

Key:

Relevant for...

- Regulated firms within scope of the new rules
- Regulated firms and their vendors
- Vendors providing important business services on behalf of regulated firms

Obligation / action	Description	Comment
Identifying important business services	<p>Firms are required to identify the services they provide which, if disrupted, could potentially cause intolerable harm to the consumers of the firm's services or a risk to market integrity</p>	<p>The FCA believes that firms are best placed to identify their important business services in the context of their business models – and so refrains from giving a prescriptive definition – but does give some guidance on how to identify these:</p> <ul style="list-style-type: none"> ▪ Generally, internal processes (such as payroll) and centrally shared services do not constitute important business services. ▪ Important business services should be clearly identifiable as separate services and firms must take care to ensure they do not conflate two services that, under the rules, should be identified separately. ▪ Some firms may find it helpful to identify all business services first, before proceeding to identify which of those are 'important'. ▪ Firms should consider both the size and nature of the consumer base when identifying important business services, although these considerations may not be determinative in all cases. <p>Firms should identify their important business services at least once a year or whenever there is a relevant change to their business or the market in which they operate. Relevant changes to a firm's business include:</p> <ul style="list-style-type: none"> ▪ carry out a new activity/ceasing to provide an existing activity; ▪ outsourcing a new/existing service to a third-party service provider; and ▪ changes to an existing service in terms of scale or potential impact.
Communications strategies	<p>Firms should have in place internal and external communication strategies to respond quickly and effectively to reduce the harm caused by operational disruptions.</p>	<p>For internal communications strategies, firms should establish the escalations paths they would use to manage communications during an incident, and identify appropriate decision makers.</p> <p>For an external communications strategy, the FCA requires that firms consider how they will provide important warnings or advice to consumers and other stakeholders, including where there is no direct line of communication.</p>

Obligation / action	Description	Comment
Self-documentation	Firms must compile a self-assessment document which shows how they meet their operational resilience requirements.	<p>Firms are not required to submit their self-assessment document to the FCA, however the document is required to be available on request from 31 March 2022.</p> <p>Boards are required to review and approve the self-assessment document regularly.</p> <p>Firms do have a degree of discretion regarding the information they include in their self-assessment document, however certain information is also prescribed under the new rules such as documenting important business services, impact tolerances, mapping approach and testing plans.</p>
Lessons learned exercises	Firms must conduct a lessons learned exercise following scenario testing or if an operational disruption occurs.	<p>The lessons learned exercises allow firms to identify any weaknesses in their operational resilience and improve their ability to respond to, and recover from, future disruptions.</p> <p>Firms should implement any actions arising from their lessons learned exercise to ensure they can remain within their impact tolerances.</p> <p>Lessons learned exercises must also be referenced in the self-assessment document.</p>
Setting impact tolerances	<p>Firms must set impact tolerances for their important business services; the point at which disruption to such services would cause intolerable harm to consumers or a risk to market integrity.</p> <p>Firms must operate within tolerance at all times including during severe but plausible scenarios.</p> <p>Firms may need to collaborate with vendors to set impact tolerances for outsourced services.</p>	<p>Severe but plausible scenarios include disruptions both inside and outside of a firm's control, such as due to cyber-attacks or wider telecommunications / power failures. The FCA encourage firms to take a pragmatic approach regarding scenarios in and out of scope.</p> <p>'Intolerable harm' is not defined under the new rules and the definition will vary from firm to firm and across sectors. However the FCA does describe intolerable harm as harm from which consumers cannot easily recover. An example includes where a firm is unable to put a client back into a correct financial position, post-disruption. Some of the factors to have regard to include:</p> <ul style="list-style-type: none"> ▪ the number and types (such as vulnerability) of consumers adversely affected, and nature of impact; ▪ financial loss to consumers; ▪ loss of functionality or access for consumers; and ▪ any loss of confidentiality, integrity or availability of data. <p>Where a firm is using a third party to provide important business services, it should work effectively with that provider to set and remain within impact tolerances, as responsibility still ultimate rests with the firm.</p>

Obligation / action	Description	Comment
Setting impact tolerances		<p>An important metric for measuring impact tolerances is the time/duration metric (specifying that an important business service should not be disrupted beyond a certain period of, or point in, time). Other metrics, such as the financial impact of a disruption event, can supplement this however.</p> <p>If a firm cannot remain within impact tolerance for any reason, it should report the issue to the FCA.</p>
Mapping	<p>Firms must identify and document the “people, processes, technology, facilities and information (resources)” necessary to deliver each of their important business services.</p> <p>Firms may require assistance from vendors to map their outsourced services, particularly where those services rely on providers further down a supply chain.</p>	<p>Mapping helps firms to identify and address any vulnerabilities in their operational resilience.</p> <p>Firms will need to map to a level of granularity that is sufficient to identify the people, processes, technology, facilities and information that support the operation of their important business services.</p> <p>The 31 March 2022 deadline requires firms to conduct mapping to a level of sophistication necessary to identify important business services, set impact tolerances and identify any vulnerabilities. Firms must then continue their mapping exercise so that they can remain within impact tolerances for each important business service as soon as reasonably practicable and by 31 March 2025 at the latest.</p> <p>Mapping will need to take place where there is a material change to the firm’s business, important business services or impact tolerances, and no later than 1 year after it was last carried out.</p> <p>Firms must also accurately map services outsourced to a third party or beyond (e.g. 4th or 5th party provider).</p>
Scenario testing	<p>Firms must perform scenario testing to test their ability to remain within impact tolerances for each important business service in the event of a range of adverse scenarios, including severe but plausible disruptions.</p> <p>Firms should approach testing with vendors in the same way as they approach mapping exercises, working with vendors to facilitate testing.</p>	<p>Several factors will influence the testing methods firms employ including the firm’s size, scale and complexity, its business (considering the sector, products, and services), and the ‘severe but plausible’ scenarios identified.</p> <p>Similarly to mapping, firms only need to carry out scenario testing by 31 March 2022 to a level of sophistication necessary to identify important business services, set impact tolerances and identify any vulnerabilities, and must continue to perform scenario testing to be able to remain within impact tolerances for each important business service as soon as reasonably practicable after that deadline and by 31 March 2025 at the latest.</p> <p>Regarding frequency, firms must scenario test when there is a material change to the firm’s business, important business services or impact tolerances, following improvements made by the firm in response to a previous test, and in any event, on a regular basis.</p>

Obligation / action	Description	Comment
		Where firms work with vendors to facilitate testing, this may be conducted by the firm itself or by the vendor. In the latter scenario, firms will need to satisfy themselves of the vendor's methodologies, scenarios and considerations as responsibility ultimately still rests with the firm.
Impact assessment	Vendors should assess the impact of the new operational resilience rules on them and their customers.	<p>Vendors are likely to be on the receiving end of the operational resilience analysis of their customers. In some circumstances, this may mean having to bolster their own operation resilience.</p> <p>Therefore, vendors should assess the impact of the new rules on their important business services to the same extent as their customers to prepare for their customers requiring compliance with the new regime.</p> <p>Vendors should also consider whether their existing contract terms in place with customers apply to any work or updates needed in this context (e.g. change in law clauses).</p>
Standardise offering	Vendors should look at standardising their offering in light of the new rules.	<p>To demonstrate their compliance capabilities to customers, vendors should look to standardising their offering, which may provide an advantage if undertaken before competitors.</p> <p>Proactive engagement with customers about how a vendor is managing the impact of the new operational resilience rules may also provide a useful approach / sales tool.</p>