www.pwc.ch

Operational resilience

Your Swiss army knife to survive the next crisis

pwc

“Operationally resilient business services provided by firms and financial markets infrastructures directly support resilient economic functions, enabling people to buy goods, borrow money and markets to transact. Resilient business services therefore support financial stability.”

Joint paper from FCA,
Bank of England and PRA

Table of contents

Some good reasons to read this document

At PwC, we define operational resilience as "an organisation's ability to protect and sustain the core business services that are key for its clients, both during business as usual and when experiencing operational stress or disruption." It is a broad definition, and as such operational resilience is prone to become just another buzzword in the business world. However, it is much more than that – and we try to unpack what operational resilience really means in this document.

We know your time is valuable, so you can find here a summary of what to expect in the document – and what value each session may bring to you.

Section	Good reasons to read the section
Why does resilience matter?	If you have read countless times why resilience is important to the business and what it really means, you can skip this section. If that is not the case, reading this section will give you a better understanding of: ▪ What does it mean – in specific terms – to be operationally resilient? ▪ What happens when organisations are not resilient? ▪ What are the drivers behind the movement towards operational resilience? ▪ What does the regulatory agenda look like when it comes to resilience?
The client is king	The most important step to becoming more resilient is understanding the areas of your organisation on which you should focus. Some people may have a good idea of what products and services to focus on, in which case you can skip this chapter. If, instead, you find yourself struggling to understand where to focus your resources, reading this section will help you to answer the following: ▪ Where should your starting point be when defining your path to resilience? (spoiler: it's your clients) ▪ How do organisations fail when it comes to defining the correct starting point? ▪ How does working on your resilience help to put the client at the centre of your organisation?
The operational resilience Swiss army knife – a framework for resilience	As we delve more deeply into the topic, it is essential to explain what the key components of a framework for operational resilience are (which we describe using the analogy of a Swiss army knife). In this section you'll find our methodology and our answers to some very specific questions: ▪ What are the building blocks (i.e. existing frameworks and methodology) for achieving operational resilience? ▪ What are the components (or foundational DNA) of an operational resilience framework?
The approach to operational resilience	As our framework leverages your existing frameworks and methodology, we try to highlight here how everything can work from a holistic point of view. This section will answer two very fundamental questions: ▪ What steps should your organisation follow to achieve operational resilience during business as usual? ▪ What governance structure should you give to a newly established operational resilience function?
Does it really work?	We appreciate this is a topic that may sound quite intangible, which is why we have added this final section. Here you will find answers to the following questions: ▪ How has PwC actually implemented this? ▪ How can PwC help you to achieve operational resilience?

Why does resilience matter?

Resilience has recently become the latest global hot topic in many industries, including financial services. As many major companies still rely on old, complex and silo-structured IT landscapes and operate equally outdated and disconnected processes, achieving operational resilience has become a crucial goal for companies looking to survive the next crisis. Moreover, customer needs – in any industry – are ever-changing, and many organisations have often used a tactical approach to meet such needs, instead of strategically considering how to integrate new processes and services into their business in a holistic way.

Five key drivers to build up operational resilience

We see many organisations moving towards operational resilience. There are 5 main drivers behind this trend:

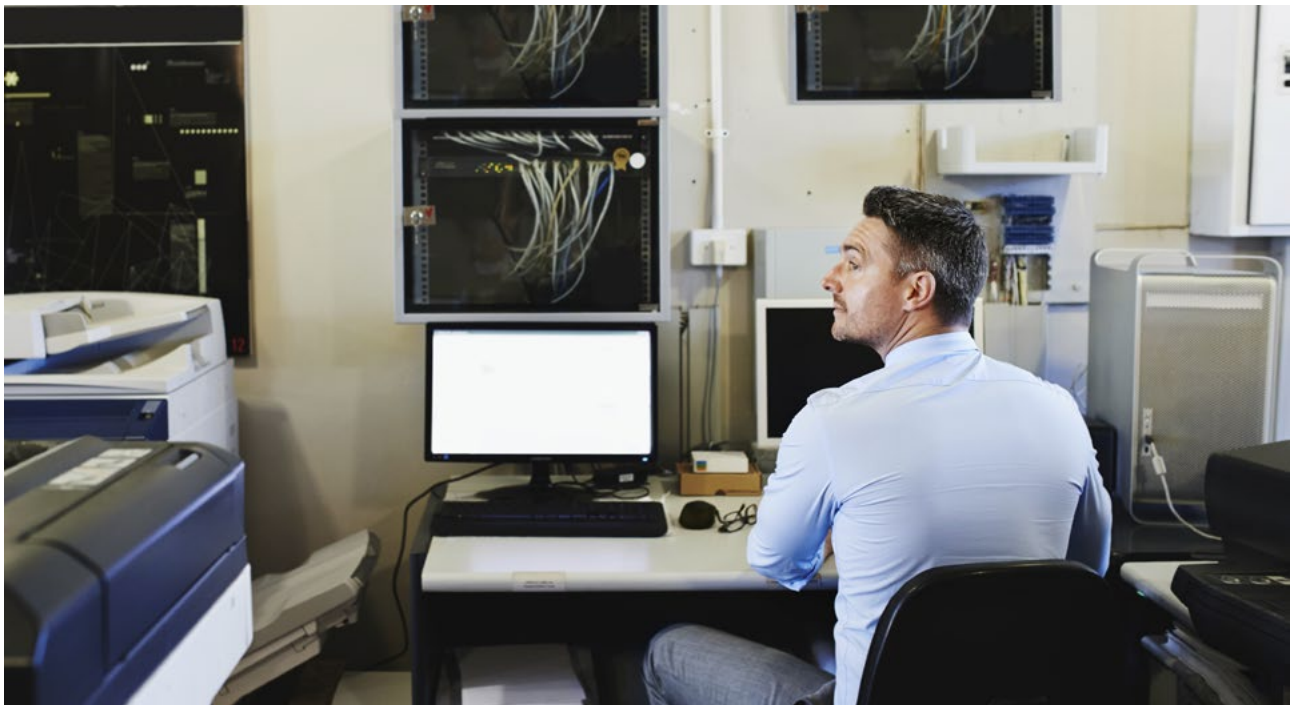
1. **Higher customer expectations with regard to 24/7 availability:** Delivering a service that is always robust and responsive in the event of issues is both the minimum customer expectation and also a necessity for building and cementing the trust between organisations and customers.
2. **Increased sophistication of cyber threats:** Organisations have widely benefited from technological innovations. However, technology has enabled the creation of cheap but effective cyber weapons, the use of which has unpredictable consequences.
3. **More severe natural disasters and extreme weather events:** Over recent years, we have witnessed climate change that is associated with extreme natural events. If either your organisation or your clients are global, you will be affected by such events. Are you prepared to serve them under "any weather conditions"?
4. **Higher risk linked to internal change failures:** Increasingly sophisticated systems are being used across application development and infrastructure change. Higher sophistication is translated into elevated risk and relative potential impact, both financial and operational, in the event of internal change failure.
5. **Increased regulatory scrutiny:** In the aftermath of the last financial crisis, the financial services sector is evolving into a highly regulated landscape, with the primary goal to protect the client. An organisation that is not operationally resilient may find itself unable to respond appropriately to an increasingly demanding regulatory landscape.

Necessitated by these factors, among others, many organisations have started building up their resilience capabilities, and regulators have started investigating this area for the first time.

