Subsidiary Legislation made under ss. 620, 621 and 627.

# Financial Services (Operational Resilience) Regulations 2023

## LN.2023/188

*Commencement* **13.7.2023**

---

**ARRANGEMENT OF REGULATIONS**

Regulation

1. Title.
2. Commencement.
3. Interpretation.
4. Application.
5. Operational resilience requirements.
6. Strategies, processes and systems.
7. Mapping.
8. Scenario testing.
9. Lessons learned exercises.
10. Self-assessment.
11. Governance.
12. Communications.
13. Group resilience.

# 2023/188 Financial Services (Operational Resilience) Regulations 2023

*In exercise of the powers conferred on the Minister by sections 620, 621 and 627 of the Financial Services Act 2019, the Minister has made these Regulations-*

**Title.**

1. These Regulations may be cited as the Financial Services (Operational Resilience) Regulations 2023.

**Commencement.**

2. These Regulations come into operation on the day of publication.

**Interpretation.**

3. In these Regulations–

"firm" means an authorised person in any category in regulation 4;

"impact tolerance" means the maximum tolerable level of disruption to an important business service, as measured by a length of time and any other relevant metrics;

"important business service" means a service provided by a firm or by another person on its behalf, to one or more its clients which, if disrupted, could–

(a) cause an intolerable level of harm to any one or more of the firm's clients; or

(b) pose a risk to-

(i) the firm's safety and soundness;

(ii) the orderly operation of the financial markets;

(iii) the soundness, stability or resilience of the Gibraltar financial system; or

(iv) an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurance or reinsurance undertaking); and

"relevant entity" has the meaning given in regulation 13.

**Application.**

4.(1) Regulations 5 to 12 apply to the following categories of authorised persons–

(a) insurance undertakings and reinsurance undertakings;

(b) credit institutions;

(c) investment firms to which regulation 4(3) or 4(7) of the Financial Services (Investment Firms) (Prudential Requirements) Regulations 2021 applies;

(d) electronic-money issuers;

(e) payment service providers; and

(f) insurance intermediaries and reinsurance intermediaries, with annual revenue from regulated intermediary business of £35 million or more, calculated on a three-year rolling average.

(2) Regulation 13 applies to relevant entities.

(3) Subject to sub-regulation (4), a firm or relevant entity must comply with these Regulations by no later than the first appointed day.

(4) A firm or relevant entity must be able to remain within the impact tolerances it has set under regulation 5(1)(b) or 13(3)(b) as soon as reasonably practicable after the first appointed day and by no later than the second appointed day.

(5) In this regulation–

the "first appointed day" means the day one year after the day on which these Regulations come into operation; and

the "second appointed day" means the day two years after the first appointed day.

**Operational resilience requirements.**

5.(1) A firm must–

(a) identify its important business services; and

(b) set an impact tolerance for each of those important business services.

(2) The impact tolerance set for each important business service must specify the first point at which a disruption to the service would–

(a) cause an intolerable level of harm to any one or more of the firm's clients; or

(b) pose a risk to-

(i) the firm's safety and soundness;

(ii) the orderly operation of the financial markets;

(iii) the soundness, stability or resilience of the Gibraltar financial system; or

(iv) an appropriate degree of protection for those who are or may become the firm's policyholders (where the firm is an insurance or reinsurance undertaking).

(3) The impact tolerance set for each important business service must specify the length of or point in time, in addition to any other relevant metrics, for which a disruption to that service can be tolerated.

(4) A firm must ensure it can remain within its impact tolerance for each important business service in the event of a severe but plausible disruption to its operations.

(5) A firm which is a member of a group to which regulation 13 applies must ensure that it takes account of any additional risks arising elsewhere within the group that may affect the firm's ability to comply with sub-regulation (4).

(6) A firm which outsources important business services must ensure that it takes account of any additional risks arising from the outsourcing that may affect the firm's ability to comply with sub-regulation (4).

