GIBRALTAR FINANCIAL SERVICES COMMISSION

GFSC Guidance Note

Operational Resilience

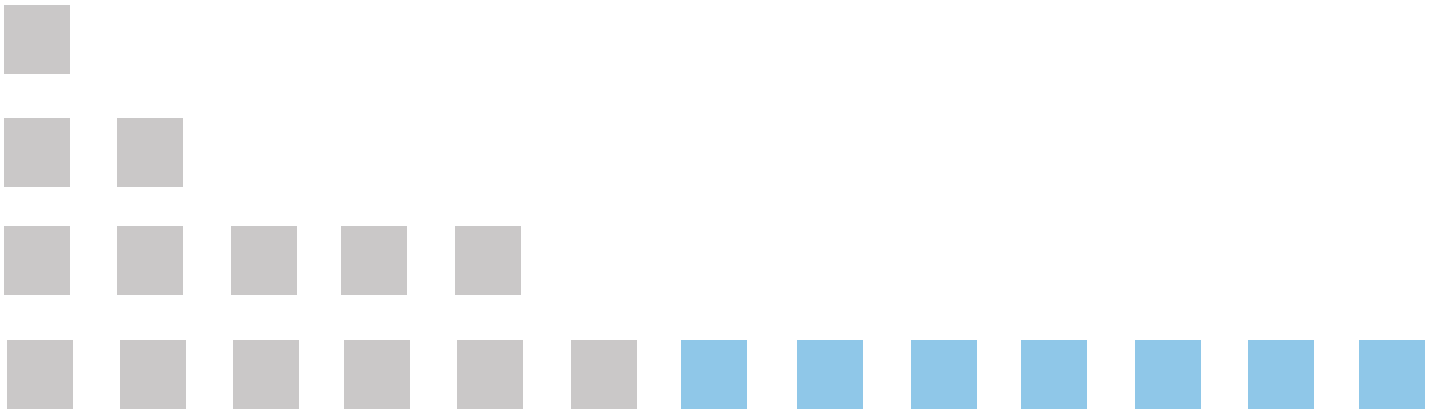

Table of Contents

1 Introduction 2
2 Important Business Services 3
3 Impact Tolerances 5
4 Mapping 9
5 Scenario Testing 10
6 Self-assessment 12
7 Governance 13
8 Communications 14
9 Outsourcing 14
10 Groups 14
11 The Relationship Between Operational Resilience and Operational Risk Policy 15
12 The Relationship Between Operational Resilience and Business Continuity Planning (BCP) 16
13 Implementation 17
14 Supervisory review and feedback 17
15 Reporting an operational incident 17
Annex – Examples 19

1 Introduction

1.1 The purpose of this document is to provide guidance around the obligations set out in the Financial Services (Operational Resilience) Regulations 2023 (the "**Operational Resilience Regulations**"). This Guidance Note is intended to complement existing legislation, policies and guidance and is not intended to conflict with, amend or supersede them.

1.2 The Operational Resilience Regulations apply to:

- insurance and reinsurance undertakings (referred to collectively within this Guidance Note as "insurers");
- credit institutions;
- investment firms to which regulation 4(3) or 4(7) of the Financial Services (Investment Firms) (Prudential Requirements) Regulations 2021 applies;
- electronic-money issuers;
- payment service providers; and
- insurance intermediaries and reinsurance intermediaries with annual revenue from regulated intermediary business of £35 million or more, calculated on a three-year rolling average.

1.3 In addition, Regulation 13 of the Operational Resilience Regulations, which concerns group resilience, applies to:

- CRR group entities (Gibraltar parent financial holding companies or Gibraltar parent institutions of a group, within the meaning of the Financial Services (Credit Institutions and Capital Requirements) Regulations 2020 and the Capital Requirements Regulation as it forms part of the law of Gibraltar); and
- Gibraltar Solvency 2 firms (Gibraltar insurers (other than small undertakings) or Gibraltar reinsurers, within the meaning of the Financial Services (Insurance Companies) Regulations 2020 which are a member of a group for which the GFSC is the group supervisor).

1.4 In order 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.

1.5 The Operational Resilience Regulations require firms to identify important business services and set impact tolerances for these services. Firms must take action to ensure they are able to deliver their important business services within their impact tolerances. Testing against severe but plausible operational disruption scenarios enables firms to identify vulnerabilities and take mitigating action. Further to this, boards and senior management are required to drive improvement where deficiencies are found.

1.6 There are various existing pieces of legislation, policies and guidelines that are relevant to operational resilience (e.g. the European Banking Authority's (EBA's) Guidelines on ICT and security risk management). The GFSC will consider all of the relevant legislation, its own policies and guidance, as well as any relevant international guidelines, when supervising firms' compliance with the Operational Resilience Regulations.

2 Important Business Services

2.1 A business service is a service that a firm provides. Business services deliver a specific outcome or service to an identifiable user external to the firm and should be distinguished from business lines, which are a collection of services and activities. Under the regulation 5(1)(a) of the Operational Resilience Regulations, firms must identify their important business services. Important business services are defined as the services a firm provides which, if disrupted, could:

- cause an intolerable level of harm to any one or more of the firm's clients; or
- pose a risk to:
  - the firm's safety and soundness;
  - the orderly operation of the financial markets;
  - the soundness, stability or resilience of the Gibraltar financial system; or
  - an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer).