> Financial institutions face an increasingly complex threat landscape and risks associated with their own digital innovations. This calls for operational resilience to be viewed as no less important than financial resilience.
>
> **Kuangyi Wei,** Parker Fitzgerald, 2019

Operational resilience is critical to modern organisations

"Bank customers hit by dozens of IT shutdowns" – so reads the title of an article from the BBC, dated February 2019. As some banks have started publishing the number of incidents they have experienced, a worrying image emerges: "major banks typically suffer well over one outage per month". This should come as no surprise, as many major banks still rely on outdated, siloed IT systems, linked to a myriad of processes often disconnected from each other. Even banks that have invested in major IT restructuring programs have still maintained a large part of their legacy systems, legacy problems included. We all have happily welcomed the technological innovation brought to the financial sector from the Fintech revolution; however, this has also meant increased complexity in banking systems, leading to reduced resilience to stress events.



Operational resilience goes beyond cyber resilience and IT infrastructure, and has a clear impact on the organisation's P&L

Furthermore, companies often focus on the IT aspect of resilience and disregard an equally important component: the processes and people that are crucial for the delivery of the final product or service. Operational resilience needs to encompass all areas of a business in order to be successful, and cannot be limited to IT (or cyber/digital) resilience. It has to encompass building blocks that include your risk frameworks and other important processes and methodologies that you are already applying today. Failing to do so, would result in a fragmented approach, limited to one or few specific functions, and as such insufficient to support the final goal of achieving resilience across the entire value chain.

Furthermore, in most cases companies highlight the benefits of resilience from an operational perspective, while ignoring or underestimating the opportunity cost and impact on the financial results. The interruption of a key service even for a short period leads to broken customer trust, customer distress and severe reputational damage. Operational resilience is strongly focused on the client needs and sees this as an opportunity for an improved financial performance of the organisation. In the dictionary of resilience, compared to "classic" risk management and recovery and resolution planning, the focus is shifted from "if" to "when" the disruption will occur.

Starting from the above and leveraging several examples of operational failures within the industry (with strong negative impact on P&L), an organisation can clearly demonstrate how investments in resilience can positively contribute towards the P&L – as it supports cementing customer trust by "always keeping the lights on" and by protecting the organisation from potential reputational damage.

The positive outcome in the P&L is derived from three main sources. In the first instance, we find a positive impact on costs, as operational resilience will enable a company to avoid unexpected financial losses derived from adverse events. The second factor is related to the impact on the profit side: serving the client continuously and seamlessly will result in increased revenues. Also in relation to profit, the increasing stakeholders' and investors' confidence could bring enhanced financial support and opportunities. Finally, resilient organisations can respond efficiently and in time to regulatory requests and therefore avoid potential fees and losses.

When one looks at these three factors together, it is clear how resilience enhances the P&L of an organisation from both the profit and loss side, and by doing so it can be a key driver in improving the financial performance of the organisation.

Many organisations are facing issues that could be avoided with an adequate level of operational resilience

Note that financial services companies are not the only ones relying on old and siloed systems, resulting in limited resilience capabilities: many organisations are facing big or small resilience problems, and it is also important to notice that stress events are not always generated by external attacks. In March 2019, Facebook suffered its longest outage to date (lasting for almost a day), which affected not only the social network but also other platforms owned by the company. In the aftermath of the event, Facebook blamed a "server configuration change" for the outage – which translates into the fact that even a modern and technologically-savvy company like Facebook is not resilient enough to maintain its key service during a server change. Clearly, resiliency problems are not limited to companies having to operate within old IT legacy systems.

The regulator lens of operational resilience

Furthermore, regulators have started to take a closer look at the matter, having realised how essential operational resilience is for a healthy marketplace. Many organisations today provide services that are vital to their customers: ensuring those services are maintained is not only in the interests of the organisations themselves, but also in the interests of the community.

In July 2018 PRA[1], FCA[2] and the Bank of England published a discussion paper on how to improve operational resilience within financial services firms. Similarly, the BIS[3] set up a Working Group on operational resilience and at the end of 2018 published the paper on cyber resilience, in which it also considered practices relevant to the broader operational resilience context. The European Central Bank has also started to focus on the topic, and has established a Euro Cyber Resilience Board for pan-European financial infrastructures. Understandably these bodies are focusing on cyber resilience, since the ramifications of both deliberate and opportunistic cyber events can be systemic, when they impact a company's strategic assets which are critical to the wellbeing of the overall market.

It is also important to mention the EBA[4] speech on the regulatory framework to mitigate key resilience risks. In the document, it is specified that "while some pieces of our work are still in the pipeline, the regulatory and supervisory framework related to operational resilience is built around the following three areas:

- Regulation: strengthening governance and risk management arrangements
- Supervision: common framework for supervisory assessment and knowledge sharing
- Resilience testing: sound and proportionate resilience testing."

To conclude, both companies and regulators agree that resilience is a fundamental aspect to any organisation. Still, many are left with an open question: what exactly is operational resilience, and how can an organisation be made resilient? While not an easy question to address, we believe it is important to build a strong foundation by starting with the basics.

Wells Fargo says it is working to fully restore systems as outage spills into day two

Liz Moyer, CNBC, 2019

CEO Tim Sloan says the recovery from the outage was not as fast as the company or its customers expected. Contact centers were up and running but customers faced longer wait times if they were phoning in.

Complaints piled up that paychecks and direct deposits weren't reflected in customer balances.

Root of the issue

The company was not quick enough to recover from the outage, causing distress to the customers.

How operational resilience would have helped

Fast response in incident management is vital, such as immediate back-up activation. With operational resilience, preparation, maintenance and testing of such incident responses are given the attention they deserve.

Ballot box not hacked, errors in the source code – Swiss Post temporarily suspends its e-voting system

Oliver Flüeler, Swiss Post, 2019

Researcher discovered that a central element of the new E-voting system had not been programmed correctly.

Root of the issue

The known gap was not addressed adequately, as the revised code component still contained vulnerability.

How operational resilience would have helped

When addressing a risk, it is important to ensure that the remediation effectively mitigates the risk. An important part of operational resilience is testing the remediation processes in place, thereby assuring quality and fast response in case of issues.

Banking on operational resilience

Editorial, Times of Malta, 2019

The cyberattack that temporarily disrupted Bank of Valletta services showed how important it is for banks to anticipate the consequences of such attempts and to have plans in place to restore services as soon as possible.

Root of the issue

Hackers were able to break into the bank's network.