(7) A firm must keep its compliance with sub-regulation (1) under review and, in particular, in the following circumstances–

(a) if there is a material change to the firm's business or the market in which it operates; and

(b) in any event, no later than one year after it last carried out the relevant assessment.

**Strategies, processes and systems.**

6.(1) A firm must have in place sound, effective and comprehensive strategies, processes and systems enable it adequately to–

(a) identify its important business services;

(b) set an impact tolerance for each important business service; and

(c) identify and address any risks to its ability to comply with regulation 5(4).

(2) Those strategies, processes and systems must be proportionate to the nature, scale and complexity of the firm's activities.

**Mapping.**

7.(1) A firm must identify and document the necessary people, processes, technology, facilities and information required to deliver each of its important business services in sufficient detail to enable the firm to identify vulnerabilities and take appropriate remedial steps to address them.

(2) Where a firm relies on a third party for the delivery of an important business service, the firm must 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 sub-regulation (1).

(3) A firm must keep its compliance with sub-regulations (1) and (2) under review and, in particular, in the following circumstances–

(a) if there is a material change to the firm's business or the important business services identified, or impact tolerances set, in accordance with regulation 5(1); and

(b) in any event, no later than one year after it last carried out the relevant assessment.

**Scenario testing.**

8.(1) A firm must develop and regularly update a scenario testing plan that sets out in appropriate detail how it will gain assurance that it can remain within its impact tolerances for each of its important business services.

(2) A firm must carry out scenario testing, to assess its ability to remain within its impact tolerance for each of its important business services in the event of a severe but plausible disruption of its operations.

(3) In carrying out the scenario testing, a firm must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to the delivery of the firm's important business services in those circumstances.

(4) The scenario testing undertaken in accordance with sub-regulation (1) must be proportionate to the nature, scale and complexity of the firm's activities.

(5) Where a firm relies on a third party for the delivery of an important business service, the firm–

(a) must work with the third party to ensure the validity of the firm's scenario testing; and

(b) to the extent that it relies on the third party to carry out testing of the services it provides to or on behalf of the firm, must ensure the suitability of the methodologies, scenarios and considerations adopted by the third party in carrying out the testing,

but the firm is ultimately responsible for the quality and accuracy of any testing carried out, whether by the firm or by a third party.

(6) A firm must carry out the scenario testing on a regular basis and, in particular, in the following circumstances–

(a) if there is a material change to the firm's business or the important business services identified, or impact tolerances set, in accordance with regulation 5(1); or

(b) following changes made by the firm in response to a previous test.

**Lessons learned exercises.**

9. After a firm has undertaken scenario testing or following a disruption of its operations, the firm must–

(a) conduct a lessons learned exercise to identify any weaknesses; and

(b) take appropriate steps to address any weaknesses identified, so as to–

(i) improve its ability to respond effectively to and recover from any future disruption; and

(ii) ensure that it remains within its impact tolerances in accordance with regulation 5(4).

**Self-assessment.**

10.(1) A firm must prepare and regularly update a written self-assessment of its compliance with these Regulations.

(2) Without limiting sub-regulation (1), a firm's written self-assessment must include–

(a) the important business services identified by the firm and its justification for their identification;

(b) the firm's impact tolerances and its justification for the level at which they have been set;

(c) the firm's approach to mapping under regulation 7, including how it has used mapping to identify–

(i) the people, processes, technology, facilities and information required to deliver each of its important business services; and

(ii) vulnerabilities;

(d) the firm's plan for scenario testing under regulation 8 and its justification for the plan adopted;

(e) details of the scenario testing carried out as part of its obligations under regulation 8, including a description and justification of the assumptions made in relation to scenario design and any identified risks to the firm's ability to meet its impact tolerances;

(f) any lessons learned exercise conducted under regulation 9;

(g) an identification of the vulnerabilities that threaten the firm's ability to deliver its important business services within the impact tolerances set, including the actions taken or planned and justifications for their completion time;

(h) its communication strategy under regulation 12 and an explanation of how it will enable the firm to reduce the anticipated harm caused by operational disruptions.

