer, as 'important business services' can mean different things to different organizations."

"All business services have been identified and ranked by impact on the client, impact on employees, and other considerations."

Q300-2 How many important business services has your organization identified?



Q300-3 How do you ensure the important business services identified are at the level to which an impact tolerance can be applied and allow boards and senior management to make prioritization and investment decisions?

Statements	Number of responses
There is a good understanding of the business services and its potential impact. Services have been identified at an individual level – they're not sub-divided into multiple services. The impact is clearly understood and tolerance has been set at the right level. Management information is produced on a regular basis to keep the relevant stakeholders informed. The business services are identified in a way that allows boards and senior management to make prioritization and investment decisions.	94
The are some gaps in the understanding of the business services and its potential impact in the event of an operational disruption. Management information is populated on an ad hoc basis with the board and senior management aware of the governance process to allow them to prioritize and make informed decisions.	115
There is weak understanding of the business services and its potential impact in the event of an operational disruption. Board awareness is limited.	6
We do not have a thorough understanding of the important business services and its impact.	4
We have not identified and documented important business services.	35

Some of the comments made by institutions:

"The important business services are identified. As work is still in progress, not all the tolerances have been developed and approved by the board and senior management."

"The information is currently documented at the operational unit level. A project is underway to centralize information for operational resilience purposes. Work is scheduled to begin shortly."

"We identify the processes at the level of the functions that are necessary to deliver a business service from end to end. Once the underlying functions within a business service are identified, they are prioritized using a risk-based approach that considers the criticality of the service and availability (...)."

Q300-4 Has the firm considered all parts of its business and all the services it provides when identifying important business services?

Statements	Number of responses
All parts of the business in Québec are considered in the identification of the business services. This has been clearly defined and fits within our organizational structure. For example, we may be able to show how our businesses are structured according to economic functions, business or products lines or end user segments. This is used as a starting point for identifying business services.	135
In identifying the important business services, consideration is given to some services supported by a credible plan to include all the services.	53
In identifying the important business services, consideration is given to the services but this is done in an ad hoc manner and does not extend to all the services.	14
Consideration is limited to the business but does not extend to all services.	12
We have not identified and documented important business services.	40

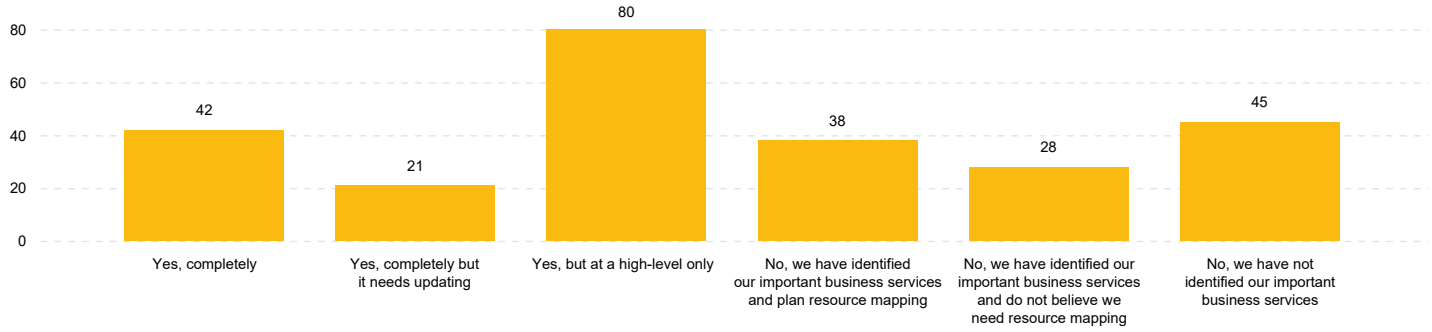
Some of the comments made by institutions:

"Although the term 'business services' is not used, all activities in each of the business lines have been assessed and their tolerances for disruption have been established."

"Critical activities have been determined via business continuity. As for resilience, the important business services will be identified."

"In the context, the concept of 'important business services' as defined by the AMF is not observable at the level of our activities."

Q300-5 Has your organization previously completed resource mapping of important business services?



Some of the comments made by institutions:

"As a small institution, resource mapping is not a necessary exercise to the extent that information is generally known to all officers and can be quickly validated."

"Resource mapping has been completed for all business services but could be improved."

"At this time, we are continuing our work to identify additional critical business services."