2.2 A firm's important business services will be a relatively short list of external-facing services for which the firm has chosen to build high levels of operational resilience in anticipation of operational disruption. Firms should not identify internal services alone (for example human resources or payroll) as important business services. Such internal services, if necessary for the delivery of important business services, would be included in the mapping, scenario testing, and any remediation work firms are required to perform.

2.3 Firms should also consider the practicalities of how they identify their important business services, for example so that:

- an impact tolerance can be applied and tested; and
- boards and senior management can make prioritisation and investment decisions.

2.4 Firms are required to review their important business services annually at a minimum, or sooner if a material change occurs, and to determine whether it is necessary to make any changes to their list of important business services.

2.5 In the course of identifying its important business services under Regulation 5(1)(a), a firm should treat each distinct relevant service separately, and should not identify a collection of services as a single important business service.

2.6 The factors that a firm should consider when identifying its important business services include, but are not limited to:

(1) the nature of the client base, including any vulnerabilities that would make clients more susceptible to harm from a disruption;

(2) the ability of clients to obtain the service from other providers (substitutability, availability and accessibility);

(3) the time criticality for clients receiving the service;

(4) the number of clients to whom the service is provided;

(5) the sensitivity of data held;

(6) the potential to inhibit the functioning of Gibraltar's financial system;

(7) the firm's potential to impact the soundness, stability or resilience of Gibraltar's financial system;

(8) the possible impact on the firm's financial position and potential to threaten the firm's viability where this could:
- cause an intolerable level of harm to any one or more of the firm's clients; or
- pose a risk to:
    - the firm's safety and soundness;
    - the orderly operation of the financial markets;
    - the soundness, stability or resilience of the Gibraltar financial system; or
    - an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer).

(9) the potential to cause reputational damage to the firm, where this could:
- cause an intolerable level of harm to any one or more of the firm's clients; or
- pose a risk to:
    - the firm's safety and soundness;
    - the orderly operation of the financial markets;
    - the soundness, stability or resilience of the Gibraltar financial system; or
    - an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer).

(10) whether disruption to the services could amount to a breach of a legal or regulatory obligation;

(11) the level of inherent conduct and market risk;

(12) the potential to cause knock-on effects for other market participants, particularly those that provide financial market infrastructure or critical national infrastructure;

(13) the importance of that service to Gibraltar's financial system, which may include market share, client concentration, and sensitive clients (for example, governments or pension funds); and

(14) in the case of insurers, the potential impact on policyholders of a disruption to the service, including consideration of:
- the type of product, type of policyholder, and their current or future interests;
- the significance to the policyholder of the risk insured;
- the availability of substitute products that would offer a policyholder a similar level of protection; and
- the potential for significant adverse effects on policyholders if cover were to be withdrawn or policies not honoured.

2.7 When assessing if an impact tolerance can be applied to an important business service, firms are expected to consider if the users of the service are identifiable. This means that the impacts of disruption should be clear. The users of the service may include retail customers, business customers, other legal entities, trustees, market participants, the supervisory authorities, or other members of a regulated entity's group.

2.8 Important business services deliver a specific outcome or service to an identifiable user and should be distinguished from business lines, such as mortgages, which are a collection of services and activities. They will vary from firm to firm. Firms should consider the chain of activities which make up the important business service, from taking on an obligation to delivery of the service, and determine those parts of the chain that are critical to delivery of the important business service. Critical parts of the chain are required to be operationally resilient, and firms should focus their work on the resources necessary to deliver them.

2.9 When assessing if boards and senior management can make prioritisation and investment decisions for an important business service, firms are expected to consider whether the number of important business services is proportionate to their business. It is likely that larger firms will identify a larger number of important business services than smaller firms.

3 Impact Tolerances

3.1 The Operational Resilience Regulations require firms to set an impact tolerance for each of their important business services. They define an impact tolerance as the maximum tolerable level of disruption to an important business service, as measured by a length of time in addition to any other relevant metrics.

3.2 When setting an impact tolerance for an individual important business service, firms must take into account the impact of failure of other related important business services. These may be related because, for example, they share common resources which support the delivery of the important business services or where simultaneous disruption could have compounding impacts on similar external end users. Firms must take a proportionate approach in making this assessment, and only consider extra layers of complexity where there are significant benefits in terms of building operational resilience.

3.3 Impact tolerances provide a standard which boards and senior management should use for prioritising investment, and making recovery and response arrangements. They may be helpful in informing decision-making during operational disruptions, when they would be considered alongside other information relevant to managing an incident effectively.

3.4 Impact tolerances must be set on the assumption that a disruption will occur. Firms should not consider the cause or probability of disruption when setting their impact tolerances.

3.5 An impact tolerance must, in all cases, include a time-based metric to measure the tolerable level of disruption to an important business service. Firms are also required to consider whether time-based impact tolerances should be used in conjunction with additional metrics, such as the volume or value of transactions that the firm can tolerate being interrupted for that period of disruption.

3.6 Firms may choose to set their impact tolerances by assuming an important business service is unavailable for a specified period of time and judging the potential impact this would have. If this disruption would not:

- cause an intolerable level of harm to any one or more of the firm's clients; or
- pose a risk to:
  - the firm's safety and soundness;
  - the orderly operation of the financial markets;
  - the soundness, stability or resilience of the Gibraltar financial system; or

- an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer),

the firm could consider the impact of a longer disruption.

3.7 If, for example, the firm judges that after an important business service has been unavailable for five days, there would be a risk to the firm's clients, this would be the point within which the firm would set its impact tolerance.