How operational resilience would have helped

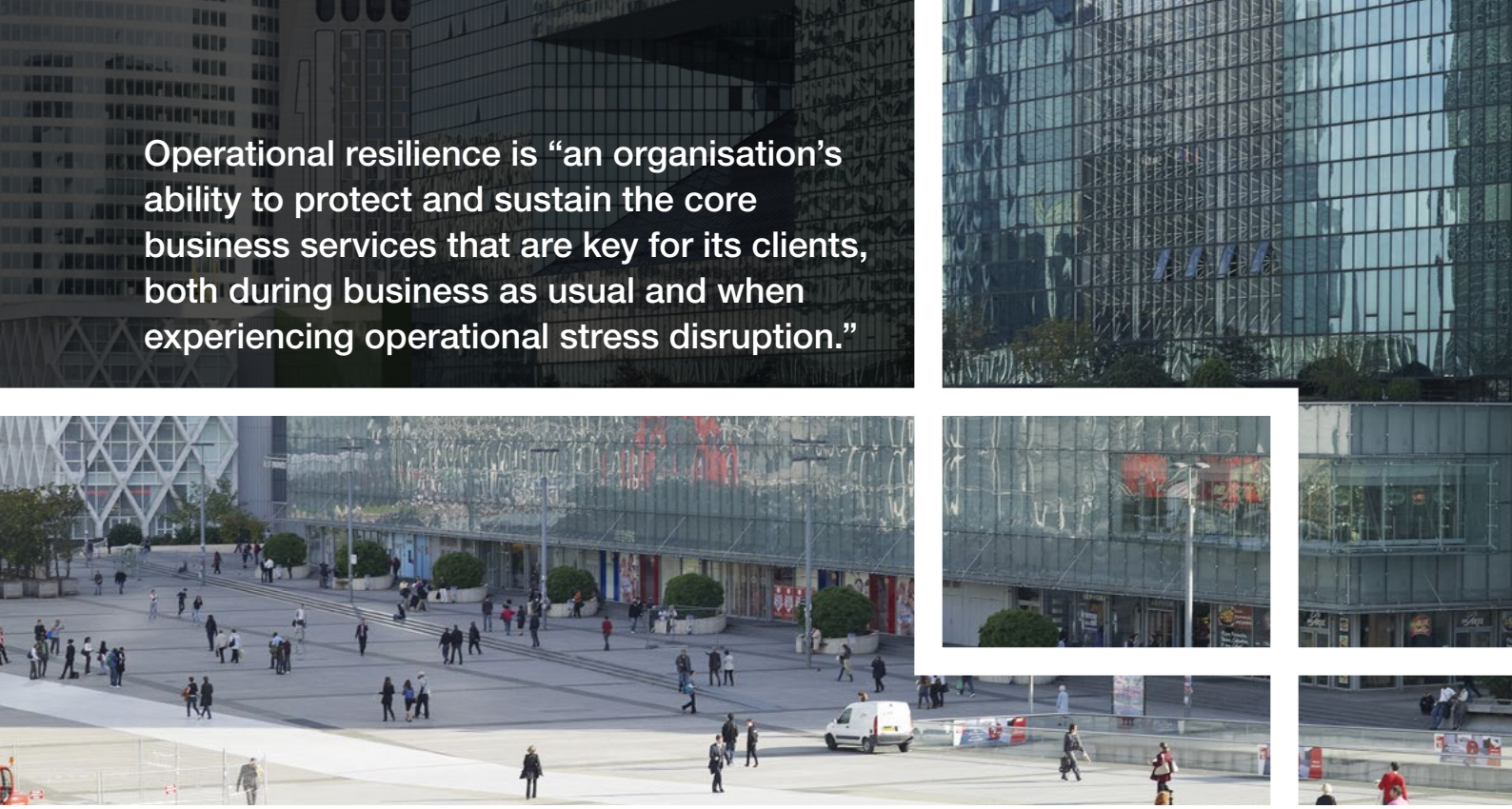
Cyber resilience incl. cyber security are integral parts of the operational resilience framework, providing a forceful countermeasure against cyber crime.

[1] PRA stands for Prudential Regulation Authority – link to the joint discussion paper: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

[2] FCA stands for Financial Conduct Authority

[3] BIS stands for Bank for International Settlement – link to the report: https://www.bis.org/bcbs/publ/d454.htm

[4] EBA stands for European Banking Authority



Operational resilience – what does this really mean?

Take your smartphone and google “operational resilience” – you will find a number of different definitions and respective frameworks, which are not always coherent with each other.

Trying to summarise the essence of what it truly means to be operationally resilient is a hard task, as being resilient entails a very long list of characteristics. Given the complexity of the topic, many have tried to define resilience by focusing on specific areas and, for this reason, most attempts at defining operational resilience are necessarily biased (e.g. you may end up focusing on cyber resilience, or on the risk management aspect of building up resilience).

Moreover, operational resilience is moving towards a broader “business resilience” definition – organisations need to start looking at this topic as a key driver for their entire business, and not just as an operational matter. Resilience (be it “operational” or “business”) is a key strategic topic, which goes beyond what may appear to be a “back-office” kind of problem, and it should be given the attention it deserves in any modern organisation. We see that resilience is normally discussed at Board level, and we recommend that a programme to achieve operational resilience should be mandated by the Board, as this would support a unity of purpose through an overarching strategy for resilience.

At PwC, we have tried to look at the very core of operational and business resilience, and – from our experience – we have seen that resilience is best defined from the perspective of the client, and by looking at key business services end-to-end. With this in mind, we structured our definition of operational resilience as “an organisation’s ability to protect and sustain the core business services that are key for its clients, both during business as usual and when experiencing operational stress disruption.”

Our experience has shown that an effective framework for operational resilience should cover – at the bare minimum – the following elements, if the bias across the key business services is to be avoided:

- the capacity to adapt and respond to stress scenarios
- the ability to maintain the key services for clients in any situation
- the capability to retain critical management activities that will allow the organisation to preserve its obligatory requirements for operating (e.g. maintain the licenses needed to operate)
- the willingness to learn from past mistakes so that they won’t happen again
- the ability to train and prepare your staff to manage difficult situations
- the capability to build efficient communication channels throughout the organisation
- the eagerness to embed a proactive culture when it comes to managing operational needs, threats and risks (as opposed to the more common reactive approach to risks)

These are high-level principles to keep in mind when approaching operational resilience in your organisation: embedding these principles in your day-to-day business, governance, culture and operating model will be the starting point for increased resilience. In this paper, we will use our experience to break down those principles into an actionable plan for organisations wishing to build their framework for operational resilience.

To answer the original question of this chapter, it is essential to understand that operational resilience is not “yet another buzzword” in the management world, but rather a very important set of characteristics that your organisation ought to have in order to survive in the ever-changing modern world and the next crisis.

The client is king

A crown-less king

In any industry, there is one single factor that – more than anything else – can lead to the success, or to the failure, of a company: the client. This is not new, and it means that any strategy should have the clients' needs at its core in order to be successful. And yet many companies repeatedly fail to focus on their customers. It is not for lack of awareness, but because other priorities often enter the agendas of key stakeholders in the organisation, starting from the C-levels. CEOs need to deal with a constantly evolving regulatory environment, an increasingly demanding work force, market instability, increasing prices, new technologically advanced competition, and many other things. Many of these items are automatically assigned higher priority (e.g. you need to comply with the new regulation now, you need to find a new provider today, you need to answer your employees' request by the end of the week). This often results in companies focusing on what is urgent and burning, rather than what is most critical to build up operational resilience – which is, as simple as it sounds, the client.

This "non-client-centric" set of priorities is then cascaded through the organisation, and all key stakeholders in a big company often find themselves dealing with a number of priorities, completely disconnected from what their clients need.

Focusing on the client is not just important from a simple "business" perspective (you can't really sell something the client does not need), it becomes of utmost importance when talking about operational resilience. When you put your clients' needs at the centre, you can understand what are the key services, products, processes and systems that you need to focus on. And you can leverage the information collected while building up operational resilience to prioritise your investments accordingly.

How did the client lose its crown?

Over time, changes in the nature of the market and in the regulatory environment have resulted in companies adopting more complex business and organisational structures. Let's take the example of a bank: when the first "modern" bank was born (it was in Italy, in 1407), it focused on one business, lending money to governments. That required a limited breadth of skill sets and resources to manage (an initial capital, someone who knows how to keep records of the banking book, someone who can manage the lending process, etc). Focusing on the client (the governments that needed financing), was fairly straightforward.