(3) The content and level of detail of a firm's written self-assessment must be proportionate to the nature, scale and complexity of the firm's activities and, where applicable, to the activities of the group of which the firm is a member.

(4) A firm must maintain and be able to provide to the GFSC on request, a current version of its written self-assessment, together with all versions produced during the preceding six years.

**Governance.**

11.(1) A firm must ensure that its management body approves–

(a) the important business services identified by the firm in accordance with regulation 5(1)(a); and

(b) the impact tolerances set by the firm in accordance with regulation 5(1)(b).

(2) A firm must ensure that its management body approves and regularly reviews the self-assessment prepared by the firm under regulation 10(1).

**Communications.**

12.(1) A firm must maintain an internal and external communication strategy to assist it in quickly and effectively reducing the anticipated harm caused by operational disruptions.

(2) A firm must provide clear, timely and relevant communications to clients and other stakeholders in the event of an operational disruption.

**Group resilience.**

13.(1) This regulation apples to relevant entities.

(2) In this regulation–

"CRR group entity" means the Gibraltar parent financial holding company or Gibraltar parent institution 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;

"external group end user" means a person who receives services and who is not a member of a relevant entity's group;

"Gibraltar Solvency 2 firm" means a Gibraltar insurer (other than a small undertaking) or Gibraltar reinsurer, within the meaning of the Financial Services (Insurance Companies) Regulations 2020 which is a member of a group for which the GFSC is the group supervisor;

"important group business service" means–

(a) in the case of a Gibraltar Solvency 2 firm, a service provided by another member of the firm's group to an external group end user which, if disrupted, could pose a risk to–

(i) the firm's safety and soundness;

(ii) the soundness, stability or resilience of the Gibraltar financial system; or

(iii) an appropriate degree of protection for those who are or may become the firm's policyholders; or

(b) in the case of a CRR group entity, a service provided by another member of the. entity's group to an external group end user which, if disrupted, could pose a risk to–

(i) the safety and soundness of any the firm within the group; or

(ii) the soundness, stability or resilience of the Gibraltar financial system; and

"relevant entity" means a Gibraltar Solvency 2 firm or a CRR group entity.

(3) A relevant entity must–

(a) identify each important group business service; and

(b) set an impact tolerance for each important group business service.

(4) A relevant entity must assess whether each member of the group providing each important group business service could remain within the impact tolerance set for that important group business service in the event of a severe but plausible disruption to its operations.

(5) The impact tolerance set for each important group business service must specify the first point at which a disruption to the important group business service would pose a risk to–

(a) in the case of a Gibraltar Solvency 2 firm–

(i) the firm's safety and soundness;

(ii) the soundness, stability or resilience of the Gibraltar financial system; or

(iii) an appropriate degree of protection for those who are or may become the firm's policyholders; or

(b) in the case of a CRR group entity–

(i) the safety and soundness of any the firm within its group; or

(ii) the soundness, stability or resilience of the Gibraltar financial system.

(6) The impact tolerance set for each important group business service must specify the length of or point in time, in addition to any other relevant metrics, for which a disruption to that important group business service can be tolerated.

(7) A relevant entity must have in place sound, effective and comprehensive strategies, processes and systems that enable it adequately to–

(a) identify each important group business service;

(b) set an impact tolerance for each important group business service; and

(c) assess whether each member of the group providing each important group business service could remain within the impact tolerance set for that important group business service in the event of a severe but plausible disruption to its operations.

(8) The strategies, processes and systems required under sub-regulation (7) must be proportionate to the nature, scale and complexity of the group's activities.

(9) A relevant entity must identify and document the necessary people, processes, technology, facilities and information required to deliver each of its important group business services, in sufficient detail to enable the firm to identify vulnerabilities and take appropriate remedial steps to address them.

(10) A relevant entity must ensure that its management body approves–

(a) the important group business services identified in accordance with sub-regulation (3)(a);

(b) the impact tolerances set in in accordance with sub-regulation (3)(b); and

(c) the assessment undertaken in in accordance with sub-regulation (4).