3.8 The factors that a firm should consider when setting its impact tolerance include, but are not limited to:

(1) the nature of the client base, including any vulnerabilities that would make the person more susceptible to harm from a disruption;

(2) the number of clients that may be adversely impacted and the nature of the impact;

(3) the potential financial loss to clients;

(4) the potential financial loss to the firm where this could:
- cause an intolerable level of harm to any one or more of the firm's clients; or
- pose a risk to:
  - the firm's safety and soundness;
  - the orderly operation of the financial markets;
  - the soundness, stability or resilience of the Gibraltar financial system; or
  - an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer);

(5) the potential level of reputational damage to the firm where this could:
- cause an intolerable level of harm to any one or more of the firm's clients; or
- pose a risk to:
  - the firm's safety and soundness;
  - the orderly operation of the financial markets;
  - the soundness, stability or resilience of the Gibraltar financial system; or
  - an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer);

(6) the potential impact on market or consumer confidence;

(7) potential spread of risks to their other business services, other firms or Gibraltar's financial system;

(8) the potential loss of functionality or access for clients;

(9) any potential loss of confidentiality, integrity or availability of data;

(10) the potential aggregate impact of disruptions to multiple important business services, in particular where such services rely on common operational resources as identified by the firm's mapping exercise under Regulation 7(1).

3.9 While under Regulation 5(4) a firm must ensure it is able to remain within its impact tolerance, it should generally not do so if this would:

- put the firm in breach of another regulatory obligation;

- conflict with the proper exercise of a discretion granted to it under any legislative provision;
- result in increased risk of an intolerable level of harm to the firm's clients; or
- pose a risk to:
    - the firm's safety and soundness;
    - the orderly operation of the financial markets;
    - the soundness, stability or resilience of the Gibraltar financial system; or
    - an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer);

3.10 Under certain circumstances, a firm may wish to resume a degraded service. This is usually only appropriate if having regard to:

- the interests of the firm's clients;
- the firm's safety and soundness;
- the soundness, stability and resilience of Gibraltar's financial system,
- the orderly operation of the financial markets; and
- an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer),

the benefits of resuming a degraded service outweigh the negatives of keeping the service unavailable until the issues have been fully remediated and the service is able to be fully restored to its pre-disruption levels.

3.11 Under Principle 12 of the Financial Services (Core Principles) Regulations 2022 (the "**Core Principles Regulations**"), the GFSC expects to be notified of any failure by a firm to meet an impact tolerance.

3.12 Payment service providers should have regard to the impact tolerance set under Regulation 5(1)(b) when complying with the EBA Guidelines on ICT and security risk management. In particular, they should, as part of their continuity planning and testing, consider their ability to remain within their impact tolerance through a range of severe but plausible disruption scenarios.

Impact tolerance metrics

3.13 Firms should state their impact tolerances using clear metrics and set at least one impact tolerance for each important business service they have identified.

3.14 Firms are required to use a time-based metric for all impact tolerances in conjunction with other metrics (where appropriate). For example, a firm could set its impact tolerance at a certain volume of interrupted transactions due to the disruption of the firm's important business service, in conjunction with the disruption continuing after a certain number of hours.

3.15 A time-based metric should specify that a particular important business service should not be disrupted beyond a certain period of, or point in, time (e.g. after 24 hours). An impact tolerance that combines time with a volume and/or value metric might state that the firm will not tolerate the business service delivering less than a certain percentage of normal operating capacity for a specified period of time.

3.16 When setting its impact tolerance, a firm should take account of the fluctuations in demand for its important business service at different times of the day and throughout the year in order to ensure that its impact tolerance reflects these fluctuations and is appropriate in light of the peak demand for the important business service.

3.17 Impact tolerances should not consider the frequency at which operational disruptions are likely to occur. Rather, should focus on setting the limit of the impact the firm can tolerate from a single disruption.

3.18 Setting an impact tolerance enables firms to assess the status of, and set resilience requirements for, the necessary people, processes, technology, facilities, and information that contribute to the delivery of important business services. These requirements might include capacity specifications, recovery time, and point objectives which should be set to enable the firm to deliver the important business service within its impact tolerance.

3.19 There may be circumstances when a firm continuing to deliver a service through disruption may have a more adverse impact than suspending it. An example of this is where the firm cannot sufficiently assure the integrity of data underpinning an important business service.

3.20 The Core Principles Regulations will remain relevant to decision making during operational disruptions, including decisions about when an important business service is suspended or restored. When setting impact tolerances, the GFSC expects firms to consider the circumstances that might be prevailing at the time of the disruption to help them make informed recovery and response decisions and when they may decide not to resume the functioning of their important business services within the specified time. The GFSC expects firms should not be forced into inappropriate actions because of their impact tolerances in the event of a disruption.

Actions to remain within impact tolerance

3.21 The Operational Resilience Regulations require firms to ensure they are able to deliver their important business services within impact tolerances in severe but plausible scenarios. Mapping and testing the delivery of important business services will equip firms to establish whether and how they can remain within impact tolerances.

3.22 Firms are expected to take action where they identify a limitation in their ability to deliver important business services within impact tolerances. Complicated business models or the provision of services across borders are unlikely to be considered as good reasons for a firm not to be able to act to ensure they can remain within an impact tolerance – these factors are themselves vulnerabilities that firms are required to address. However, incidents such as rapid technological change may be a reason for a firm to not be able to remain within an impact tolerance, as it may take time to improve resilience under those conditions.