"The materiality assessments have been completed. Assessments of the impact on activities completed at the business line level. Order of system recovery determined by criticality."

Q300-6 What is your governance and accountability structure for the identification, delivery and maintenance of resilient business services?

Statements	Number of responses
There is well defined governance structure in place outlining the accountability and ownership of important business services. An up-to-date ownership of important business services, supporting resources and interdependencies is maintained and reviewed.	69
Ownership of important business services is documented and includes business ownership of supporting resources (enablers). The process is dynamic and any changes in business services and supporting resources are timely reflected in ownership responsibilities.	75
Ownership of important business services and required resources is documented however, supporting resources are not mapped and addressed in an ad hoc manner.	64
The governance structure has not been fully developed. As a result, the accountability and ownership for important business services is not defined or incomplete.	46

Some of the comments made by institutions:

"The very structure of the organization makes it easier to identify the owners of the business services and the necessary resources supported by the data collected as part of the business continuity program."

"Having the correct ownership, keeping documentation up to date and reassessing criticality if something changes, are all part of the plan for building the operational resilience program."

"Based on the described categorization, ownership is clearly articulated. Documentation of the interdependencies between processes is still under development."

Q300-7 How do you ensure that all business services, required resources, and interdependencies have been identified and the completeness have been verified?

Statements	Number of responses
All business services, required resources, and interdependencies are identified and documented. There is a process to capture changes in the business and respectively reflect in the documented inventory of business services, required resources, and interdependencies.	71
All business services, required resources, and interdependencies are identified and documented. Changes are updated and reflected in the inventory on an ad hoc basis.	48
Business services, required resources, and interdependencies are identified for important business services and documented on an ad hoc basis.	97
No business services, required resources or interdependencies are identified or documented. Any requirement for resources is dealt with on a reactive basis.	38

Some of the comments made by institutions:

"Although the term 'business services' is not used, all interdependencies of critical activities have been documented as part of the business continuity program."

"Critical activities were determined via business continuity. As for resilience, important business services will be identified."

"We have a process in place to carry out an annual assessment of the business services performed, as well as an ad hoc process if a material change is made, which are identified through normal project or risk processes."

"We have put in place business continuity plans that are updated every year. (...) There is a change management process that includes identifying updates for the BCP and disaster recovery. This has not yet been done for all the business services."

Q300-8 How do you identify and classify critical/important business services including any external and internal factors to timely reflect in the criticality ratings? Does this process incorporate the resource requirements and interdependencies?

Statements	Number of responses
A criticality assessment for identified business services, required resources, and interdependencies is performed and documented. There is a process in place to capture changes in the criticality due to changes in internal or external factors, and respectively reflect in the documented inventory of business services, required resources, and interdependencies.	34
Criticality assessment for all identified business services, required resources, and interdependencies is performed and documented. Periodic reviews are undertaken to incorporate any updates/changes to ensure the list is maintained and is kept up to date.	107
Criticality assessment of identified important business services, required resources, and interdependencies is performed and documented however, the list is not maintained or kept up to date.	67
No criticality assessment is undertaken to identify the important business services, required resources and interdependencies. Requirements are assessed and addressed in a reactive manner.	46

Some of the comments made by institutions:

"There are criticality assessments in place for business continuity, succession and incident management issues and for resolution and recovery plans. This exercise has not been completed for operational resilience."

"The criticality assessment has been carried out but not documented."

"We are currently in our first cycle of operational resilience practice. Periodic reviews will therefore be conducted to incorporate updates/changes into future cycles."

"Criticality is assessed (...) documented for all identified business services and updated at least once a year. Clear criteria have been defined to assess criticality and recovery priorities."

Q300-9 How do you identify the resilience requirements for your most important business services? How do you ensure the requirements are reviewed and kept up to date?

Statements	Number of responses
Resilience requirements for all important business services are identified and documented. There is a process in place to capture change in the requirements due to changes in internal or external factors, and respectively reflect in the documented inventory of business services.	46
Resilience requirements for all important business services are defined and documented. An up-to-date inventory is maintained, and the requirements are periodically reviewed and improved when required.	69
Resilience requirements have been defined for the important business services. An inventory has been established and reviewed on an ad hoc basis.	80
No resilience requirements have been defined for the important business services. A need for an inventory has been identified and will be developed in due course.	59

Some of the comments made by institutions:

"Resilience requirements are established for technological systems and in managing the most significant third parties."

