TC NOTES

PRACTICAL **LEADERSHIP**
AND **GUIDANCE** FROM
TORONTO CENTRE

OPERATIONAL RESILIENCE: THE NEXT FRONTIER FOR SUPERVISORS?

APRIL 2021

TORONTOCENTRE
Global Leadership in Financial Supervision

OPERATIONAL RESILIENCE: THE NEXT FRONTIER FOR SUPERVISORS?

TABLE OF CONTENTS

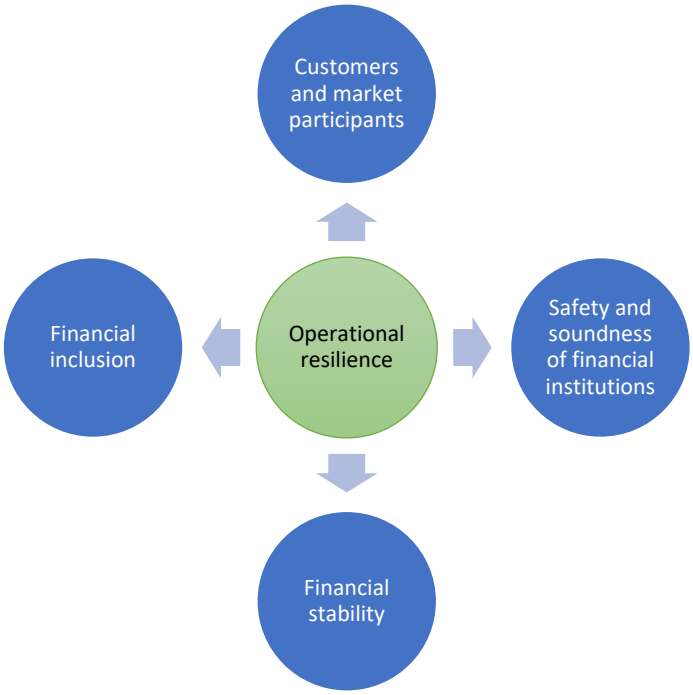
OPERATIONAL RESILIENCE: THE NEXT FRONTIER FOR SUPERVISORS?

Introduction[1]

Operational resilience can be described as an outcome in which the continuity of the key business services provided by supervised financial institutions is preserved (or is restored rapidly and effectively when operational disruptions occur). To deliver this outcome, financial institutions need to put in place measures not only to prevent operational failures from occurring, but also to respond, recover, and communicate effectively and quickly if and when such failures do occur.

Operational disruptions to the products and services provided by financial institutions have the potential to threaten the viability of financial institutions, to cause harm to consumers and market participants, to reduce financial inclusion, and to cause financial instability. Operational resilience is therefore relevant for financial institutions and supervisors across all sectors (including financial market infrastructures, such as payment systems and stock exchanges) and across prudential, conduct, financial stability, and financial inclusion objectives.

Figure 1: The importance of operational resilience



[1] This Note was prepared by Clive Briault with helpful input from Phang Hong Lim and Paul Wright.

Two key features of operational resilience are that first, some of the costs of a lack of operational resilience fall as externalities on users of financial products, on financial stability, and on financial inclusion; and second, its focus is on not only preventing operational disruptions from occurring but also on how quickly a financial institution can recover and restore the key financial services it provides. The ability to recover quickly is crucial to building trust in the financial sector.

Supervisors have focused for many years on areas such as operational risk (including various types of technology risk and cyber security), outsourcing, and business continuity planning (BCP). The growth in the use of technology and data by financial institutions, and more recently the COVID-19 pandemic, has increased supervisory intensity in many of these areas.[2]

However, this supervisory focus has often been somewhat piecemeal, jumping between areas of risk in response to events and imposing different requirements on closely related aspects of how financial institutions undertake their business. Some supervisors have therefore begun to develop an overarching framework here, to provide a more consistent, proportionate, and risk-based approach to the operational resilience of supervised firms.

This Toronto Centre Note:

- outlines the definition of operational resilience;
- explains why operational resilience is important for supervisors;
- describes how some supervisors are beginning to take a more overarching approach to operational resilience;
- shows how supervisors can assess a financial institution's operational resilience as part of their supervision; and
- discusses how operational resilience fits within a risk-based supervisory approach.

What is operational resilience?

Definitions

In the corporate world, operational resilience is usually defined as the ability of a firm to change or adapt during times of stress, disruption, or uncertainty. The focus here is mostly on operational disruptions, but it is possible to extend this to the ability of firms to change their strategies, organizational structures, and business models where and when necessary to preserve their viability.

Financial supervisors that have focused on operational resilience have emphasized the impact of operational disruptions on the ability of a financial institution to maintain the delivery of its key business services, which is a crucial component in the smooth functioning of the financial sector.[3]

[2] Toronto Centre (2020e).
[3] See, for example, Bank of England et al. (2018), Basel Committee (2021a), and Board of Governors of the Federal Reserve System et al. (2020).