The concept of the bank has evolved since then: multiple products and services are now offered to a vast range of clients, located in different countries and interacting with the bank via different means (email, phone, internet banking, traditional branch). Not only has the offer diversified, but the environment in which the banks operate is now more complex, with stricter regulations (Basel, MiFid, data protection, to mention just a few) and more volatile markets. An organisation cannot simply focus on "how can we best serve our clients", but has to answer hundreds of other questions before it can even get there. These range from "how can we comply with the banking regulations in Brazil?" to "how can we protect our investments in the UK from a potential negative outcome of Brexit?"

Your client is your most important stakeholder and your operational resilience framework needs to be tailored to its needs and the offered services/products.

Understanding what your clients need is the first step for operational resilience

It is important to notice that clients' expectations have evolved over recent decades. Here are some of the most crucial aspects that organisations should consider:

- In many industries, customers today expect a service that is fully functional on a 24/7 basis.
- While expecting an "always available" service, clients also require that organisations take into consideration their specific needs – whatever the product offered, this should be continuously available and highly customisable.
- An enormous amount of data is exchanged between clients and organisations, and customers are today more and more aware of the value of such data. As such, they expect organisations to adhere to minimum standards regarding the security of such data. Clients today are constantly informed of new trends and technologies – almost in a real-time fashion. The expectation is that any organisation would keep up with the most recent development, and clients are often ready to move to a more technologically advanced competitor if they see that their company is "resistant to change".

Note that – adding to the more sophisticated clients' need – there is an even more important consideration to make. Thanks to the power of the Internet, a minor disruption of a strategically important service may become viral in minutes, and cause major negative consequences to any organisation. For this reason, it is important to clarify what your clients really need and value – and ensure that such products or services are resilient in time.

An operationally resilient organisation can give the crown back to the client

Different key stakeholders are responsible – together – for ensuring that the client is consistently at the centre of the organisation's strategy; however, they are often led by very different objectives. The CEO needs to steer the ship, keeping in mind the profitability for the shareholders. The CIO is often confronted with cost-cutting in IT while being requested to maintain up-to-date and efficient systems. The COO is confronted with regulatory constraints and growing business needs, which constantly put operations under pressure to deliver faster, more accurate and less expensive outputs. The CRO in a financial institution needs to ensure that risks are well managed, with adequate capital buffer, but also has to save as much capital as possible.

Every single priority is obviously important, and organisations need to focus on all of them. However, what normally happens is that every stakeholder looks at this from a siloed perspective, without considering the higher view (client is king). Having a function that sees things holistically and tries to consolidate priorities under the assumption that the clients' needs come first, is the first step towards a more resilient company.

It might be argued that, if you set up your company in the right way from the start, with the client at the centre, things should work out fine. Indeed, most companies that are successful today are in this situation because they did effectively put the client first – in their early days. However, quite often, the client-centric structure of any company changes over time, to the point where the clients' needs are only a small factor in a very complex mechanism. Where are the clients' needs in the agenda of a CEO, CIO, CRO, COO?

Note that the risk of losing the client focus is especially real for successful and "status-defining" brands: when you know your clients will keep buying your products or services no matter what, it's easy to focus on more burning priorities – be it cost-cutting, or regulatory response – rather than on what your clients need.

The operational resilience Swiss army knife – a framework for resilience

Bringing it all together

Nothing in the operational resilience definition should sound new – focusing on what matters to the client, ensuring the company can withstand changes and recover from stress events: these are all obvious goals for a successful company. However, these can also remain intangible objectives, too disconnected from reality. It is hard to measure "adaptability to stress", while it is very easy to quantify how much profit a company has produced by year end.

Leveraging our experience, we have created a framework that supports a pragmatic approach to operational resilience, to make it more tangible and – ultimately – measurable for your company. The first thing we need to present, from our framework, is the tool needed to make it work – we like to call it the "operational resilience Swiss army knife". For us, being resilient is equivalent to having a flexible, "easy-to-reach" unit , a tool to help connect the dots across the different frameworks you already have in place. All the frameworks can then be regarded as part of a bigger tool – this helps to understand how our methodology can support you in moving from a siloed approach (where all frameworks are disconnected) to a more holistic and integrated one.

You may think of the framework for operational resilience as being your company's Swiss army knife. As a first step in the framework, we are identifying the key functions, processes, frameworks that you are already using in your business, and leveraging them into a framework that focuses on serving the client in an ever-changing environment.

What we advocate is that you start using those frameworks with a "customer lens" instead of a "process lens". You can do so by developing a proactive approach to your clients' needs, which translates into ensuring that client needs are constantly and seamlessly met (leveraging your existing processes, systems and resources). Note that many organisations are already partially doing this via their recovery capabilities, however that is just one side of the resilience equation: being resilient should also include newly developed "protective" capabilities (i.e. resilience needs to focus on being proactive to possible stress events, rather than simply reactive).

We are not advocating rebuilding the entire corporate structure, but instead ensuring that the key components of the organisation always work together with an ultimate common goal: that of restoring the crown to your clients.

Every organisation needs six pillars in place to achieve operational resilience

There are six pillars that need to be in place in every organisation in order to ensure operational resilience. These also define the level of maturity of operational resilience in your organisation.

01

Define the framework to achieve operational resilience

The framework has to be current, communicated and understood by the organisation. It is in place across the entire organisation, with clear definition and accountability for the different aspects of resilience.

02

Embed operational resilience in the governance structure

The Board and Executive Management have accurate and adequate oversight of resilience activity, trends and remediation, which empowers them to make the correct investment and risk decisions.

03

Ensure effective capacity management

Through testing and monitoring, organisations can demonstrate the effectiveness of capacity management.

04

Strengthen the management of own risks

Managing risks adequately is a key prerequisite for resilience, as the easiest way to withstand a stress is by reducing its impact. Managing the risks of a stress event entails splitting responsibilities into separate lines of defence and ensuring that all lines contain elements of resilience.

05

Enhance resilience capability and agility

The organisation has sufficient skills, resources, agility and clear understanding of roles and responsibilities to deliver and help ensure operational resilience.

06

Promote a culture of learning and continuous improvement

Encourage your organisation not only to anticipate, but also to learn from adverse events affecting your organisation, collaborators or competitors. Continuously improve your framework and evolve more strongly from these events.

The building blocks of a successful framework for operational resilience

The framework for operational resilience can support building up resiliency in every organisation. In the graphic below, we highlight which existing frameworks and methodology should be used in the journey to achieve operational resilience. These are essentially the building blocks of the framework that – based on our experience – can successfully lead to increased resiliency. The next table highlights in more detail the purpose of each one of the building blocks.