3.23 Firms must develop and implement effective remediation plans for the important business services that would not be able to remain within their impact tolerance. They must take prompt action where they cannot remain within the impact tolerance, so these plans should include appropriate timing for the necessary improvements.

3.24 In developing these plans to improve resilience, firms should consider the:

- nature and scale of the risk that disruption to the important business service could pose to:
    - the firm's clients;
    - the firm's safety and soundness;
    - the soundness, stability or resilience of Gibraltar's financial system;
    - the orderly operation of the financial markets; or
    - an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer),

  and firms should prioritise those that pose the greatest risk;

- time-criticality of the important business service, which is high when the impact tolerance is set for a short amount of time. Firms are required to have undertaken planning and set up recovery and response arrangements in advance to be able to respond quickly to disruptions when they occur;

- scale of improvement necessary to remain within the impact tolerance. An important business service that is far from remaining within the impact tolerance may need to be prioritised over a business service that could nearly remain within its impact tolerance in a severe but plausible disruption.

4 Mapping

4.1 The Operational Resilience Regulations require firms to identify and document the necessary people, processes, technology, facilities, and information (the 'resources') required to deliver each of their important business services. This identification process is referred to as 'mapping'.

4.2 Adequate mapping should enable firms to meet the following outcomes:

- **The identification of vulnerabilities** – Mapping an important business service should allow a firm to identify the resources that are critical to delivering the important business service, ascertain whether they are fit for purpose, and consider what would happen if resources were to become unavailable.

- **Test ability to remain within impact tolerances** – Mapping should facilitate the testing of a firm's ability to deliver important business services within impact tolerances. To design and understand the full implications of scenarios, a map of the relevant business service is necessary.

4.3 Firms are required to map their important business services to the level of detail necessary to use the mapping to identify vulnerabilities and test their ability to remain within impact tolerances. They are required to map the resources necessary to deliver important business services irrespective of whether the resources are being provided wholly or in part by a third party, which may be an intragroup or external provider.

4.4 Firms should understand how their outsourcing and third party dependencies support important business services. They should also understand the reliance placed on sub-outsourcing arrangements and if these arrangements pose a threat to their operational resilience. Where a firm relies on a third party for the delivery of an important business service, we would expect the firm to have sufficient understanding of the people, processes, technology, facilities, and information that support the provision by the third party of its services to or on behalf of the firm so as to allow the firm to comply with its obligations under Regulation 7(1).

4.5 Mapping information should be accessible and usable for the firm. Firms should document their mapping in a way that is proportionate to their size, scale, and complexity. Firms are expected to develop their own methodology and assumptions for mapping to best fit their business.

4.6 Firms must update their mapping annually at a minimum, or following a material change if sooner.

5 Scenario Testing

5.1 The Operational Resilience Regulations require firms to regularly test their ability to remain within impact tolerances in severe but plausible disruption scenarios. Impact tolerances assume a disruption has occurred, and so testing the ability to remain within impact tolerances should not focus on preventing incidents from occurring. Firms are required to focus on recovery and response arrangements.

5.2 Firms should identify the severe but plausible scenarios they use for testing. When setting scenarios, firms could consider previous incidents or near misses within the firm, across the financial sector, and in other sectors and jurisdictions. A testing plan should include realistic assumptions and evolve as the firm learns from previous testing.

5.3 Firms are required to prepare a written self-assessment of compliance with the Operational Resilience Regulations. Firms should document details of their scenario testing, including assumptions made in relation to scenario design and any identified risks to the firm's ability to remain within impact tolerances.

5.4 Over time, a firm's scenario testing is expected to become more sophisticated as firms develop operational resilience for each important business service. Firms will be expected to test against more severe but plausible scenarios, proportionate to the firm and the degree of operational resilience each important business service has.

5.5 When considering the important business services to prioritise for testing, firms should consider the relative risk they pose to:

- the firm's clients;
- the firm's safety and soundness;
- the soundness, stability or resilience of Gibraltar's financial system;
- the orderly operation of the financial markets; or
- an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurer).

5.6 Firms are required to develop a testing plan that details how they will gain assurance that they can remain within impact tolerances for important business services. The nature and frequency of a firm's testing should be proportionate to the potential impact that disruption could cause and whether the operational resources supporting an important business service have materially changed. When developing a testing plan, firms should consider the following:

(1) the type of scenario testing undertaken – for example, whether it is paper-based, simulations or through the use of live-systems;

(2) the scenarios in which the firm expects to be able to remain within their impact tolerances and those in which they may not;

(3) the frequency of the testing – firms that implement changes to their operations more frequently should undertake more frequent scenario testing;

(4) the number of important business services tested – firms that have identified more important business services should undertake more scenario testing to reflect this;

(5) the availability and integrity of supporting assets – impact tolerances are concerned with the continued provision of important business services. An important business service that can continue

to be provided but has insufficient integrity should not be within a firm's impact tolerance. Firms should test their recovery plans for both availability and integrity scenarios, proportionate to their size and complexity;

(6) how the environment is changing and whether this could give rise to different vulnerabilities; and

(7) how the firm expects to communicate with internal and external stakeholders effectively to reduce the harm caused by operational disruptions.

5.7 Scenario testing should not pose a material risk of creating a disruption. Where firms consider that live-systems testing is most appropriate for scenario testing their ability to remain within impact tolerances, firms should assess the risk that the scenario testing may create a disruption to the delivery of important business services. Firms should conduct scenario testing with due skill, care, and diligence, act prudently, have effective risk strategies and risk management, and control their affairs responsibly and effectively.