> "The ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimize their impact on the delivery of critical operations through disruption." – Basel Committee (2021a)

> "The ability of firms and financial market infrastructures and the financial sector as a whole to prevent, adapt, respond to, recover from, and learn from operational disruptions." – Bank of England et al. (2018)

> "The ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard." – Board of Governors of the Federal Reserve System et al. (2020)

Implications

These definitions imply that operational resilience:

- Is applicable to all types of financial institutions in all sectors, although the principle of proportionality should apply here – the likelihood of operational disruptions occurring and the costs of business discontinuity (to both financial institutions themselves and to others) are higher in some financial institutions than in others.
- Is not only about preventing (minimizing the probability of) various types of operational failure from occurring, but also about adapting systems and processes to continue to provide services and functions in the event of an incident; returning to normal operations promptly when the disruption is over; communicating to stakeholders; and learning and evolving from operational disruptions and near misses.
- Does not have to involve any financial loss to the financial institution itself (so is different from operational risk, which is usually defined as the risk of loss arising from inadequate or failed internal processes, people, and systems, or from external events).
- Should focus on the end outcome of maintaining or restoring key financial services, not just on individual systems or processes.
- Should extend beyond the often rather limited focus of business continuity planning and disaster recovery, because financial institutions should have plans in place to deliver key services, no matter what the cause of the disruption. This includes human-made threats such as physical and cyber attacks, IT system outages and third-party supplier failure, and natural hazards such as fire, flood, severe weather, and pandemics.

Why should supervisors care about operational resilience?

Operational resilience protects a financial institution itself, its customers, other market participants, financial stability, and financial inclusion. The risks from inadequate operational resilience – in terms of both the incidence of operational disruptions and a delayed or otherwise inadequate response to, and recovery from, such disruptions – could arise in any type of financial institution, and in any financial system.

Financial institutions – the disruption of a financial institution's business services could cause financial losses or reputational damage to that financial institution. Financial losses could arise from operational disruptions that prevent a financial institution from taking deposits or other funding, collecting premiums, receiving funds to manage, extending credit, writing insurance, executing trades, accessing customer data, hedging its positions, or collecting margin payments. Reputational damage could arise from disruptions that prevent a financial institution from making payments (deposit withdrawals, insurance claims, fund redemptions, etc.), fulfilling customer orders, transferring funds between accounts, marking positions to market, providing investors with real time valuations, meeting other contractual obligations, or accepting new business. Substantial disruptions that are not resolved quickly could threaten the viability of a financial institution.

In addition, inadequate operational resilience could hinder the ability of financial institutions to meet regulatory and supervisory requirements, for example with respect to prudential, conduct, and anti-money laundering and countering terrorist financing requirements; timely and accurate reporting; and data confidentiality.

Harm to consumers – customers and counterparties of financial institutions depend on the continuity and predictability of financial services. The disruption of a financial institution's business services could harm existing or potential new customers, who may be unable to access existing business services or unable to access new products and services. Examples of customer access to existing business services include the ability to access their deposits, savings, and investments; check account balances or make a money transfer; claim on an insurance contract; trade investments; receive accurate and timely valuations of their investments; or make an inquiry or complaint. Examples of consumers wanting to access new services and products include the ability to open a bank account or receive a loan; renew or take out a new insurance contract; invest in a managed fund or open a trading account; or take financial advice.

Harm to market participants and market integrity – the disruption of a financial institution's business services could harm market participants and market integrity, for example as a result of a financial market infrastructure (such as a national stock exchange, or a major wholesale or retail payment system) failing to operate, an inability to access market data to price trades, an inability to complete post-sale activity, or the unintended disclosure and misuse of market-sensitive information.

Financial stability – financial stability could be threatened by operational disruptions that caused the failure of a large financial institution or financial market infrastructure, of a large

number of smaller financial institutions (for example as a result of a cyber attack), or of critical outsource providers (for example those providing services such as cloud computing[4]).

Financial inclusion – inadequate operational resilience could have a negative impact on financial inclusion, because operational disruptions may prevent access to financial services and products, and may generate wider concerns or uncertainty about the reliability of financial institutions and of the financial system.

Not all supervisory authorities will be equally concerned about these five types of risk. This will depend on which of these risks pose a risk to the objectives of a supervisory authority. For example, a prudential supervisor with only a safety-and-soundness objective would focus primarily on the financial risks facing the institutions it supervises. This will include operational risk because that is defined to be the risk of loss arising from events such as the inadequacy or failure of internal systems and processes.[5] But in practice, many prudential supervisors also have a financial stability objective,[6] which includes some focus on the continuity of important financial services. A supervisor of financial market infrastructure is also very likely to have a financial stability objective, and in some cases a specific objective to preserve the continuity of services provided by financial market infrastructures.

Meanwhile, and in particular in many emerging markets and developing countries, some supervisory authorities have objectives to enhance financial inclusion. And the consumer (or investor) protection objectives of retail and wholesale conduct supervisors should include the harm to consumers and investors arising from disruptions to financial services.