"We identify resilience needs (in terms of recovery time objectives) by business line/service function and update business continuity plans at least once a year. We carry out the exercise in respect to the business line one process at a time, on an end-to-end basis."

"Clear criteria have been defined to assess the criticality of all business processes as well as recovery priorities and requirements (resilience). All business processes are reviewed at least once a year. This review process is managed by the business continuity team."

Q300-10 To what extent have you completed the inventory of your important business services and its interdependencies?

Statements	Number of responses
Inventory of important business services and interdependencies is reviewed on a periodic bases and kept up to date. There is a process in place to capture and reflect changes in the internal or external dependencies. The list and the underlined process is independently reviewed.	71
A full inventory of important business services and interdependencies is maintained but not fully reviewed. Appropriate tools are in place to capture and reflect any changes to the inventory.	56
Inventory of business services and its interdependencies is maintained and includes any 3rd party dependencies. Any changes to the inventory are identified and documented in an ad hoc basis.	69
There is no inventory of business services, required resources and interdependencies. All requirements are currently maintained by individual business units and not consolidated in a central place.	58

Some of the comments made by institutions:

"We have identified the recovery time objectives, dependencies and criticalities that inform the resilience requirements."

"The inventory of significant third-party dependencies is made and maintained at the level of business lines' critical activities."

"As work on the program is still underway, we have identified the important business services and are well on our way to mapping interdependencies. A process is in place to reassess any significant changes."

"We have an inventory of important services, but we have not mapped interdependencies."

Q300-11 How do you ensure that all the resilience requirements for your most important business services and its interdependencies have been documented and kept up to date?

Statements	Number of responses
Resilience requirements have been identified, classified and documented for all important business services including any external and internal factors. The list reflects the criticality ratings and is reviewed on a periodic basis to ensure it remains up to date. The list also incorporates the resources requirements and interdependencies and is independently reviewed.	48
Resilience requirements have been identified, classified and mapped across all important business services at a business unit level. A consolidated list of the requirements is being developed to maintain a single source and ensure integrity of the requirements. Furthermore, the list will also include service criticality rating, resources requirements and interdependencies.	95
Resilience requirements have been identified and classified on an ad hoc basis for all important business services. Requirements for any external and internal factors and any interdependencies is not fully considered or consistently applied.	62
No resilience requirements for business services or interdependencies are identified and documented. Resilience requirements including any interdependencies are addressed on a reactive basis.	49

Some of the comments made by institutions:

"We have set recovery time objectives as part of the business impact analysis, but we recognize the need for an inventory of all operational resilience requirements."

"While we have identified and documented the important business services for legal entities in other countries, we have not yet done so for Canada."

Q300-12 In the event of an operational disruption, how do you prepare and prioritize your resources and actions in order to ensure continuity of your business services and minimize harm to consumers/customers?

Statements	Number of responses
Process in place to capture near misses, lessons learned and feed into testing and assessment processes. Horizon scanning is embedded to identify and prepare for potential events as part of BAU. Business continuity process is matured and fully embedded across the organization with senior management participation. Unannounced tests are carried out to test the framework. Business continuity framework is tested on a periodic basis to assess its effectiveness.	42
Integrated detection and notification process in place with other key stakeholders and 3rd parties are in place and tested periodically. Data recovery arrangements and testing includes scenarios informed by past incidents, management information and 3rd party dependencies. A business continuity framework in place to ensure a co-ordinated response can be provided during an operational incident. Simulations are carried out with relevant stakeholder, including senior management on a periodic basis.	100
In the event of an operational disruption, data recovery arrangements and testing requirements are determined by the business and include service providers (including 3rd party service providers) with relevant metrics and/or frameworks defined. *There is a business continuity framework in place to ensure a co-ordinated response during an operational disruption. Simulations are carried out on an ad hoc basis to test the business continuity framework.*	107
In the event of an operational disruption, service recovery arrangements are not determined or are determined in isolation. For example, IT determines the actions without any input from the business. Response to ensure any continuity during an operational disruption is ad hoc.	5

Some of the comments made by institutions:

"For now, because of your small size, we are using near-misses or incidents such as the pandemic to test the business continuity framework rather than simulations."

"For now, tests are 'announced,' but test participants are not informed of the type of disturbance scenario (...) have organized unannounced exercises in the past and we will seek to implement them in the near future."

"Tests are carried out periodically. Breach coaching exercises are also carried out periodically. Disaster recovery tests are carried out annually on critical systems and networks."