Framework for operational resilience – building blocks	What is the purpose of the building block?
Digital resilience and service operations	Digital resilience ensures that your digital processes and systems in the value chain of your core products and services are always on, and that vital technologies are not disrupted by newly introduced systems. Therefore digital resilience can act as a driver behind the digitalisation of processes with the successive digitalisation of systems. In the era of digital transformation, blockchain and AI, digital resilience is vital to maintain a competitive advantage.
Data resilience	Most industries today are extremely data-intensive. Ensuring the quality and availability of data is vital if you want to be resilient. Data resilience is also about knowing what data is critical to provide the key services and products to your client. In order to have this clear view, data inventories and data flows become indispensable. Being data-resilient starts with appointing a CDO (chief data officer) whose goal is to ensure the CAVR (completeness, accuracy, validity and restricted access) of the data supporting your key processes.
Cyber resilience	Cyber resilience mechanisms to prevent, detect, respond and recover from cyber-related threats should be in place, aligned to the wider response and contributing to recovery capabilities.
Sourcing and external dependencies	Sourcing and external dependencies (including TPRM – Third-party risk management) serve to ensure that key services to the clients are maintained. This is key to understanding dependencies of such services on third parties, and to managing the respective risks adequately.
Business strategy	Business (and corporate) strategy defines the commercial objectives and social licence to operate – in other words, it identifies what matters the most to your business. It drives strategic decisions on operational resilience investments and risk appetite levels.
Incident management	Incident response processes are in place to identify, classify and to help ensure appropriate, measured responses, in order to recover from any stress with the minimum impact on clients.
Crisis management	Organisations should try to anticipate risks and stress scenarios in order to avoid them. However, a crisis might still happen due to un-expected events, in which case it is essential to ensure proper management of the situation with a view to restoring business as usual in the shortest period possible.
Operational risk framework	Operational risk framework is used for understanding, classifying and mapping business risks across the delivery journey of core products and services. Understanding and quantifying the exposure of your key processes with KRIs is essential in order to remediate resilience gaps and interdependencies.
Change management	Well governed, documented change processes that are in place and are fully understood by the organisation ensure that resilience is embedded in change control and SDLC (software development life cycle) activity.
Continuity management	Continuity management: having a structured and formal plan in place to ensure that business continues in case of stress events is a key building block for resilience (including contingency plans).
Physical security and facility management	This is not limited to access control – an organisation should ensure that its key locations and facilities are protected from external events and that actionable measures are in place in the event that the security, the availability or the usability of any of those locations and facilities are compromised.

Focus point: special considerations for TPRM

The general trend within the industry is to outsource services to external providers resulting in benefits such as higher efficiency and quality, and lower costs. On the other hand, companies are facing higher risks in different areas such as compliance, legal, reputational, operational and information security risks, which are closely linked to operational resilience. This was also recognised in recent years by regulators and as a response the regulations have been increased significantly (e.g. FED (OCC), EBA, MAS). Here are a couple of examples:

- Fourth-party risk management: under TPRM, organisations try to have a low concentration risk when it comes to service providers by using different vendors where possible. Furthermore, organisations have to ensure that their third parties comply with any legal requirements (e.g. they are not located in sanctioned countries). This is not sufficient as your provider may use a subcontractor, which may result in a high concentration risk (if different vendors rely on the same subcontractor) or – worse still – in a breach of legal obligations (e.g. if the subcontractor is in a sanctioned country).
- Dynamic TPRM: it is important to move away from the static view of TPRM. An easy way to explain this is by talking about certification checking. Quite often, a provider needs to present some sort of risk/control certificate (e.g. ISAE or SOC reports) in order to provide a certain service. In these cases a check is done at the beginning of the relationship, but quite often is not done again afterwards. However, it is important that the vendor is monitored throughout the entire vendor life-cycle – starting with the on-boarding, through continuous reporting and monitoring, to off-boarding/termination. Aligned to the concept of operational resilience, TPRM could be used as a living methodology throughout the value chain rather than as a simple check-box at the beginning of the relationship.

Success factors to achieve operational resilience

Before building operational resilience in your organisation, it is essential to understand which factors make up a successful framework:

1. **Appropriate level of sponsorship:** this should be at executive committee level, giving operational resilience the attention it deserves.
2. **Dedicated function:** with direct reporting line to the CRO, COO or CEO (these three different models are explained in the focus point in the next pages), you should seek expertise and knowledge from all the elements of operational resilience – processes, technology, data, people, premises and third parties.
3. **Dedicated programme:** with clear governance and deliverables, driving operational resilience in a holistic manner.
4. **Communication and change management:** these are integral components for building operational resilience. Clear internal communication about why operational resilience is required, what needs to be done and how to address it is essential.
5. **Strong data analysis and integration:** which is based on consistent and ongoing data gathering, in order to understand how a failure in one system could create a butterfly effect. This data is gathered from the back end (key processes/systems) to client feedback and demographic changes; the operational resilience function should be able to use and translate insights from such data into the business strategy and vision.

Building operational resilience

Find the right people with the right skills and establish a team. Define a clear scope for the operational resilience function and programme, set objectives and define interactions with other existing teams. Collect and consolidate data from well-established frameworks, processes and controls (e.g. risk framework, cyber security framework) to:

1. **Identify overlaps:** in order to eliminate silos and bring together functions, knowledge and expertise with one goal – to drive efficiency and resilience.
2. **Identify the connections:** among the threats and risk mitigation measures across key processes. Leverage the best practices and ensure consistency.
3. **Ensure improvement:** and follow up on any changes and materialised events. Implement operational lessons learnt not only from your organisation, but also from your competitors.

The approach to operational resilience

The operational resilience function is key to restoring your client's crown

Once the components of the operational resilience framework are clear, the typical question we receive from our clients is: where do we start? How do we make this tangible? And, more importantly, is operational resilience a new capability to cascade to existing functions, or is it even a new function at all? We believe organisations should set up a new, separate function, and we explain here why.

As mentioned in the previous chapter, we understand that modern organisations have a number of different priorities, often incompatible with each other. Every key actor in a big corporation has his/her own agenda, and might have a hard time adjusting to a newly defined set of priorities. As such, the option of simply cascading a new capability to existing functions can not help solve the problem of having disconnection across those functions.

For this reason, we advocate that the first step you need to perform to achieve operational resilience is to create a dedicated function in your company, with a clear mandate, objectives and roles and responsibilities. By formally defining an operational resilience function, you are also giving out a strong message: that resilience is of great importance to your business, and that you are prepared to dedicate the necessary resources to it.

Such a function should have direct and appropriate reporting to a senior executive, its own budget, and a clear agenda: to ensure that the products and services that are key to the clients are always maintained, including during periods of operational stress or disruption. Note that this also includes the capacity to maintain the core services when it's the business itself that is changing (e.g. if the company is deploying a completely new online portal for web-based services. How do you ensure a seamless transition to the new website without creating any negative impact on the client?).

This function should be able to work in close collaboration with all the other key functions in your organisation, and should be able to influence their agenda in order to reach the final goal: that of putting the client at the centre of your operations.

Starting from building up a clearly defined operational resilience function will help you establish some prerequisites for achieving increased resilience:

1. Defined **governance,** with clear roles and responsibilities assigned to the function and across your organisation.
2. Ensured **oversight:** the new function should have a role in the centre between your front-end and your control functions. Your existing frameworks are vital for achieving resilience; however, you need a central function to oversee your key processes and ensure that they are not managed in the old "siloed" way.
3. Structured **communication** across functions. One of the reasons processes are often managed in silos is that different functions tend to "speak different languages". The operational resilience function should facilitate adequate communication between different functions and ensure that the right information reaches the right stakeholders in a timely manner during periods of stress.

Once you have set up a function, you can start implementing the next phases to ensure your organisation becomes operationally resilient, and as such prepared for the next possible crisis.

Focus point: where should the operational resilience function be positioned in your organisation?

The first and most important step to achieving resilience, is to build a function that could maintain the necessary holistic view of your frameworks and methodologies. This function could ensure that all the eight steps described in this chapter become part of your organisation's DNA, and will help you build your operational resilience.

In our experience, we have seen that – depending on the needs of your organisation – the operational resilience function can report to different existing functions. In general, we are seeing a shift in the market from a model with operational resilience built into the second line of defence (reporting to a controlling function, e.g. CRO) to a model where the accountability is shifted to the business and operational resilience belongs in the first line (e.g. reporting to COO).