Contributors to operational resilience

There are many examples of international standard setters and national supervisory authorities focusing on individual elements of operational resilience. These include the long-standing presence of operational risk within regulatory and supervisory frameworks,[7] and – either within or alongside operational risk – more recent regulatory and supervisory initiatives in areas such as information technology and communications, cyber security,[8] outsourcing,[9] and data protection. Meanwhile, disaster recovery and business continuity planning have increased in prominence as a result of the COVID-19 pandemic.[10]

[4] Toronto Centre (2020f) discusses the risks arising from cloud computing outsourcing, the concentration of providers in this area, and the difficulties in finding substitute providers or taking the service back in-house when problems arise.
[5] For example, Basel Committee (2011) defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.
[6] Revisions to the Basel Core Principles (2012) following the global financial crisis emphasize that the objectives of banking supervisory authorities should include the safety and soundness of the banking system, not just of individual banks, and that supervisors should consider the systemic importance of each bank. Similarly, the IAIS Core Principles (2019) recommend that insurance supervisors should identify and address the build-up and transmission of systemic risk at both the individual insurer and the sector-wide level.
[7] See, for example, Basel Committee (2021b), International Association of Insurance Supervisors (2019), and International Organization of Securities Commissions (1998).
[8] Toronto Centre (2018b).
[9] See, for example, International Association of Insurance Supervisors (2019), and International Organization of Securities Commissions (2020).
[10] Toronto Centre (2020b and 2020e).

This topic-by-topic approach may reflect a supervisory emphasis on:

- where significant operational disruptions have occurred in practice (for example, successful cyber attacks, failures of ATM systems, failures in platforms for internet- or mobile-based provision of financial services and products, and problems with outsourcing);
- where financial institutions have not responded effectively to operational disruptions (for example, delays in restoring services and poor communication with customers and supervisors); and
- where supervisors believe that problems might arise, not least because of the impact of the increasing use of technology, data, and data analytics.

Figure 2: Some contributors to operational resilience

However, this approach does not embrace the totality of operational resilience. It may not focus sufficiently on:

- response and recovery,[11] not just prevention;[12]
- the risk of harm to consumers, market participants, financial stability, and financial inclusion, not just the risk of loss to individual financial institutions;
- a wide range of potential disruptions, not just the loss of buildings or IT systems typically covered in disaster recovery plans; and
- the end objective of the continuity of key business services, not just avoiding disruptions to specific systems and processes.

[11] There is a similarity here with recovery planning, although that focuses more on taking recovery actions to restore financial resilience. See Toronto Centre (2020d).
[12] The supervisory approach to cyber security – with its focus on preparedness, risk identification, protection, detection, and incident response – comes closest to the end-to-end scope of operational resilience, but is not always linked sufficiently closely to preserving the continuity of key business services.

Taking an overarching approach to operational resilience

Some national supervisory authorities and the Basel Committee on Banking Supervision have established frameworks for operational resilience.

Basel Committee

The Basel Committee (2021a) has set out seven principles (see Box 1) that banks should meet to achieve operational resilience.

Box 1: Basel Committee principles for operational resilience

1. **Governance**: Banks should utilize their existing governance structure to establish, oversee, and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimize their impact on delivering critical operations through disruption.

2. **Operational risk management**: Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes, and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations, and manage the resulting risks in accordance with their operational resilience approach.

3. **Business continuity planning and testing**: Banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios to test their ability to deliver critical operations through disruption.

4. **Mapping interconnections and interdependencies**: Once a bank has identified its critical operations, the bank should map the relevant internal and external interconnections and interdependencies to set operational resilience expectations that are necessary for the delivery of critical operations, consistent with its approach to operational resilience.

5. **Third-party dependency management**: Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intra-group entities, for the delivery of critical operations.

6. **Incident management**: Banks should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with the bank's risk tolerance for disruption. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.

7. **ICT including cyber security**: Banks should ensure resilient Information and Communication Technology (ICT) including cyber security that is subject to protection, detection, response, and recovery programs that are regularly tested, incorporate appropriate situational awareness, and convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the bank's critical operations.

Source: Basel Committee (2021a).

Consistent with the discussion in the previous section, the principles draw in part from previously issued principles on corporate governance (principle 1), operational risk management (principle 2), business continuity planning (principle 3), outsourcing (principle 5), and cyber (and wider IT) security (principle 7).

However, these principles go further than previous Basel Committee standards in emphasizing:

- the importance of delivering key business services during disruptions, not simply restoring systems and processes (principles 3 and 6);
- the importance of incident response (including recovery and communications), continuous learning, and adaptation (principle 6);
- the need for firms to identify the systems and processes on which their key business services depend (principle 4); and
- the role of corporate governance in establishing and overseeing an effective approach to operational resilience (principle 1).

The Basel Committee is taking a pragmatic, principles-based approach to operational resilience that will help to ensure proportional implementation across banks of various size, complexity, and geographical location. Although these principles are directed at banks, they are equally applicable to any other type of financial institution. All supervisors can therefore build on these principles.

The Basel Committee states that banks need to undertake further work to strengthen their ability to respond effectively to operational disruptions (such as pandemics, cyber incidents, technology failures, or natural disasters) that could cause significant operational failures or wide-scale disruptions in financial markets.