5.8 The entire chain of activities that has been identified as the important business service should be considered when developing testing plans.

5.9 The severity of scenarios used by firms for their testing could be varied by increasing the number or type of resources unavailable for delivering the important business service, or extending the period for which a particular resource is unavailable. The mapping work that firms will undertake is likely to be useful in informing them how their scenarios could be made more difficult.

5.10 It would not be proportionate to require firms to be able to remain within impact tolerances in circumstances which are beyond severe or are implausible. There will be scenarios where firms find they would not be able to deliver a particular important business service within their impact tolerance. For example, if essential infrastructure (such as power, transport, or telecommunications) were unavailable, some firms may not be able to deliver their important business services within their impact tolerance.

5.11 Firms should test a range of scenarios, including those in which they anticipate exceeding their impact tolerance. Understanding the circumstances where it is impossible to stay within an impact tolerance will provide useful information to firms' management and to the GFSC. Boards and senior management will need to judge whether failing to remain within the impact tolerance in specific scenarios is acceptable and be able to explain their reasoning to supervisors.

5.12 Where a firm relies on a third party for the delivery of its important business services, they should work with the third party to ensure the validity of the firm's scenario testing under Regulation 8(2). To the extent that the firm relies on the third party to carry out testing of the services provided by the third party to or on behalf of the firm, the firm should ensure the suitability of the methodologies, scenarios and considerations adopted by the third party in carrying out testing. The firm is ultimately responsible for the quality and accuracy of any testing carried out, whether by the firm or by a third party.

5.13 In carrying out the scenario testing, a firm should, among other things, consider the following scenarios:

(1) corruption, deletion or manipulation of data critical to the delivery of its important business services;

(2) unavailability of facilities or key people;

(3) unavailability of third party services, which are critical to the delivery of its important business services;

(4) disruption to other market participants, where applicable; and

(5) loss or reduced provision of technology underpinning the delivery of important business services.

6 Self-assessment

6.1 Firms are required to document a self-assessment of their compliance with the Operational Resilience Regulations. Firms are expected to document the methodologies they have used to undertake these activities. Firms' boards are accountable for and should approve the information provided in these documents. Boards and senior management should seek to build resilience so that they gain a high level of assurance that their firm is able to deliver its important business services within impact tolerances. Firms should document this information in the form of a self-assessment.

6.2 A self-assessment should directly address the requirements set out in the Operational Resilience Regulations. Broader elements of firms' operational resilience, for example, operational risk management and business continuity planning, should only be referenced where they directly pertain to the requirements under the Operational Resilience Regulations. Broader elements of firms' resilience should be captured in existing firm practices.

6.3 When documenting a self-assessment, firms should:

(1) list their important business services and why each of these have been identified;

(2) specify the impact tolerances set for these important business services and why each impact tolerance has been set;

(3) detail their approach to mapping important business services, including how the firm has identified the resources that contribute to the delivery of the important business services and how they have captured the relationships between these. Firms should also document how they have used mapping to identify vulnerabilities and to support testing activity;

(4) describe their strategy for testing their ability to deliver important business services within impact tolerances through severe but plausible scenarios. Firms should also describe the scenarios used, the types of testing undertaken, and specify the scenarios under which firms could not remain within their impact tolerances;

(5) identify any lessons learned when undertaking scenario testing or via practical experience, including the actions taken to address the issues encountered or risks highlighted;

(6) identify the vulnerabilities that threaten their ability to deliver important business services within impact tolerances. Firms should make every effort to remediate these vulnerabilities, detailing the actions taken or planned and justifications for their completion time. The completion time should be appropriate to the size and complexity of the firm, and large and complex firms will be expected to take prompt action; and

(7) identify any additional risks to their ability to deliver important business services within impact tolerances arising from elsewhere in their group.

7 Governance

7.1 The role of firms' boards and senior management is central to compliance with the Operational Resilience Regulations. Boards are accountable for and should approve the identification of their firms' important business services and impact tolerances, and their self-assessments.

7.2 The ability of firms to deliver their important business services within their impact tolerances depends on there being appropriate reporting and accountability in place throughout the firm. Where limitations are identified, leadership from firms' boards and senior management is essential to prioritising the investment and cultural change required to improve operational resilience.

Board responsibilities

7.3 Boards are specifically required to approve the important business services identified for their firm and the impact tolerances that have been set for each of these. The Operational Resilience Regulations require that a firm's board approve and regularly review the firm's important business services, impact tolerances, and written self-assessment. In delivering this responsibility, boards must regularly review assessments of the firm's important business services, impact tolerances, and the scenario analyses of its ability to remain within the impact tolerances for the important business services.

7.4 While individual board members are not required to be technical experts on operational resilience, boards must ensure that they have the appropriate management information. Boards should also collectively possess adequate knowledge, skills, and expertise to provide constructive challenge to senior management and inform decisions that have consequences for operational resilience.

7.5 When assessing whether a firm's board is meeting its wider obligations, the GFSC will consider various matters relating to operational resilience, such as whether the board:

- has appropriate management information available to inform decisions that have consequences for the firm's operational resilience;
- has adequate knowledge, skills, and experience in order to provide constructive challenge to senior management and meet its oversight responsibilities in relation to the firm's operational resilience; and
- articulates and maintains a culture of risk awareness and ethical behaviour for the entire organisation, which influences the firm's operational resilience.

Management responsibilities

7.6 Firms should establish clear accountability and responsibility for the management of operational resilience. They should structure their oversight of operational resilience in the most effective way for their business, using existing committees and roles, or establishing news ones if necessary.

