What is operational resilience and how can an organization become operationally resilient?

An FCG whitepaper

Operational Risk and Resilience goes hand in hand

Operational resilience refers to an organization's ability to *prevent* as well as *handle* potential threats and disruptions in critical operations and *maintain* these abilities over time. Naturally, the challenge of establishing an operationally resilient organization concerns the latter, i.e., making sure it stays resilient. In a digital and fast-paced industry such as the financial industry, this becomes even more challenging. Ensuring, establishing and maintaining operational resilience while also being able to focus on business development and innovation can be tough and puts high demands on efficient and effective organizations, management and processes.

As the concept of operational resilience is broad, it can be hard to know where to begin and the challenges varies depending on the organization. Guidance can be found in existing regulation in terms of processes and other tools that, if properly implemented, provide a good foundation for operational resilience. Based on regulation, industry experience and best practice, we have summarized three starting points together with do's and don'ts. If implemented correctly, it can provide a start for anyone working within the financial industry who wishes to improve the operational resilience of their organization. But before we dive into this, we need to clarify the range of operational resilience somewhat more.

As previously stated, operational resilience is the continuous work of *preventing* and *handling* disruptions effectively and efficiently. A large part of the preventive actions is prudent and proactive risk management where threats, vulnerabilities and risks are identified. This can have both a high and a low impact on the operational resilience depending on the nature of controls and mitigating actions. An important part of prevention is also to test and verify that controls and plans for keeping the organization resilient work as intended. The handling part of operational resilience refers to the abilities to adapt, respond to, recover and learn from disruptions. The adapt, respond and recover parts are closely linked to the process of managing incidents, where input from operational resilience scenarios can be helpful in handling the incident. To learn from these disruptions is key to having efficient resilience. Without learning from disruptive events there is a risk that the work with operational resilience is not a continuous process which is essential. To make sure that operational resilience does not become an administrative burden it is important to collaborate within the organization and make use of work that is already performed as a part of other processes. Here are some starting points to provide guidance in navigating the subject of operational resilience.

ÖSTERMALMSTORG 1, 5TR
SE-114 42, STOCKHOLM, SVERIGE
FCG.GLOBAL

Process mapping – Understand your business

To be able to be operationally resilient, an organization must understand its business and identify dependencies and critical resources in order to learn its weaknesses. Only when weaknesses have been identified and understood, potential risks can be determined together with the associated probability and impact of each risk. A first step to do this, is to ensure proper process mapping and good governance of these. This is key since it highlights what activities are performed, what resources are required and where dependencies exist. Furthermore, it shines light upon which processes that are the most crucial for the business to operate as well as the maximum tolerable downtime that can be accepted for each process. Our experience is that larger companies tend to have clear responsibilities and ownership within the organization, but struggle with extensive process mapping, often in many different versions where some may be incomplete and some outdated. Smaller companies tend to have fewer processes, which makes it easier to keep these up to date, but struggle with assigning clear and consistent roles and responsibilities.

Do not: Map all processes at once or map the process at a too detailed level.

Do: Identify and agree upon the essential processes, assign ownership and begin by mapping these processes according to a predefined template.

Risk assessment – Understand your risks

Ensure that results from risk assessments come to use. Organizations tend to see the risk management process as done when risk assessments are finalized, or only act on the most prominent (or easily mitigated) risks. To reduce risk, controls and mitigation actions can be implemented in many different parts of an organization and range from purely technical mechanisms (e.g. security monitoring and vulnerability scanning) to more qualitative measures (e.g. educational efforts, establishing a security function, reviews and audits). All of these have different impact on the organization's resilience, based on what kind of control it is and where it is implemented. The key of deciding on what to implement is to understand a) what are the company's critical resources and b) what are the threats and vulnerabilities that needs to be mitigated from a resilience perspective. An organization that is not aware of its critical resources and associated risks, can be challenged with an overflow of controls and arbitrarily "mitigating" actions. Not only does that produce an unnecessary administrative burden and consumes resources, but it can also create a false sense of security. Understanding risk is therefore essential to be able to prioritize between different actions and ensuring operational resilience. A thorough risk analysis together with a proper process mapping will provide valuable and necessary insight to define relevant, potential scenarios and the corresponding risks of each scenario.

ÖSTERMALMSTORG 1, 5TR
SE-114 42, STOCKHOLM, SVERIGE
FCG.GLOBAL

Do not: Hurry through risk assessments or leave results unused.

Do: Analyze what the risk implies for your organization and how well existing controls mitigate risk from a resilience perspective. Analyze what it would cost in a short- and long-term perspective, both in terms of impact and cost of mitigation.

Governance – Ensure a maintainable governance model

To maintain operational resilience, an organization must ensure that fundamental activities such as process mapping and risk assessment are performed consistently and improve over time. A governance model should be proportional to the organization's size, and it should clarify responsibilities and ownership. Easy at it sounds, this is often where organizations halter, small or large. Unclear ownership and responsibilities as well as overly complicated processes are common and could easily turn into a source of frustration and even have demotivating effects on innovation and change.

Do not: Create an overly detailed governance model.

Do: Focus on assigning clear ownership for processes, risks, systems, etc. and keep the governance model as simple as possible to be able to maintain and adjust it over time. If there is no governance model in place, it is better to start somewhere than to include every detail at once.

In conclusion, there are many ways to build and maintain an operationally resilient organization. The examples mentioned above might seem straightforward but tend to consist of more work and difficulties to implement than initially thought. Operational resilience in itself is not new, and every organization has processes, methods, competence and other tools in place to start from. An overall recommendation is to use these structures and already existing competence within the company instead of recreating everything from scratch. Lastly, operational resilience cannot be achieved without being on the board and management's agenda. There has to be a strong and pervasive risk culture and risk management framework approved by the board to be able to work continuously with operational resilience, as managing risk is core in the process of establishing resilience.

Visit www.fcg.global for more insights

ÖSTERMALMSTORG 1, 5TR
SE-114 42, STOCKHOLM, SVERIGE
FCG.GLOBAL