United Kingdom

In the UK, the Bank of England, Prudential Regulatory Authority, and Financial Conduct Authority (2018) issued a joint Discussion Paper on operational resilience, highlighting its relevance for all financial institutions (including financial market infrastructures) across all sectors, for both prudential and conduct supervisors, and for financial stability. The UK authorities stressed that the operational resilience of financial institutions is a priority for the supervisory authorities and is viewed as being as important as financial resilience. Final rules and guidance were issued in 2021.[13]

As with the Basel Committee's principles, the UK authorities emphasize that financial institutions – and the financial system as a whole – need to be able to absorb shocks rather than contribute to them, and therefore need an approach to operational resilience that includes not only preventative measures but also the capabilities to adapt and recover when operational disruptions occur. The speed and effectiveness of communications with the people most affected, including customers, is an important part of any financial institution's overall response to an operational disruption.

[13] See Bank of England (2021), Financial Conduct Authority (2021), and Prudential Regulation Authority (2021).

For firms to be operationally resilient, they should be able to:

- prevent disruption occurring to the extent practicable;
- adapt systems and processes to continue to provide services and functions in the event of an incident;
- return to normal running promptly when a disruption is over; and
- learn and evolve from both incidents and near misses.

Prudential Regulation Authority (2021).

The UK authorities also stress the importance of financial institutions setting impact tolerances, to quantify the amount of disruption that could be tolerated in the event of an operational disruption.[14] This is seen as an important element of how boards and senior management should set their own standards for operational resilience, and use these to prioritize and take investment decisions (including upgrading IT, and investing in people and systems). Tolerances could be expressed in terms of the maximum duration that a key business service was unavailable for;[15] the number of customers affected by an operational disruption; and levels of data security and integrity. These impact tolerances are different from the more typical risk appetite or tolerance statements of financial institutions, which tend to focus only on the financial losses that a financial institution is prepared to accept.

In setting impact tolerances, a financial institution's board or senior management should prioritize those business services that, if disrupted, have the potential to threaten the firm's viability; cause harm to consumers and market participants; or undermine financial stability. Financial institutions should also test their ability to stay within their impact tolerances in severe but plausible scenarios, and to take mitigating action if this indicates that impact tolerances might not be achievable.

Box 2: What should an operationally resilient financial institution have in place?

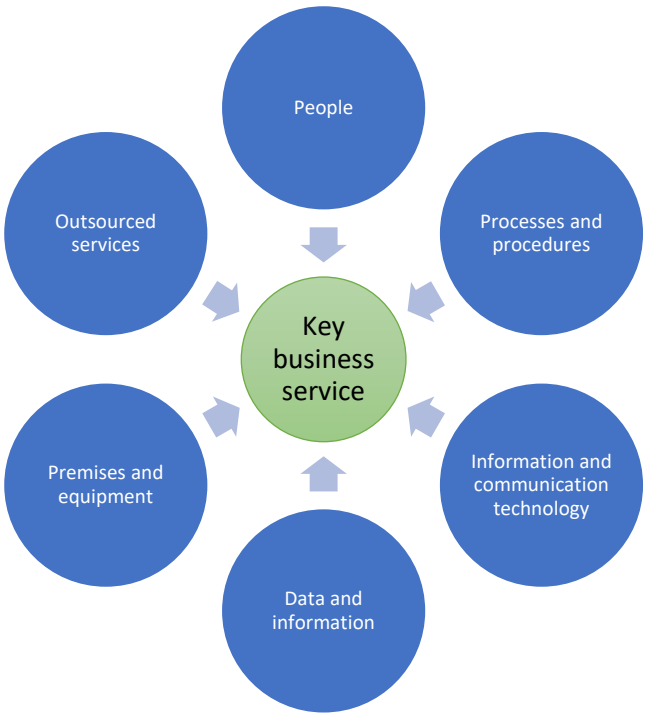
- A clear understanding of its most important business service or services.
- A comprehensive understanding and mapping of the systems and processes that support these business services, including those over which the financial institution may not have direct control (see Figure 3). This would include an understanding of the resilience of outsourced providers or entities within the same group but in another jurisdiction.
- Knowledge of how the failure of an individual system or process could have an impact on the provision of one or more key business services.
- Knowledge of which systems and processes are capable of being substituted during disruption so that business services can continue to be delivered.
- Tested plans that would enable a financial institution to continue or resume business services when disruptions occur.
- Effective internal communication plans, escalation paths, and identified decision makers.
- Specific external communication plans for the most important business services, which provide timely information for customers, other market participants, and the supervisory authorities.

Bank of England et al. (2018)

[14] Bank of England et al. (2019).

[15] For example, Committee on Payments Systems and Market Infrastructures and International Organization of Securities Commissions Principle 17 (consideration 12) for financial market infrastructures (2012) states that a financial market infrastructure should design and test its systems and processes to aim for the safe resumption of critical operations within two hours of an operational disruption.

