eraneos

FOCUS

Resilience

From left to right: **Dr. Christian Mauz,** Partner; **Adrian Anderegg**, Head of Financial Services; **Dr. Pascal Bettendorff,** Senior Manager; **Dominik Moser,** Senior Consultant; **Dr. Adrian Marti,** Head of Cyber Security & Privacy; **Stephan Gerber,** Consultant; **Johannes Vamos**, Consultant; **Dr. Thomas Rhomberg**, Head of Security Operations & Transformation

Contents

Mastering the risks on our journey to digitalization

The VUCA[1]-World describes our new reality of volatility, uncertainty, complexity and ambiguity. Like the great discoverers at the beginning of modern times, we must find our way in this new world and align our organizations accordingly. The first sailors set sail without knowing what to expect. Over time, we have developed tools to make risks manageable. For Christopher Columbus, the journey to America was a life-threatening adventure. Today this is nothing special for us anymore.
Dr. Christian Mauz

With digitalization and VUCA-World we find ourselves in a very similar situation. We don't know the exact threats and enemies and the environment is constantly changing. All we know is that apart from many opportunities our organizations face serious threats as well. Classical risk management and future planning are reaching their limits here. To succeed in such an environment, organizations must be highly resilient.

> " Resilience is mandatory for organizations to survive in the VUCA-World."
>
> **Dr. Christian Mauz**
> **Partner**

Nature and biological systems are good models for resilient systems. Concepts such as redundancy, encapsulation, decentralization, autonomy or polyvalence help people to successfully establish themselves in a wide variety of environments and survive even the most serious illnesses and accidents.

In this Eraneos Focus we would like to give you approaches on how to make your organization fit for this new world and become resilient.

We wish you an exciting and informative read.

1 Volatility, Uncertainty, Complexity, Ambiguity

Resilience Our under-standing

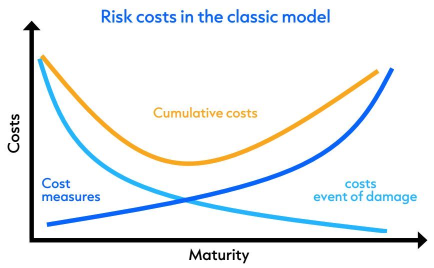
At present, the catchword resilience is omnipresent in the entrepreneurial context. Not even experts agree on its definition and characteristics. However, it is clear that the ability of a company to withstand unknown and mostly negative events can be increased by means of resilience. The high importance of resilience can be summarized under the collective term VUCA (Volatility, Uncertainty, Complexity and Ambiguity): It is becoming increasingly difficult to predict the future in concrete terms.

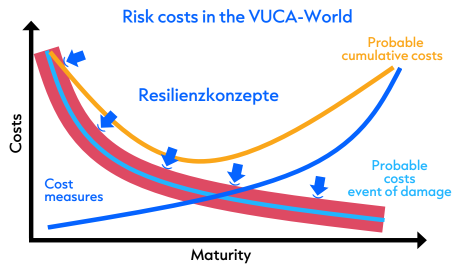
Dr. Pascal Bettendorff, Johannes Vamos

With the increasing digitalization and collaboration of companies, the identification and control of risks is becoming increasingly complex. Traditional risk management assigns a financial value to risks by assessing the amount of damage and the probability of occurrence. An attempt is made to optimize the cost of the measures taken in the event of damage and the costs incurred as a result. In a complex and volatile threat landscape, however, not all risks can be identified. In addition, the numerous dependencies make it difficult to quantify the consequential costs of risks. The extent of the damage blurs to a damage area.

Resilience does not aim to protect against individual, clearly defined risks. But rather, so-called resilience concepts try to reduce the potential damage range of all risks - both known and unknown. Instead of focusing on individual risks, the extent of the damage is estimated for certain risk groups and compared with the costs of the necessary measures. The basis for the definition of risk groups is the threat landscape, which must be continuously updated, and the experience gained within the company. The classic cost-benefit comparison between risk and measures is shifting to an even more abstract level.

Resilience is therefore not only about identifying, preparing and coping with emergency or crisis scenarios, but also about surviving under challenging conditions and adapting to the new environment.





In the age of Digitalization and Collaboration, risks are becoming increasingly difficult to grasp

Operational resilience as a corporate key capability

The case of the Canadian Fintech QuadrigaCX, a former major Canadian exchange for crypto currencies, illustrates why classical risk management is inadequate. As a technologically modern company, the Fintech held the cryptographic keys in a so-called cold wallet[2]. In December 2018, the CEO died unexpectedly in India. Since there were no authorized representatives, the access data was no longer available and the company lost access to almost 200 million dollars for which the access key was required. It had neglected the organizational resilience.

Eraneos understands resilience as the ability of organizations to tolerate threatening business events over a period of time and to adapt flexibly to changing circumstances. Resilience considers the holistic robustness of the organization as well as its responsiveness, and not just individual business processes. In this Focus article, we will discuss operational resilience in more detail, as companies often face major challenges in this area.