Q300-13 What is your testing approach and how frequently are your continuity arrangements tested to ensure your business services remain effective and fit for purpose?

Statements	Number of responses
Test plans include scenarios that take into account systemic, environmental issues impacting multiple business services. Both short duration and long duration incidents that impact business services are assessed in test plans. Plans are tested on a periodic basis and updated to reflect any changes.	53
Testing approach is well defined and driven by established policies and procedures. Tests plans and scenarios facilitate decision making and cover business services as a whole including 3rd parties. Test plans accommodate for flex resources to ensure continuity of priority services to minimize business disruption and harm to consumers based on the impact and duration of the incident/test plan as required. Continuity testing is carried out as per scheduled and lessons learned/enhancements are incorporated in the test plans.	61
Testing approach is well defined and driven by established policies and procedures. The testing approach defines the test frequency, types of tests, use of drills etc. and is limited to individual platforms or systems. Continuity testing is carried out as per schedule on and the test outcome is recorded for transparency.	110
Testing approach is not fully developed and is applied in an ad hoc manner. Continuity testing is not carried out and response to an operational incident is purely reactive.	30

Some of the comments made by institutions:

"Third-party assessments and testing are areas of focus and continuous improvement."

"Tests are performed out throughout the year for systems identified as critical. Test scripts are updated annually based on the critical processes identified in each business continuity plan. Lessons learned are recorded after each test and incorporated into future test plans."

"We organize a disaster simulation event every year. The disaster event varies from year to year (...) select events that will impact multiple disaster scenarios (workplace, workforce, IT/technology, supplier) and services."

"Tests have not yet been carried out because resilience deployment is being developed pending standards (...)."

Q300-14 How frequently are you testing your response and recovery capabilities for different disruptive scenarios?

Q300-15 What communication plans and systems (for both internal and external stakeholders) do you have in place to deal with operational disruptions?

Statements	Number of responses
Automated system/call trees and communication plans are in place to contact all staff during an incident, and this is sustained and consistent throughout any disruption. The communication protocol is periodically reviewed and tested to incorporate service providers, partners, customers and lessons learned incorporated.	80
Communication plans include all the relevant information to enable a co-ordinated communication strategy for various communication channels/stakeholders. Plans include predetermined holding lines/templates for communications and are periodically tested for effectiveness and improvements made as part of lessons learned. Plans also include details of external service providers, partners and service recipients to ensure any interdependencies are addressed in a timely manner to minimize disruption.	57
Tools/mechanisms in place to update the contact information on a periodic basis. Call cascades are invoked in a timely manner during an incident. All stakeholder and customer communication is embedded as part of the crisis communication plan and is aligned to an agreed escalation path. Plans also include details of external service providers, partners and service recipients to ensure any interdependencies are addresses in a timely manner to minimize disruptions.	110
There is no formal communication plan in lace to address external stakeholders. As for internal stakeholders, contact information is recorded but not kept up to date and any communication cascade is managed informally.	7

Some of the comments made by institutions:

"The size of the business means it is possible coordinate all stakeholders and remain in contact with senior management and key staff in the organization, enabling it to respond quickly to crisis situations."

"We manage internal communications with our collaborators via a mass communication system, which is regularly used and tested, while business contacts (service providers, third parties, clients) are contacted via established business communication procedures."

Q300-16 How do you seek assurance that an event/operational disruption has been recovered to a satisfactory conclusion and normal service has been resumed?

Statements	Number of responses
Recovery strategy and testing approach in place to cover end to end disaster recovery for business services as well as cover a range of environmental, external, geopolitical scenarios. 3rd parties are included in test scenarios. Root cause analysis is performed on all disruptions with the board and senior management having oversight of any remedial action. Plans are independently reviewed by 3rd line of defence.	38
Resilience is embedded and the recovery strategy aligned to business requirements supported by infrastructure, e.g., frequent and scheduled replication backups on and offsite. Paper copies of plans are kept off site where they can be accessed securely. Effective vendor support process with SLAs are in place and contracts are consistently assessed especially where recovery of business service is solely dependant on 3rd parties. Disaster recovery testing of business services is carried out through severe but plausible scenarios, i.e., firm and 3rd party are tested together.	84
Physical controls and technical infrastructure in place to enable recovery of business services. Recovery process follows set controls which are repeatable and are aligned with policies and plans. If reliant on external support, recovery is limited to the contracts in place. Defined recovery time objectives (RTO) for core applications and overall recovery of business service in place. Data centres are purpose built and adhere to industry standard.	125
There are no formal procedures in place to address recovery to business as usual following an operational disruption. Recovery to business as usual is managed in an ad hoc manner and does not follow set controls, is not aligned with any plans, and does not match agreed SLAs.	7

Some of the comments made by institutions:

"We obtain assurance with a post-event root cause analysis, taking into account significant elements."