Figure 3: Mapping key business services to the systems and processes on which they depend



United States

In the US, banking supervisors have issued a set of sound practices to strengthen operational resilience.[16] These sound practices are applicable to larger and more complex banks, and are similar to those established by the Basel Committee. They cover:

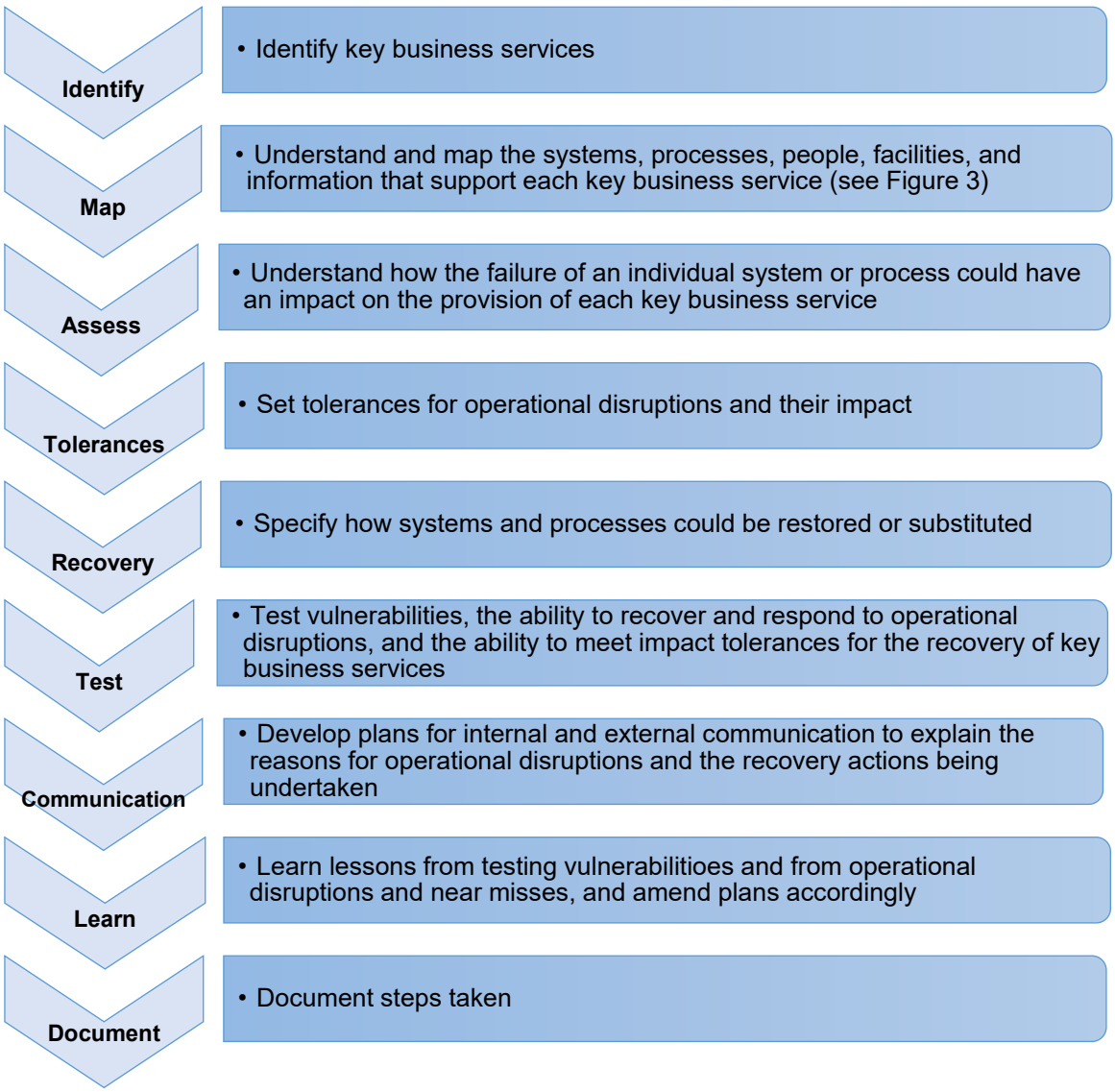
- governance;
- operational risk management;
- business continuity management;
- third-party risk management;
- scenario analysis – to help a firm to develop, validate, and calibrate its tolerance for disruption;
- secure and resilient information systems management; and
- surveillance and internal reporting.

[16] Board of Governors of the Federal Reserve System et al. (2020).

Supervisory assessment

Supervisors wanting to focus on operational resilience should check that financial institutions have taken the necessary steps to embed operational resilience (see Figure 4). This should be proportionate to the size and importance of each financial institution – large financial institutions on which many customers or market participants depend, and those capable of creating systemic or wider financial instability, should be expected to take a more thorough and robust approach to embedding operational resilience than smaller financial institutions.[17]

Figure 4: Steps a financial institution should take to embed operational resilience



[17] This is consistent with the more general supervisory approach to systemically important financial institutions since the global financial crisis, with a greater focus on more intensive supervision, on financial resilience (capital surcharges and recovery planning), and on expecting larger and more complex financial institutions to adhere to higher standards of risk management.