Here are some examples of where such a function may report, depending on what matters the most to the organisation.

Model A: Direct reporting line to the CEO

Considering the strategic importance of operational resilience, this seems to be the most appropriate solution. Especially if your focus is on the products and services, and you want to ensure operational resilience becomes an integral part of your company strategy, this might be the appropriate governance decision for your company.

Model B: Direct reporting line to the COO

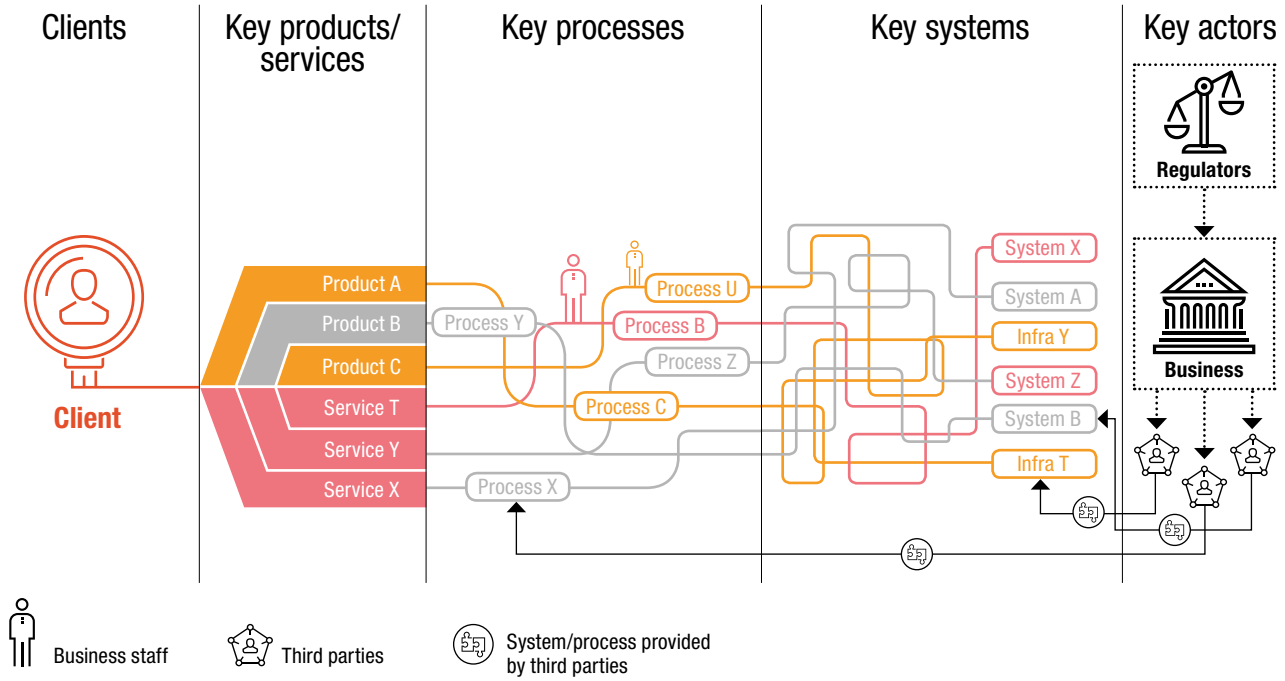
Operational resilience obviously has a strong link to an organisation's operations management. Your COO is probably the function that knows best how your systems, processes and people interact with each other, in order ultimately to offer the products and services to your client. Positioning your operational resilience function in this area would ensure that the right knowledge on how your organisation works is available and "ready-to-use".

Model C: Direct reporting line to the CRO

Operational resilience is closely interconnected with risk management. Many synergies exist naturally between any risk management framework and any operational resilience framework and methodology. Therefore, if your focus is more on managing risks, you may consider positioning this new function under the CRO area.

The eight steps to resilience

0	1	2	3	4	5	6	7	8
Know **your clients:** who are your key clients, what do they need?	Identify the **products and services** that are key to your clients	Identify the main **processes (and staff)** linked to the core business and identify dependencies (existing or in design phase)	Identify the main **digital systems,** infrastructure and **data** that support these core processes (existing or in design phase)	Identify which **third parties** are involved in the value chain of these key products and services	Identify adverse scenarios that can impact these processes and systems **(threats)**	Identify **risks** that can impact these systems and process (apply risk framework)	Expand **incident management** to learn from materialised risks to systems and processes	Measure the **performance** of your processes and systems (KRIs)



Start with the client

Resilience is about being able to maintain the level of service even in stress situations. Ideally, an organisation should be able to maintain its business-as-usual activities at any point in time, yet we all understand that is not realistic, as mistakes happen.

As may be expected, the first step in building up resilience has to be to identify the products and services that are really key to the clients. But before that can be judged, there is a more fundamental question to ask: who are the clients of an organisation? Which ones are its key clients?

Organisations may consider every client to be equally important. But one may consider the possibility that certain client groups or types are "more important" for the business due to the type of offers, products or level of services provided. In a situation where servicing capacity is limited, you may want to prioritise focus on certain types or groups of customers.

1. What do your clients really need from you?

Whether or not you have decided to segment your client population, there is another important question to ask: what needs to be maintained "no matter what" for your (key) clients? If your organisation is a bank, these products may include eBanking and online trading, while an insurance company may want to ensure 24/7 phone support to clients who have had accidents. We will discuss here possible ways to build resilience, starting with the example of the insurance company's telephone helpline.

Please note that this step needs to be taken once for all existing products and services, while it should become a standard question when defining new products and services or when changes are planned within the value chain (**change management** and changes in **business strategy**). The organisation should enter a stage where it considers "operational resilience" to be a default condition for any product or service that is key to its clients.

2. Reverse-engineer the key products and services.

Once you have identified the key products and services, focus on the value chain that created them. First, you need to identify the key processes contributing to that output.

Note that we also talk here about key processes: any product in complex organisations is naturally the result of a number of processes and interactions. The question here is: what is key (in terms of processes and staff) in order to maintain, unaffected, the offer of such a product?

Let's take our example of a 24/7 insurance telephone helpline. Multiple processes contribute to such a service, including a triage stage to assign the call to the most expert person available, and a process to record the conversation for compliance purposes. Most importantly, for the service to be available, the organisation needs people answering the call. What is really key in all this? Clients calling the central line are looking for immediate support, so they will not accept a "no-answer", although they may be willing to accept that the call is not recorded if such a process fails. Similarly, they might accept not being able to talk to an expert immediately (if the triage process fails), as long as someone else is supporting them in the meantime. So, what is really key in this case, is a minimum number of people able to answer the calls and able to stay with the clients until an expert is available for them.

3. Identify digital dependencies

One of the results of the reverse-engineering should be the list of IT systems (and respective data) and dependencies that are key to delivering the products and services (**digital resilience and service operations, and data resilience**). What software is used? What networks are leveraged, what digital infrastructure is utilised? A service provided via a mobile network will need different considerations than a service provided via landline. What databases are used, where are the servers located, etc. The number of questions in this regard are quite varied, and cover more or less everything that ensures a product is delivered to a client, net of processes/people and third parties.

Going back to the example: a key IT requirement is maintaining an open line so that the available staff can be called. This includes having a working connection (be it LAN or Wi-Fi), a working software for receiving calls and a working hardware to allow staff to listen to and talk to clients.