"We have never had a major disruption."

"At the enterprise level, the severity of the disruption determines the level of management with which root cause analysis is shared."

"The monitoring of significant incidents/operational disruptions is documented and validated by the business units as part of the post-event assessment process. This is an area of continuous improvement."

Q300-17 Please select the most appropriate approach for your post-incident reviews.

Statements	Number of responses
Post-incident review includes (or makes reference to) vendor post-incident review or incident analysis. Clear and effective lessons learned fed back into relevant areas. Root cause analysis undertaken for all operational outages impacting business services. Board and senior members have oversight of any remedial actions. As part of continuous improvement lessons learned are incorporated in the operational resilience planning documents.	51
A formal post-incident review process is in place. The process defines the steps to be completed during and following an operational disruption. Incident documentation including the ticket data, timelines and root cause analysis is populated for all disruptions during and post-incident. Trend information populated and allows senior management to make informed decisions. Root cause is undertaken and lessons learned is incorporated in test plans for completeness.	91
A formal post-incident review process is in place. The process defines the steps to be completed following an operational disruption. Post-incident review is compiled with information collated after (rather than during) the incident. Actions are agreed and remediated in line with post-incident review. Trend information is populated on an ad hoc basis. Root cause analysis undertaken in an ad hoc manner and where appropriate, test plans are updated to incorporate lessons learned.	82
There is no formal post-incident review policy/process in place. The review is carried out in an informal manner for any operational disruption. Learnings from the incident are updated/ incorporated as part of the test plan.	30

Q300-18 How do you seek assurance and validate the effectiveness of the disaster recovery and continuity plans for business services especially where the services are provided by 3rd party supplier?

Statements	Number of responses
Incident training or war game exercising is carried out on a periodic basis and include all facets of the plan. Exercises include unannounced simulations and cover full spectrum of test types and business services (desktop to end-to-end including external parties etc.). Playbooks are tested internally along with 3rd parties and vendors and independently assured by 3rd line of defence. As for disaster recovery testing, backup and recovery test assess that single points of failure, recovery point objectives are defined and mitigated and if not the risk has been accepted. 3rd parties are fully involved in the planning and end to end testing of important business services.	8
Test plans are aligned to key objectives and risks appetite and these are tested on a periodic basis. Lessons learned are incorporated and addressed as part of the updated documentation for business continuity planning requirements. Regular schedule of exercises include a variety of different types of realistic scenarios (desktop, simulation, etc.). Exercises include a variety of primary and secondary responders. Assurance program includes independent (3rd line of defence) verification and validation of the plans and testing. 3rd parties that support important business services are considered and included in the tests.	57
Formal schedule of exercises to train and rehearse the business continuity plan and crisis management capability exists. Exercising includes conducting desktop reviews to test primary and/or secondary responders. Test plans are linked to business service continuity objectives and risks. Assurance program (1st line of defence) includes verification and validation of the plans and testing. 3rd parties are considered as part of the planning process but not involved in the testing.	131
No formal assurance is undertaken to validate the effectiveness of the disaster recovery and continuity plans for services supported by 3rd parties. Instead, reliance is placed on the 3rd party to provide continued service (in line with the service level agreement) and inform business of any shortcomings. 3rd parties are not included in any exercises or crisis simulation.	58

Q300-19 Have you engaged with critical 3rd parties to understand the potential contagion risk and taken steps to ensure that recovery activities are clearly understood by both parties?

Statements	Number of responses
Recovery arrangements are well defined and embedded across the organization. Planning takes into account the critical 3rd party dependencies and their recovery capabilities. 3rd party supplier are involved in developing test plans/scenarios that take into account systemic and environmental impacts to understand and mitigate any contagion risk for important business services.	17
Recovery arrangements involve detailed scenarios for all critical/important business services informed by past incidents, management information and 3rd party dependencies. Testing is carried out jointly by both parties and includes validation of key dependencies to understand the potential contagion risk.	26
Recovery arrangements are defined by the business and based on identifying the critical/important business services and their dependency on 3rd party service providers. Testing is carried out on an ad hoc basis and is limited to component level test.	183
Recovery arrangements are not determined or are determined in isolation and does not consider 3rd party service provides.	28

Some of the comments made by institutions:

"Some third-party service providers cannot be tested (i.e., Microsoft, Bell, Vidéotron, etc.)."