This supervisory assessment could begin with a stock-take of what the supervisor already knows about a financial institution's operational resilience from whatever supervisory work has already been undertaken in areas that contribute to operational resilience (see Figure 2), such as operational risk management, business continuity planning, outsourcing, and cyber security. The supervisor may also have some knowledge of operational disruptions that have occurred at the financial institution – or at comparable financial institutions – and their impact on the key business services provided by the financial institution.

The next step could be for the supervisor to request and review documentation from a financial institution on its approach to operational resilience and the steps it has already taken to embed and test operational resilience. The supervisor could ask for documentation relating to each of the steps outlined in Figure 4, and then review this in much the same way as a supervisor reviews and evaluates a bank's individual capital adequacy assessment (ICAAP), an insurer's own risk and solvency assessment (ORSA), or a major financial institution's recovery plan.

In addition to this off-site review of documentation, a supervisor can use on-site supervision (if necessary, virtually through telephone or video conferencing) to interview board members (including non-executive directors), senior management, business heads, risk management heads and others, and to review relevant files, to check that the processes, procedures, and systems described in documentation are in place, followed in practice, and effective.

Roles and responsibilities of the board and senior management

Boards and senior management should focus on the operational resilience of key business services, because this is a key issue for financial institutions. Indeed, the strength of a financial institution's operational resilience will depend on its governance, culture, controls, and its ability to respond effectively to operational disruptions.

Supervisors should therefore be able to explore a range of issues with board members and senior management, some of which are set out in Box 3.[18] The intention here would be to establish the extent to which the board has a clear view of the operational resilience of a financial institution and is driving improvements, as necessary.

[18] Boxes 3-6 are designed to be illustrative rather than comprehensive. They are intended to provide a starting point for a supervisory review and evaluation of operational resilience in any financial institution across all sectors, through a list of suggested open-ended questions for discussion with a financial institution, not a standardized checklist. This review and evaluation should of course be proportionate to the size and importance of the financial institution – smaller financial institutions might only be covered on a sample or thematic basis, as discussed in Toronto Centre (2020a and 2020c).

Box 3: Questions supervisors should be asking when assessing operational resilience: Corporate governance

Board involvement in operational resilience

- What discussions of operational resilience have taken place at the board?
- What expertise and experience do board members and senior management have in operational resilience?
- Who is responsible and accountable for operational resilience?
- Is the board clear about the key business services of the financial institution, and the people, processes, and systems that support these services?
- Has the board discussed not only how operational disruptions can be prevented, but also how the financial institution would respond if such disruptions did occur?
- Has the board set impact tolerances for disruption to key business services, based on a broad range of severe but plausible scenarios?
- What reports does the board receive on operational resilience, including on how the extent of the financial institution's operational resilience is measured and tested?

Assurance

- How strong and robust is the financial institution's operational resilience?
- How does the board gain assurance that the financial institution has embedded operational resilience?
- What does the board know about the systems, controls, policies, and procedures intended to deliver operational resilience?
- How is operational resilience covered in the internal audit program?
- Which operational disruptions and near misses are reported to the board?
- How does the board encourage a culture of learning and making improvements to operational resilience?

Prevention

The first part of operational resilience is to reduce the probability of an operational disruption occurring, in particular disruptions that could have a significant adverse impact on the ability of a financial institution to provide key business services. This is where many financial institutions (and their supervisors) have probably devoted most of their efforts in the past, so reasonably good progress should already have been made here. However, looking at this again through the lens of operational resilience may reveal some areas where further progress needs to be made. For example, good operational risk management alone may not be sufficient to deliver even the prevention part of operational resilience.

Some avenues of supervisory review and evaluation in this area are set out in Box 4. These questions might be addressed to a wide range of people at a financial institution, including board members, senior management, heads of business and risk management functions, specialist staff in areas such as IT and outsourcing, and internal audit.

Box 4: Questions supervisors should be asking when assessing operational resilience: Prevention

First steps

- Has the financial institution identified its key business services?
- Has the financial institution mapped the systems, processes, people, facilities, and information that support each key business service, including those dependent upon third parties or intra-group arrangements?
- Does the financial institution understand how the failure of an individual system or process could have an impact on the provision of each key business service?
- Where are these first steps documented?
- Is there evidence that all relevant people and departments within the financial institution have a shared common understanding of key business services and their interdependencies with systems and processes?

Risk management

- How does senior management implement the financial institution's approach to operational resilience?
- Is there a clear focus on key business services and end outcomes for customers and market participants, not just on individual systems and processes within the financial institution?
- How do the three lines of defence (front line, risk management, and internal audit) approach operational resilience?
- What controls and procedures are in place to identify threats and vulnerabilities in a timely manner and, to the extent possible, to prevent these threats from affecting key business services?
- Are these controls and procedures properly documented? This should include governance and oversight requirements, risk ownership and accountability, security measures, and the periodic evaluation and monitoring of controls.
- Do the relevant functions assess regularly the effectiveness of the implemented controls and procedures?
- Is the allocation of people, financial, technical, and other resources sufficient to support the financial institution's delivery of operational resilience?
- Do staff have the necessary expertise, experience, and training?
- How does the operational risk management function work alongside other relevant functions (for example, business continuity planning, third-party dependency management, and recovery planning) to manage and address any risks that threaten the delivery of key business services?