7.7 Where a firm has a senior individual with overall responsibility for internal operations and technology, that individual should have overall responsibility for implementing operational resilience policies and reporting to the board.

7.8 Where a firm does not have a board, senior management should take responsibility for compliance with the Operational Resilience Regulations.

8 Communications

8.1 Firms must develop communication strategies for both internal and external stakeholders as part of their planning for responding to operational disruptions. These communication plans should be developed with a view to reducing harm to counterparties and other market participants, and supporting confidence in both the firm and financial sector.

8.2 As part of a firm's communications strategy, a firm should:

- consider, in advance of a disruption, how it would provide important warnings or advice quickly internally and to clients and other stakeholders, including where there is no direct line of communication;
- use effective communication to gather information about the cause, extent, and impact of operational incidents;
- ensure that its choice of communication method takes account of the circumstances, needs and vulnerabilities of its clients and other stakeholders; and
- establish the escalation paths it would use to manage communications during an incident and to identify the appropriate decision makers.

9 Outsourcing

9.1 Firms that enter into outsourcing arrangements remain fully accountable for complying with their regulatory obligations. This is a key principle underlying all requirements and expectations regarding outsourcing and other third party arrangements.

9.2 Firms are expected to be operationally resilient regardless of any outsourcing arrangements or use of third parties. They should not allow their ability to deliver their important business services within their impact tolerances to be undermined when they are delivered wholly or in part by third parties, whether these third parties are other entities within their group or external providers.

9.3 A firm will remain responsible if a third party provider on whom it relies (whether wholly or in part) to provide an important business service, fails to remain within impact tolerances or causes the firm to do so. This means that firms should effectively manage their use of third parties to ensure they can meet the required standard of operational resilience.

9.4 Although firms may assume that an arrangement is inherently less risky where the service provider is part of its own group, this is often not the case. Firms are required to manage risk and make appropriate arrangements to be able to remain within impact tolerances, whether using third parties that are other entities within their group or external providers.

10 Groups

10.1 CRR group entities and Gibraltar Solvency 2 firms (as defined in the Operational Resilience Regulations, and together referred to as "relevant entities") are required to identify a proportionate number of important group business services and respective impact tolerances at the level of the group. Taking a group level view of operational resilience ensures that the risks arising in parts of the group that are not subject to the individual requirements are taken into account.

10.2 When identifying important group business services, relevant entities are expected to consider disruption to services in other entities within the group which could transmit risk to the safety and soundness of the relevant entity either directly or via the group. This includes, for example, where the relevant group has a subsidiary outside Gibraltar providing a service to customers which could, if disrupted, pose a risk to:

- in the case of CRR group entities, the safety and soundness of any firm within the group or, where relevant, the soundness, stability or resilience of the Gibraltar financial system;
- in the case of Gibraltar Solvency 2 firms, the firm's safety and soundness, policyholder protection or, where relevant, the soundness, stability or resilience of the Gibraltar financial system.

10.3 Impact tolerances should be set in the same way as they are for an individual firm. Boards and senior management should consider the level of disruption that would represent a threat to the relevant entity, for example via a threat to the viability of the group, and therefore pose a risk to the firm's safety and soundness, to the soundness, stability or resilience of the Gibraltar financial system, or (in the case of Gibraltar Solvency 2 firms) to there being an appropriate degree of protection for those who are or may become the firm's policyholders.

10.4 In complying with the Operational Resilience Regulations, relevant entities should have regular dialogue with other members of their group so as to take account of any additional risks to their safety and soundness when assessing their ability to remain within impact tolerance for their own important business services.

10.5 Relevant entities should work with other members of their group to take action, should it be likely that a relevant important group business service could not be delivered within their impact tolerance. Firms are required to cover analysis of risks arising from elsewhere in the group in their self-assessments.

11 The Relationship Between Operational Resilience and Operational Risk Policy

11.1 Operational risk management supports both operational resilience and financial resilience. Firms should have effective risk management systems in place to manage operational risks that are integrated into their organisational structures and decision-making processes.

11.2 When assessing a firm's operational risk management, the GFSC will consider the extent to which firms:

- have reduced the likelihood of operational incidents occurring;
- can limit losses in the event of severe business disruption; and
- hold sufficient capital to mitigate the impact when operational risks crystallise.

11.3 The additional requirements the Operational Resilience Regulations place on firms to limit the impact of disruptions when they occur, whatever their cause, develop the broader approach to operational risk under Gibraltar's financial services regulatory framework in two key ways:

- they increase firms' focus on their ability to respond to and recover from disruptions, assuming failures will occur; and
- they address the risk that firms may not necessarily consider the public interest when developing their operational resilience.

Risk Appetite and Impact Tolerances

11.4 Impact tolerances differ from risk appetites in that they assume a particular risk has crystallised instead of focusing on the likelihood and impact of operational risks occurring. Firms that are able to remain within their impact tolerances increase their capability to survive severe but plausible disruptions, despite the fact that their risk appetites are likely to be exceeded in these scenarios. Impact tolerances are set only in relation to impact on the firm's clients, the firm's safety and soundness, the orderly operation of the financial markets, and in the case of insurers, the appropriate degree of policyholder protection.

Financial Resilience

11.5 Firms are required to hold capital to ensure they can absorb losses resulting from operational risks such as fraud, damage to physical resources, business disruption, and system failures. However, the Operational Resilience Regulations do not have an associated capital requirement and therefore do not affect the GFSC's approach to assessing firms' operational risk capital or add additional considerations for firms when they make capital calculations.