"Since all the interdependencies of the important business services have not been taken into account, we are currently requiring exit strategies only for the most critical suppliers."

"Suppliers deemed critical are asked to provide their business continuity plan pursuant to the policy at the time of the third-party information security assessment, which is reviewed by our CISO."

Q300-20 How do you intend to use important business service mapping in your testing approach?

Statements	Number of responses
We can demonstrate how we will use the mapping tool to facilitate testing. For example, we will use our mapping to help design severe but plausible scenarios, increase or decrease the severity of the scenarios, etc. Our test planning considers the entire chain of activities that underpin the important business service, leveraged from the mapping data. We can demonstrate how our testing approach will provide appropriate coverage over the resources that support the delivery of the service including third parties that support the delivery of the important business services.	24
We have plans in place to fully consider and test the end-to-end activities that underpin the important business services. The test plans consider and include the activities that underpin the important business services, leveraged from the mapping data. We are considering extending this to include other resources including critical third parties that support the delivery of the important business services.	76
We have a good understanding of the important business services mapping data and plan to include it as part of our overall testing approach. We are developing test plans that will fully consider and test the end-to-end activities that underpin the important business services.	112
Our testing plan does not consider and/or include the important business services mapping data. We have no plans yet in place to address this.	42

Some of the comments made by institutions:

"We use extensive mapping of important business services to help us develop and carry out exercises involving severe but plausible disruption scenarios. We will continue to build on our exercises in order to make them more complex and reflect emerging disruptions."

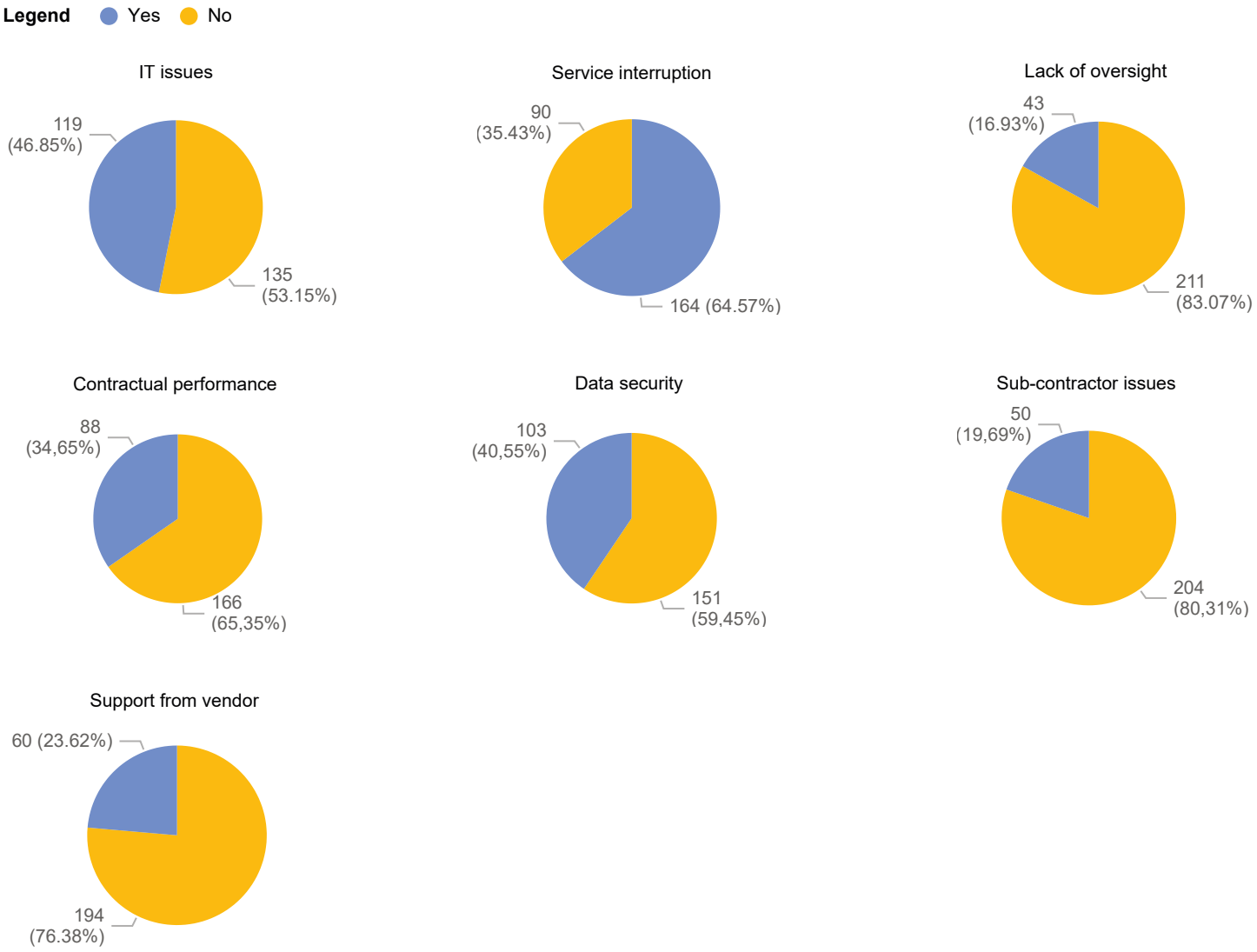
"The operational resilience program has only recently been implemented, and the important business services and associated mappings have not yet been defined."