Recovery, response, and communication

Financial institutions should assume that operational disruptions will occur and should plan accordingly for when such events do occur. One useful perspective here – for both financial institutions and their supervisors – is to view this as the operational equivalent to recovery planning against financial shocks and disruptions.[19] Many of the core considerations central to recovery planning for financial shocks – governance, planning, matching recovery options to potential incidents, communications, etc. – are equally relevant to planning for the recovery and response to operational disruptions. Similarly, it is important for financial institutions to consider a range of possible recovery options for operational disruptions. For example, in addition to

[19] Toronto Centre (2020d) sets out how a supervisor can assess a recovery plan.

repairing a failed system or process, a financial institution might consider operating a backup for core or essential services, moving functions to a different geographical location, bringing outsourced functions back in-house, or buying a substitute system.

Again, some avenues of supervisory review and evaluation in this area are set out in Box 5.

Box 5: Questions supervisors should be asking when assessing operational resilience: Recovery, response, and communication

Recovery and response

- Has the financial institution identified a full range of recovery options that would enable key business services to be maintained, or restored within impact tolerances, in the event of operational disruptions?
- What processes and procedures are in place to identify that a disruptive event (or a near miss) has occurred?
- What governance and decision-making procedures are in place to initiate responses to an operational disruption?
- Do contractual agreements with third parties and intra-group entities cover how to maintain operational resilience in both normal circumstances and in the event of disruption?
- How would the financial institution decide between restoring a process (for example, trying to fix an IT fault), adapting a process (for example, switching to a backup system), or substituting a process (for example, switching an outsourced service back in-house) in order to recover a key business service within impact tolerances?
- How are the impact tolerances set by the board monitored and tested?
- What severe but plausible scenarios are used for the testing of whether the financial institution is likely to be able to remain within its impact tolerances?
- Are incident response and recovery procedures periodically reviewed, tested, and updated?

Communication

- What plans are in place for internal communication in the event of operational disruptions, so staff know what has occurred and how the financial institution is responding to these disruptions?
- What plans are in place for external communication?
- Have all relevant stakeholders been identified?
- Where operational disruptions cause problems in key business services for retail customers, how would the financial institution communicate effectively and rapidly to a potentially large number of customers to explain the problem and keep them informed of developments? For example, how would it communicate when its own website or mobile applications are out of service?

Learning lessons and implementing changes

Operational disruptions, near misses, and restoring key business services will all provide financial institutions (and their supervisors) with important lessons about what can go wrong, and about what went well (or less well) in responding to operational disruptions. Financial institutions should therefore ensure that they learn lessons from such experiences, and where necessary and practicable make improvements accordingly. Supervisors should also consider

whether some lessons could usefully be shared across financial institutions so they can all learn and make improvements.

Box 6: Questions supervisors should be asking when assessing operational resilience: Learning lessons and implementing changes

- Does the financial institution have a culture of learning lessons and making improvements?
- What lessons has the financial institution learned from previous operational disruptions (including disruptions suffered by other financial institutions) and near misses?
- How have these lessons been used to reduce the probability of an operational disruption occurring?
- Have root causes been identified and eliminated to prevent the serial recurrence of operational disruptions or near misses?
- What changes have been made to improve the response to future disruptions?

Risk-based supervision

A supervisory emphasis on operational resilience will require some adjustment to the focus of supervision, and more intensive supervision for some financial institutions (and, with constrained supervisory resources, a corresponding shift of resources away from other supervisory activities). It is important that any such shift in the use of supervisory resources reflects the various risks to the mandate and objectives of a supervisory authority.

For supervisory authorities using a risk-based approach to supervision, consideration of a financial institution's operational resilience and its systemic impact on the financial sector should be captured as part of the risk-based supervisory framework. This can help to ensure that the supervisory authority takes a proportional approach, based on impact – the impact that business service discontinuity in a financial institution would have on supervisory objectives[20] – and the likelihood that such discontinuity might occur.[21]

In practice, and using as a starting point the generic risk matrix illustrated in Toronto Centre (2018a), a financial institution's key business services should be captured as significant activities in the rows of the risk matrix. A supervisory authority wanting to assess the operational resilience of a key business service might then add operational resilience as an inherent risk in the matrix, to capture its assessment of how inherently vulnerable each key business service might be to operational disruption. In assessing this inherent risk, a supervisor should consider not only the potential financial losses for the financial institution itself[22] from operational disruptions but also the externalities that may cause harm to consumers, market participants, financial inclusion, and financial stability.