12 The Relationship Between Operational Resilience and Business Continuity Planning (BCP)

12.1 The Operational Resilience Regulations complement requirements under sector-specific regulations that also seek to ensure firms' response and recovery capabilities. For example:

- under Regulation 42(3) of the Financial Services (Credit Institutions and Capital Requirements) Regulations 2020, the GFSC is required to "ensure that contingency and business continuity plans are in place to ensure an institution's ability to operate on an ongoing basis and limit losses in the event of a severe business disruption"; and

- under Regulation 43(6) of the Financial Services (Insurance Companies) Regulations 2020, an insurer "must take reasonable steps to ensure continuity and regularity in the performance of its activities, including the development of contingency plans".

12.2 BCP requirements in sector-specific regulations and those in the Operational Resilience Regulations are closely linked. However, the Operational Resilience Regulations focus on a firm's ability to deliver its important business services rather than single points of failure. The GFSC considers both BCP and operational resilience requirements together when supervising firms. For example, when assessing whether banks are meeting their internal governance obligations, the GFSC will consider if their:

- recovery priorities for their operations prioritise the delivery of important business services within impact tolerances;
- allocation of resources and communications planning for business continuity planning focuses on the delivery of important business services; and
- tests of business continuity plans complement the testing of disruption scenarios and relate to impact tolerances.

13 Implementation

13.1 By 13 July 2024, firms must have identified their important business services and set impact tolerances. In order to achieve this, and to identify any vulnerabilities in their operational resilience, firms should have mapped their important business services and commenced a programme of scenario testing.

13.2 Firms are not expected to have performed mapping and scenario testing to the full extent of sophistication by 13 July 2024. Both mapping and scenario testing are ongoing processes, and firms are expected to perform them at varying levels of sophistication over time. Firms' approaches to both mapping and scenario testing should evolve over time.

13.3 Firms are expected to have a prioritised plan which sets out how they will comply with the requirement to be able to remain within their impact tolerances within a reasonable time, and no later than 13 July 2026. For a firm's plan to be effective, firms must have started putting the plan into effect by 13 July 2024.

13.4 After 13 July 2026, maintaining operational resilience will be a dynamic activity. By this point, firms should have sound, effective and comprehensive strategies, processes, and systems that enable them to address risks to their ability to remain within their impact tolerance for each important business service in the event of a severe but plausible disruption.

14 Supervisory review and feedback

14.1 The GFSC may provide a view or guidance on an individual basis during the course of its supervision as to whether a firm's compliance with the Operational Resilience Regulations and this Guidance Note is adequate and, if necessary, require a firm to take the necessary actions or steps to address any failure to meet the relevant requirements.

14.2 A firm should have regard to the views provided by the GFSC in relation to the firm's compliance. If a firm considers that any individual view or guidance given to it by the GFSC is inappropriate to its circumstances it should, consistent with Principle 13 of the Core Principles Regulations, inform the GFSC that it disagrees with that view or guidance. The GFSC may reissue the individual view or guidance if, after discussion with the firm, the GFSC concludes that the appropriate actions or steps a firm should take is different from that initially suggested by the GFSC.

14.3 If, after discussion, the GFSC and the firm still do not agree, the GFSC may consider other tools available to it (including its powers under sections 69 and 70 of the Financial Services Act 2019) on its own initiative, to require the firm to take specific steps in line with the GFSC's view to comply with the relevant Operational Resilience Requirements.

15 Reporting an operational incident

15.1 Under Principle 12 of the Core Principles Regulations, firms are required to deal with the GFSC in an open, cooperative and timely way and to disclose to us any matter of which we would reasonably expect notice. This means that firms are required to report material operational incidents to the GFSC. An incident may be material if it:

- results in a significant loss of data;
- results in the unavailability or control of the firm's IT systems;
- affects a large number of customers; or
- results in unauthorised access to the firm's information systems.

Note that this list is not exhaustive. Payment service providers should also be aware of their obligations to report major operational or security incidents under the Financial Services (Payment Services) Regulations 2020.

15.2 If a firm considers an incident to be material, it should report it to the GFSC by:

- disclosing it to the firm's main supervisory contact; or
- contacting the GFSC via our contact page.

15.3 Firms should also consider whether they may need to report the incident to anybody else:

- If firms believe the incident is criminal, they should report it to the Royal Gibraltar Police as well as the GFSC.
- If the incident involves a data breach, firms should report it to the Gibraltar Regulatory Authority as well as the GFSC. Note that there is a requirement to report it to the GFSC as soon as the firm becomes aware of the breach, and to the GRA within 72 hours of becoming aware of the breach.

Annex – Examples

Below, two fictional firms are used to illustrate how some elements of the Operational Resilience Regulations might apply to different types of firms. We acknowledge that in practice firms delivering business services would consider many other operational issues, dependencies, nuances in business models and risk management considerations. There examples are non-exhaustive and purely illustrative. Firms will need to consider how the elements apply to their own circumstances.

Firm background

Firm A is an electronic money institution with global operations, with core markets in Gibraltar, the UK and the European Economic Areas (EEA). It offers multiple payment products including electronic money 'e-wallet accounts' and pre-paid cards. Users based in Gibraltar and the UK make up about 20% of the firm's daily active users and 25% of daily transactions.