4. Map third-party dependencies

It is essential to know who the critical third parties are in the identified processes and infrastructure (**sourcing and external dependencies**). Whether they are in the organisation that provides the internet connection, or the company that rents you the building where your staff are located: you need to understand which third parties you "cannot live without". When it comes to third parties, it is also important to understand any interdependencies with other processes – is the same third party a key stakeholder in delivering a number of products that are apparently disconnected from each other?

Returning to the example, a third party may provide you with the IT infrastructure that you rely on to answer the calls, or you may rely even more on third parties to provide you with the staff necessary to cover the service 24/7. Try to investigate this point in detail – you might be relying on third parties without realising it, e.g. if an internal function providing you with a service is actually itself relying entirely on a third party for this process.

5. Define possible threat scenarios

You should now have a clear picture of which services and products you need to be able to maintain in stress conditions, and which key processes/people/IT systems/third parties actually deliver those products and services.

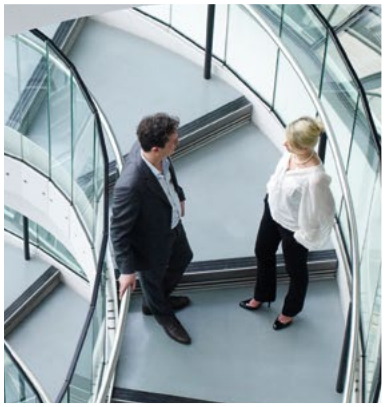
Although resilience should mean being able to withstand any type of stress scenario, one should be pragmatic and start with a rather simple question: what can possibly go wrong with the identified value chain components? Note that we start from the assumption that the organisation already has controls in place to ensure that each individual process functions at all times, so it is now time to forget about the siloed approach and try to look at the question from a holistic perspective. It is necessary to identify potential risk scenarios that impact the entire value chain, rather than single, isolated events that are already addressed by the standard risk management framework. Also, it is essential that you consider scenarios that are physically threatening the business (**physical security** and **facility management**), as well as scenarios that threaten the viability of the business overall (**continuity management**).

Let's consider our example: instead of focusing on isolated risk scenarios affecting one component of the value chain (e.g. all employees from one office falling sick from food poisoning), we should see how an event could impact the entire value chain. Let's say that in Asia the insurance company relies on a third party both to provide staff to answer the calls and to provide IT support. This company happens to belong to a bigger organisation, which also provides you with the internet connection needed to answer your clients' calls. What would happen if such an organisation were to be subject to an all-out strike tomorrow?

6. Map risks to the value chain

The chances are that your organisation has in place a working risk management (including operational risk management) framework. Yet even in this case, risks are often considered in isolation. IT will have considered certain risks, while the business has other risks on its radar. It is now time to consider all the identified risks, and list those risks that are linked to the value chain of your key products and services. What are those risks? Are they interrelated? What regulations impact my key processes, and how does this reflect on the risk profile of the entire value chain? When identifying risks, special focus should be given to cyber risks, as **cyber resilience** is a key pillar for any modern organisation trying to build operational resilience.

When we consider in our example the threat of a strike at the third-party company servicing the Asian location, different risks may materialise from such a threat and it is key at this point to consider how they are interconnected with each other. What happens in the event that you not only have no staff, but also that the calls received in Asia cannot be redirected to other locations as you do not have the internet connection to do so? You have probably considered both risks, but did you consider those risks materialising at the



It is important to outline that, to build resilience, you first need a functioning process. Trying to improve resilience in a process that is not working is like trying to fly a plane without checking how much fuel it has. It may seem to work at the beginning – until it doesn't any more.

same time and affecting your entire value chain in such a fundamental service? When defining mitigation measures, you need to ensure that you consider the interdependencies of the threats and risks to your value chain.

It is important that you identify all of these risks before they materialise, so that you can implement adequate mitigation measures in your processes (e.g. differentiate risks more, or include internal redundancies for processes where risks cannot be differentiated).

7. Learn from the past

Even when you have executed all previous steps, you may still find yourself in the situation where a key service experiences an outage due to an unpredictable event (black swan) or to un-identified interdependencies within your organisation (black spots). Either way, you need to ensure that the lessons learnt as part of your **incident management** and **crisis management** processes are used to define better controls or mitigation measures for your key processes and infrastructure.

In our example, you may have two different locations relying on different internet providers to ensure coverage (when one location is down, the other location covers for it). You couldn't know, but both companies rely on the same servers – when such a server experiences an outage, both your locations are unable to connect to the internet, even if you did try to differentiate the risk of an outage by using two different providers. Once you have resolved the incident, you should add this piece of information to your threat and risk assessment.

8. Monitor your risk exposure

Every big organisation has KRIs (Key Risk Indicators) in place. Ideally, your organisation's risk exposure will remain relatively low when it comes to risk management. However, in the context of operational resilience, you need to ensure that your organisation always keeps the lights on and the processes and systems that form the value chain for your key products and services are always available. If there are indications that your service may not be provided continuously and effectively, but this is not reflected in your KRIs, you may need to reconsider those indicators. Are you measuring the right parameters? Are you applying the correct thresholds?

In other words, the KRIs should reflect the exposure and weaknesses of your resilience capabilities, which include both protective and reactive measures. Understanding and quantifying the exposure of your key processes and effectively monitoring them is essential for remediating resilience gaps and interdependencies. This approach assists with driving resilience decisions and investments for discussions at Board level.

In summary

In our approach, operational resilience materialises when you make good use of the capabilities already in your hands, and when you start following a holistic approach to the value chain related to products and services that are key to your clients.

You should be able to do so for existing processes and systems, and try to embed this thinking as part of your strategy and change management framework – in order to build a "resilient-by-default" culture in your organisation when it comes to key products and services.

Once you have built this basic level of operational resilience, you can consider moving further in the "resilience" maturity curve towards "strategic resilience" (where you give even more space to considerations about your clients, who they are, what feedback they are providing, how their demographic is changing).

Does it really work?

A number of companies have already initiated their journey towards operational resilience.

PwC has supported some of them in achieving their goals – here are just some examples of how our methodology can help you achieve operational resilience.