This assessment should enable a supervisor to compare the operational resilience inherent risk against other inherent risks (for example, credit, market, insurance underwriting, conduct, money laundering) – if, for example, the financial institution is judged to be relatively vulnerable in the area of operational resilience (and is assigned a relatively high rating for inherent risk)

[20] As discussed above, this will depend on the mandate and objectives of each supervisory authority – prudential, conduct, financial inclusion, and financial stability.
[21] Toronto Centre (2018a) describes this risk-based approach.
[22] This column might therefore encapsulate operational risk as a sub-element of this column, thereby covering both the financial and the operational risks inherent in the operation of each significant activity.

while other inherent risks (such as credit or insurance underwriting) are judged to be relatively lower, that would increase the focus on the governance and controls relating to operational resilience.

Then, under the governance and controls part of the matrix, a supervisory authority could add an additional column to capture the governance and controls that would need to be in place both to reduce the likelihood of operational disruptions occurring and – importantly – to respond, recover, and communicate effectively if and when such disruptions did occur. Alternatively, this could be captured under the existing columns of the generic risk matrix (board, senior management, risk management, and internal audit), provided that supervisors are properly trained to assess both the prevention and the incident management response elements of mitigating operational disruptions, and that supervisors are able to adequately distinguish and give weight to all areas of governance and controls in the overall assessment, including those relating to operational resilience.

The net risks to supervisory objectives (the inherent risks and the extent to which these are mitigated by governance and controls) from operational resilience are likely to be greatest – and to require the allocation of supervisory resources and supervisory intervention – where impact and likelihood ratings are high, and controls ratings are weak. This would be the case where, for example, (a) a financial institution provides one or more business services where the impact of operational disruptions could be large (for example, a financial institution providing a retail payment system for a large number of customers, or a financial market infrastructure providing large-scale trading, payment, settlement, or custody services); (b) these business services are prone to operational disruption (for example, because they depend on IT-based systems and processes); and (c) governance and controls to prevent operational disruptions or to manage incidents when they occur are weak.

Conclusions

Operational resilience is important for financial institutions (including financial market infrastructure, such as payment systems and stock exchanges) and their supervisors because operational disruptions to the products and services provided by financial institutions have the potential to threaten the viability of financial institutions, and to harm consumers, market participants, financial inclusion, and financial stability.

Key considerations here include the focus on the continuity and recovery of key business services provided by financial institutions (not just on systems and processes), and the focus not just on preventing operational disruptions but also on the strength of the incident management capabilities that enable financial institutions to respond, recover, and communicate effectively when disruptions do occur.

To some extent, supervisors – and financial institutions – will already be looking at some elements of operational resilience through their work on business continuity, IT and cyber security risks, outsourcing, and systems and processes. However, this may be being undertaken in a somewhat piecemeal manner.

There is value in supervisors taking a more overarching approach to operational resilience, and in requiring or encouraging financial institutions to do the same. Supervisors have considerable scope to pursue this further, but should do so within a risk-based approach so that the allocation of supervisory resources reflects the risks that failures in operational resilience may pose to their mandate and objectives.

References

Bank of England, Prudential Regulation Authority, and Financial Conduct Authority. *Building the UK financial sector's operational resilience*. Discussion Paper. July 2018.

Bank of England, Prudential Regulation Authority, and Financial Conduct Authority. *Building operational resilience: Impact tolerances for important business services*. December 2019.

Bank of England. *Bank of England policy on Operational Resilience of FMIs*. March 2021.

Basel Committee on Banking Supervision. *Principles for the Sound Management of Operational Risk*. June 2011.

Basel Committee on Banking Supervision. *Core Principles for Effective Banking Supervision*. September 2012.

Basel Committee on Banking Supervision. *Principles for operational resilience*. March 2021a.

Basel Committee on Banking Supervision. *Revisions to the principles for the sound management of operational risk*. March 2021b.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency. *Sound Practices to Strengthen Operational Resilience*. October 2020.

Committee on Payments Systems and Market Infrastructures and International Organization of Securities Commissions. *Principles for financial market infrastructures*. April 2012.

Financial Conduct Authority. *Building operational resilience: Feedback to CP19/32 and final rules*. March 2021.

International Association of Insurance Supervisors. *Insurance Core Principles*. November 2019.

International Organization of Securities Commissions. *Risk Management and Control Guidance for Securities Firms and their Supervisors*. May 1998.

International Organization of Securities Commissions. *Principles on Outsourcing*. Consultation Report. May 2020.

Prudential Regulation Authority. *Operational resilience: Impact tolerances for important business services*. March 2021.

Toronto Centre. *Risk-Based Supervision*. March 2018a.

Toronto Centre. *Supervision of Cyber Risk.* September 2018b.

Toronto Centre. *Risk-Based Supervision for Securities Supervisors (and Other Supervisors of Small Firms).* February 2020a.

Toronto Centre. *Business Continuity Planning for a Supervisory Authority.* April 2020b.

Toronto Centre. *Supervising Corporate Governance During Crises*. April 2020c.

Toronto Centre. *Recovery Planning.* August 2020d.

Toronto Centre. *Guide to Supervision in the COVID-19 World.* September 2020e.

Toronto Centre. *Cloud Computing: Issues for Supervisors.* November 2020f.