Q300-21 What type of tests do you intend to use and will they provide sufficient assurance of the effectiveness of your firm's response and recovery capability?

Statements	Number of responses
Our testing plans covers the assurance levels gained from the type of scenarios – testing this may include paper-based assessments (lower assurance), simulations (medium assurance) or live-systems testing (high assurance). Testing of our recovery plans for both availability (e.g., system outages) and integrity scenarios (e.g., data corruption or loss), proportionate to our size and complexity and considers the vulnerabilities, e.g., adoption of new tech/cloud. The testing approach is reviewed and approved by an appropriate governance body to ensure they provide sufficient assurance on the effectiveness of its response and recovery capabilities.	77
Our testing plan is based on and linked to the mapping of our important business services. The mapping data and the underlined activities is updated and signed off by the appropriate governance forums. We have clearly articulated the inclusion of third parties as part of our testing approach.	99
The test data is based on and linked to the mapping of our important business services however, the data is not regularly updated and maintained on an ad hoc manner. We have not considered how third parties are going to be included in scope for testing. The testing approach is not reviewed on a regular basis.	67
We use out of date/inaccurate mapping data for our testing (i.e., not based on important business services mapping) which does not provide any assurance on how important business services are covered.	11

Q300-22 What third-party or outsourcing issues has your financial institution experienced, if any?

Statements	Number of responses
IT issues	119
Service interruption	164
Lack of oversight	43
Contractual performance	88
Data security	103
Sub-contractor issues	50
Support from vendor	60



Q300-23 How do you identify your dependency on services provided by 3rd parties (including intra-affiliates) for the delivery of important business services which could result in customer harm?

Statements	Number of responses
3rd parties and associated dependencies have been identified and mitigation strategies documented to ensure continuity of services across the important business services. The 3rd party register is independently reviewed for example by 3rd line of defence on a periodic basis and issues are escalated as appropriate to senior management and/or the board.	63
3rd parties and associated dependencies have been identified and mitigation strategies documented to ensure continuity of service across the important business services. The 3rd party register includes some 4th parties and is maintained on a periodic basis. Exceptions are escalated to senior management and/or board via appropriate management information. No independent reviews are carried out to validate the list.	33
3rd parties have been identified and categorized based on their criticality to the delivery of the important business services they support. Interdependencies are mapped and documented in a 3rd party register and includes a list of relevant 4th parties. Concentration risk is not fully understood/mapped. The level of engagement is commensurate with the criticality of the supplier.	112
There is no formally documented view of critical 3rd party suppliers. 3rd parties are listed in an ad hoc manner and identified based on their materiality (financial value) and criticality of the services they support.	46

Some of the comments made by institutions:

"The integration of third-party risk management is currently a deficiency that the organization is seeking to address (...)."

"Third-party dependencies are identified in the third-party inventory as well as in impact assessments and continuity plans (...) third parties used for multiple business services are partially identified (...) concentration risk has not been fully assessed."

"The third-party register does not include a list of any fourth parties concerned."