Financial services company

Functional resilience governance and programme

Client's challenge

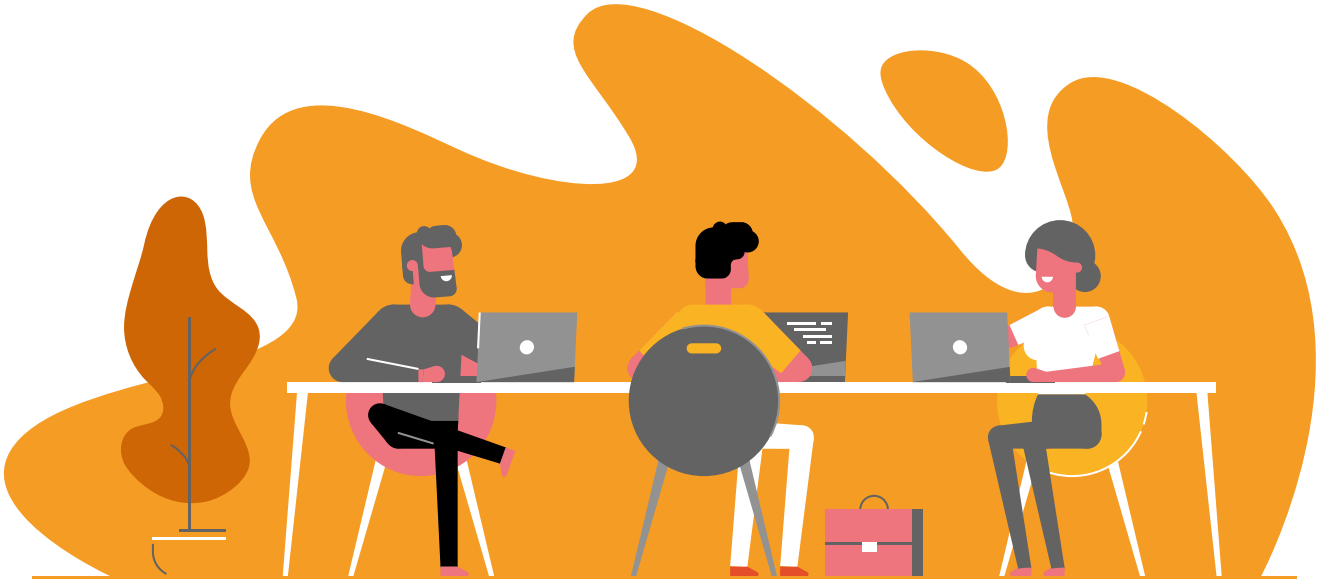
Three business areas critical to resilience had created separate resilience plans, but there was no integration, common language or clarity of accountability and governance between the areas.
The company needed to create a Resilience programme that would encompass the three areas: Business Continuity Management, Corporate Security and Technology.

PwC approach

- Understand and baseline current programmes through sessions held with the three key stakeholders.
- Evaluate the three separate sets of resilience programmes for integration/coordination effectiveness.
- Assess the existing programme procedures, policies, reports etc. based on: programme execution timing, common taxonomy usage, other industry practices for programme integration
- Identify interdependencies across programmes.

The outcome

- The client received guidance for improvements to their existing programme including a perspective and recommendation for a resilience governance and operating model, and recommendations on how to enhance the existing operational resilience model.
- The client gained clarity on their current state, gaps, and where the opportunities lay. This was detailed in a roadmap to resilience document.



Retail bank

IT resilience – operational to enterprise

Client's challenge

Increasing regulator activity prompted the client to look into the maturity of its IT operational resilience. They wanted to identify which areas required focused improvement and needed a roadmap to get there. They also sought greater insight into the themes emerging from regulator activity.

PwC approach

- To understand current and desired maturity levels, we held workshops and carried out interviews for evidence verification. We used our operational resilience Maturity Assessment to cover 9 domains, 34 sub-domains and 92 core competencies of the bank.
- The assessment scores highlighted gaps between the current and desired maturity levels. We then prioritised remediation strategies to meet the desired maturity score.
- We validated the outcomes through discussions with senior management and aligned desired maturity levels of competencies with the organisation's strategy and investment.

The outcome

- The bank gained insight into the current state of its IT operations resilience, understood the gaps against desired maturity, and received high-level recommendations to address the gaps. They also were made aware of other areas where deeper investigation into resilience maturity could be worthwhile.
- The bank was able to prioritise areas requiring improvement and investment and received a roadmap for improvement including remediation quick wins.
- They were also provided with a benchmark to use for internal comparison

Global financial services provider

Operational resilience benchmark tool

Client's challenge

In the aftermath of a regulatory review, this global financial services provider needed to thoroughly review its payment services resilience programme.

PwC approach

- Initially we used our operational resilience benchmark tool to inform the client about the true scope of resilience in an organisation.
- The tool's maturity model formed the building blocks against which the client's resilience framework was compared. We analysed the output to assess whether the client's approach was thorough, comprehensive and adaptable enough to improve resilience now and in the future.
- PwC provided a heat-map indicating which areas of the client's original framework needed further consideration.

The outcome

- The client gained a wider view of resilience than their initial framework provided. They learnt that creating resilience long-term requires consideration of multiple dimensions of the organisation rather than solely focusing on how discrete factors, such as IT or cultural failures, had led to one specific incident.
- The client understood which areas they could initially address in their resilience programme, such as cyber security and organisational behaviours. We also highlighted key risks in each area of resilience, providing the client with a number of first steps that they could take to improve the resilience of their business.

How can PwC help you?

We are a global team of professionals with deep expertise in all the building blocks of operational resilience. We have supported our clients in their journey to resilience, and we can help you achieve the resilience maturity level that you are aiming for, following our standard methodology.

Thanks to our methodology, you can set up your operational resilience function, leverage your existing frameworks and complete the eight steps to resilience.

1

Assessing your current OR status

1.1 Assess your OR maturity: Assessment of current OR maturity by reviewing your OR capabilities against our key building blocks that define a successful OR programme.

1.2 Define your OR ambition: Develop an ambition for your OR capability, by taking into consideration the assessment outcome and your organisation's overall strategy.

2

Designing the operating model

2.1 Establish a mandate for resilience: Board level mandate, with unity of purpose through a common definition and strategy for resilience. Set up an operational resilience function, with ad-interim nominations.

2.2 Identify what matters most: Customer first, alignment with firm's strategy, commercial objectives and social licence to operate. Regulatory landscape, market integrity and stability, customer detriment, key business services.

2.3 Understand the risks and set the risk appetite: Top down from the board. Integrated with enterprise risk management – applied at the firm and critical service level.

3

Delivering the operating model

3.1 Build and sustain an integrated operating model: Design and implement an operational resilience model. Coherence through alignment of operating and business engagement model across resilience disciplines.

3.2 Governance and control environment: Active Board oversight of resilience activity. Measure, report, challenge – Key Performance and Risk Indicators, adequate and effective governance.

4

Delivering business as usual

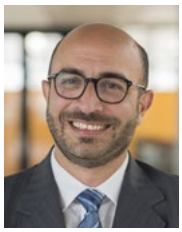
4.1 Assess resilience of critical services end-to-end: Service ownership for resilience, map and assess business process against critical dependencies End-to-End, including the associated People, Technology, Premises and Third Parties.

4.2 Remediate resilience gaps: Execute a BAU programme to remediate resilience gaps – maximise ROI by targeting what matters most. At a speed and in an order that reflects organisation capacity and risk appetite.

4.3 A sustainable OR function: The set up OR function transitions to BaU, with final appointments and clear governance oversight. Operates within the first line with second line oversight.

Notes

For additional information, please contact our experts



Patrick Akiki
Partner
Finance Risk and Regulatory Transformation

+41 79 708 11 07
akiki.patrick@ch.pwc.com

Adam Mikulka
Partner
Financial Services Advisory

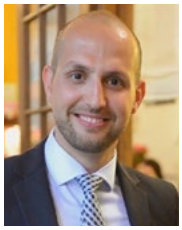
+41 79 126 70 37
adam.r.mikulka@ch.pwc.com

Wolfgang Schurr
Partner
Cyber Resilience

+41 79 708 11 07
akiki.patrick@ch.pwc.com

Thomas Busch
Senior Manager
Third Party
Risk Management

+41 79 878 01 68
thomas.busch@ch.pwc.com



Morris Naqib
Senior Manager
Risk and Regulatory Transformation

+41 79 902 31 45
morris.naqib@ch.pwc.com

Isabella Sorace
Manager
Risk and Regulatory Transformation

+41 79 742 37 16
isabella.sorace@ch.pwc.com

Key contributors:
We would like to thank Ioannis Katranzis, Silvano Engel and Davide Quadraccia for their valuable contribution to this publication.

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00