Firm B is an insurance intermediary that sells insurance products to retail customers to help them meet their specific needs. In addition, certain insurers have outsourced claims handling to Firm B and it holds claims money to be paid to customers under risk transfer agreements. Firm A offers its services mainly via its online portal as well as via agents in its contact centres.

How our example firms might identify important business services

Firm A identifies the provision of its multi-currency e-wallet account from which users can initiate electronic payment transactions as one of its important business services for the purposes of operational resilience. Users access their e-wallet account through the firm's proprietary Apple and Android mobile apps. Access is via App only, there is no web-browser option. Firm A considers that loss of access to the e-wallet accounts can cause significant harm to its users, many of which are consumers, as that is the primary channel through which they manage payment transactions and interact with the firm.

Firm B identifies claims handling for its customers as one of its important business services for the purposes of operational resilience.

Firm B considers that disruption to the claims handling process could cause intolerable harm to consumers. For example, if consumers are unable to notify Firm B of their claim, submit a claim and/or and receive a claims payout/benefit under the policy.

How our example firms might set impact tolerances

Firm A - To set an impact tolerance relevant to its important business service of the provision of multi-currency e-wallet accounts from which users can initiate electronic payment transactions, Firm A considers the potential harm in the event of loss of its mobile app platform functionality. It identifies that consumer harm is the most relevant harm given the number of consumers affected and their reliance on the service for bill payments.

Firm A quantifies the proportion of daily active users of its platform including the average volume of transactions and determines that there are a sizable number of consumers who may rely solely on its service to manage their finances (including to make bill payments) and are therefore susceptible to greater detriment. Firm A also considers substitutability from the users' perspectives and concludes that the unavailability of its e-wallet account will be particularly detrimental to users whose e-wallet accounts do not have card or ATM functionality, thereby leaving users with no alternative way to access their funds. Using a

time-sensitive metric, Firm A concludes that the appropriate impact tolerance is 2 hours to reflect the maximum disruption before there is an intolerable risk of consumer harm.

Firm B has identified that disruption to its claims handling process for motor insurance could lead to potential consumer harm. For example, consumers being unable to obtain a courtesy car in a timely manner which could cause further disruptions in their lives.

Firm B expects that consumers may want to notify them of a claim as soon as possible in order to progress their claim and obtain peace of mind. It further recognises that customers with courtesy car cover are likely to be seeking the courtesy vehicle soon after the accident. So, Firm B considers the maximum tolerable period for disruption to both their online portal and contact centre should be set at 2 days. Firm B considers it is important to have both channels available as some consumers may not have access to one channel or have preferences to use one channel over another.

How our example firms may approach the mapping exercise

Firm A conducts a mapping exercise to fully outline the underlying systems, technology and people, including material third party suppliers, and their interdependencies that enable its mobile platform app. From its mapping, Firm A concludes that its proprietary software engineering procedures and code enhancement (a core dependency) ensures resiliency by design including advance monitoring tools for early detection of availability and performance anomalies.

Firm A also engages with critical third-party suppliers including data centre providers (Cloud Provisioning) where mobile app servers are hosted to understand their risk controls and agree a compatible service level agreement. It leveraged an existing map used for its annual business impact analysis during its mapping exercise.

Firm B undertakes a mapping exercise of the resources that support the delivery of claims handling process. Firm A's mapping reflects that it employs 180 contact centre agents (inbound call handlers) who work across two 7-hour shifts during office hours in their main office location, and have the appropriate technology to work from home if required.

Firm B has identified most of the technology infrastructure including the online portal are hosted in the cloud provided by an external cloud service provider. The contact centre is located at the same location as the main office, and its technology and infrastructure are outsourced to a major telecom company where a service level agreement is in place.

How our example firms may conduct scenario testing

Firm A conducts regular reviews of resources that enable the delivery of its business services as part of its annual business impact analysis. It designs severe but plausible scenarios, considering the potential impact of loss of third-party provision, and engages third parties to test the enablers of its e-wallet account provision for users. These tests indicate some residual risks and resilience gaps when faced with a severe but plausible scenario including those associated with channel of service delivery and cloud service provisioning by third parties.

Following a review of lessons learned, Firm A provides a web channel as an additional service delivery channel to users as a back-up solution, and as an alternative in all eventualities. Among other actions, the firm also conducts a benchmarking exercise to identify alternate cloud providers with dispersed data centres across broader geographical spread where servers can be hosted to enable seamless continuity of service in all eventualities. It sets in motion plans to refresh its data protection policy to recognise cross-jurisdictional legal

and regulatory requirements and develops a communication plan to advise users about alternative ways to access services and updates for service resumption.

Firm B works with its cloud and contact centre infrastructure providers to design and test severe but plausible scenarios, considering the potential impact of cloud disruption, to ensure it can remain within its impact tolerance.

During testing, Firm B has identified challenges with its contact centre provider, where there were significant dependencies on the provider's sub-contractor based in a different country, and due to resource stretch and poor change management practices, the sub-contractor was unable to bring Firm B's contact centre systems back online within the 2-day time frame.

Firm B has also identified there was a significant backlog of cases after a disruption, and its current call handling resourcing plans were inadequate to deal with the backlog of cases.

Firm B initiated a review to improve its controls over the monitoring and oversight of the contact centre provider. It also revisited its contractual terms and service level agreement (including the use of sub-contractors) with the provider, to ensure appropriate service and support can be provided to enable Firm B to remain within tolerance.

Firm B also updated its resourcing plans to allow additional call handlers to be brought in and trained up straight after an outage to minimise the backlog of cases.