Q300-24 How do you perform due diligence (both operational and financial) over new and existing 3rd party arrangements to assess and manage the risks and vulnerabilities that a 3rd party may introduce to your operating environment?

Statements	Number of responses
The due diligence process and controls have been independently reviewed on a periodic basis and matters of concerns are escalated as appropriate to senior management and/or the board. Exceptions to the 3rd party due diligence are escalated to senior management and/or the board via appropriate management information.	53
Due diligence is periodically performed over new and existing 3rd parties to assess and manage the risks and vulnerabilities that a 3rd party may introduce to the operating environment. Exceptions to the 3rd party due diligence are escalated to senior management and/or the board via appropriate management information. Due diligence covers a range of technology domains as well as consider adequacy of resources and should provide for differing operational risks within arrangements such as sensitive data, cloud service provision bespoke and standard services, concentration and overseas considerations.	66
Due diligence is periodically performed over new and existing 3rd parties to assess and manage the risks and vulnerabilities that a 3rd party may introduce to the operating environment. The due diligence considers the risks associated with the 3rd party's ability to deliver continued service for across the important business services and any potential conflicts of interest and its financial resilience. The rigour of the due diligence process is commensurate to the nature, scale and complexity of the 3rd party arrangement.	128
There is no formal due diligence carried out for new or existing 3rd party suppliers.	7

Q300-25 What is the nature/level of termination rights (the ability to formally end a contract) and how does your exit plan take into account the minimum regulatory obligations?

Statements	Number of responses
Termination rights are documented and validated. Documented evidence of 3rd party exit plans are also maintained, validated and independently reviewed including compliance across regulatory provisions. Exit plans also take into account; a) minimum period to execute a termination provision, b) provisions to facilitate transferability of the services to a bridge-institution or another 3rd party (or equivalent alternative).	63
3rd party exit contracts include termination rights for a breach of the contract. For example, if the counterparty consistently fails to meet the agreed service levels the firm is able to end the arrangement and bring the service in-house or transfer to another 3rd party service provider. Timelines are mutually agreed and acted upon.	142
Termination rights and appropriate exit strategies are not fully developed for all critical 3rd party service arrangements. Exit plans are under development and will be included as part of the contractual agreement.	40
No formal exit plans exist. 3rd party relationships are managed on a mutual agreement and not enforceable by law.	9

Some of the comments made by institutions:

"Formal exit strategies are developed, approved by senior management and reviewed periodically for all important/critical third parties."

"Critical suppliers have more robust termination provisions and a more in-depth analysis of exit strategies/scenarios."

Q300-26 Do you know the services provided by third parties and their suppliers?

Statements	Number of responses
An accurate register is maintained of all services provided by 3rd parties. Processes and procedures are in place to ensure that new 3rd parties and/or changes in existing services are captured within the register. The list is validated on a periodic basis and independently reviewed by 3rd line of defence.	49
A register is maintained of all critical 3rd party providers and the services they provide. Concentration risk across all critical suppliers has been identified and mitigation strategies documented. The level of engagement is commensurate with the criticality of the supplier. Processes and procedures are in place to ensure that new critical 3rd parties and/or changes existing services provided are captured within the register.	120
A list is held of critical 3rd party providers and the services they provide and maintained on an ad hoc basis. Concentration risk across all critical suppliers is not fully understood and in the process of being mapped.	72
There is no centrally held list of 3rd party providers and services. Business units are responsible to manage the individual relationships. Concentration risk is not considered.	13

Q300-27 Do you have effective processes and procedures in place to assess the operational resilience risks and capabilities of your 3rd party service providers?

Statements	Number of responses
3rd party providers and their service provision are risk assessed in line with their potential impact upon the delivery of a firm's important business services and incorporated in any scenario testing/exercising. Relevant management information is shared with the board to help make informed decisions and any findings are recorded and acted upon.	71
Operational resilience risks across all critical 3rd party providers are reviewed in line with policy but on an ad hoc basis.	129
All critical 3rd party are reviewed only once, at the on-boarding stage and in line with the risks they represent. Findings are recorded. No further reviews are carried out throughout the life cycle.	38
No assessment of 3rd party providers is undertaken specifically in relation to risks they represent.	16

Toll-free: 1-877-525-0337
lautorite.qc.ca

Québec City
418-525-0337
Place de la Cité, tour PwC
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

Montréal
514-395-0337
800, rue du Square-Victoria, bureau 2200
Montréal (Québec) H3C 0B4