Operational resilience ensures that the provision of internal and external services is guaranteed even in the event of failure of sub-processes or suppliers. Although it is based on Operational Risk Management, it does not only deal with explicit risks. Resilience is very strongly oriented to the changing threat landscape and pursues the goal of controlling unidentified risks that exist due to the complexity of today's service provision.

In some cases, financial inefficiencies have to be consciously accepted in order to increase operational resilience. For example, over-dimensioning, redundancy or fallback levels maintain a stable service even under difficult conditions.

Resilience in the Operating Model

To create resilience, recurring resilience concepts act on the operating model in the domains of People & Skills, Organization & Governance, Technology & Information, Partners & Ecosystems and Business Processes. A resilient company has a similarly high maturity level in all the domains mentioned. If one domain is neglected, the missing maturity cannot be compensated by maturity in the other domains. Similarly, a very mature domain cannot compensate for the weaknesses in the other domains.

Involving **people and skills** as well as **organization and governance** is essential for a resilient company. Employees must be adequately trained and equipped. The roles and responsibilities within the company must be clearly defined. At the same time, the required roles must be available during business hours and full substitutions must always be ensured. In practice, representation is often misunderstood as holiday representation. As a result, organizational resilience is less pronounced than assumed. It is particularly important for a resilient company to adapt quickly. This requires an established culture that welcomes change and avoids an overly cemented expert and silo culture.

2
Cold Wallet: a virtual wallet for crypto currencies not connected to the Internet

In many places, **technology and information** show a great and expensive need to catch up in terms of resilience. Often resilience was equated with redundant infrastructure, while the application part was neglected. Even simple measures, such as regular updates and systematic lifecycle management, can significantly increase the maturity rate. There are many possible options in this domain. However, since these are associated with high costs, only a systematic approach to the planning and implementation of measures to increase resilience enables optimal use of resources.

Partners and ecosystems are an essential part of the company in the age of digitalization. This requires Partner Management that is equally established for strategic, tactical or operational partners. Well-managed and well-maintained partners can become one of the strongest drivers of resilience and at the same time massively reduce costs. Poorly managed partners, on the other hand, carry a high risk and can represent a financial burden.

Business processes that are related to the core competencies of the company must be considered in the course of increasing resilience. It is crucial that resilience is already taken into account in the design of processes, e.g. through redundant support systems or collaborations with business partners. Resilience may not impair the efficiency of a process. Rather, process efficiency must be guaranteed even under difficult conditions.

All domains mentioned are coupled. Good technological solutions are worthless if the solution is not used, and good core processes are ineffective if employees do not adhere to them.

Target Operating Model

Mechanisms have an effect on the Target Operating Model and generate Resilience within the Company

Concepts for increasing resilience

From the practice one knows recurring patterns (resilience concepts), which can be used, in order to increase the maturity of the Resilience of the Operating Model. Examples of simple concepts are redundancy, encapsulation, scaling, decentralization and autonomy. All these concepts can be used in any domain. Redundant technology means duplicated systems, while in the organizational domain redundancy is about full substitutions. There are also more complex concepts such as know-how management, automation and collaboration.

A resilient company creates efficient mechanisms selectively in order to be as well-equipped as possible against the threat landscape. Not all resilience concepts are sensibly applicable for every company in every domain. However, the concepts offer a good starting point for further improving the resilience maturity throughout the company and identifying gaps in operational resilience. While the lack of such resilience concepts in individual domains can indicate a low resilience maturity, it does not make sense to arbitrarily combine resilience concepts without integral control.

We would like to deepen this through the example of encapsulation. In the technology domain, encapsulated systems consist of subcomponents that can be replaced during the lifecycle. In this way, different components can be replaced, assigned to partners and better scaled. In the domain processes encapsulation leads to resilience as well. Clear and simple interfaces allow the failure of sub-processes and alternative procedures. In the persons domain, encapsulation is already generated by a clear distribution of tasks and competences, while clearly defined contracts and SLAs convey an encapsulated structure to the partner domain.

The combination of different resilience concepts further increases the maturity. State-of-the-art approaches, such as "Chaos Testing" influenced by Netflix, work under the premise that systems are constructed modularly by means of encapsulation so that they can be restarted at short notice or replaced by a new instance. Netflix uses a central service, the "Chaos Monkey", which randomly puts selected systems under pressure during operation. Through established concepts in scaling and well-rehearsed teams, such situations can be mastered without the customer noticing the effects in daily operations. In addition, information is collected on dependencies that are difficult to estimate due to the complexity of the systems. With "Chaos Testing" one's own readiness is permanently tested and the maturity of the resilience is continuously increased.

Success factors for a resilient company

To make a company resilient, it must understand itself and its environment. This is becoming increasingly difficult due to increasing networking and decentralization. Therefore, the approach of a central body, from which all resilience should emanate, is becoming less and less practicable. The decisive factor for success is that every component and every employee in the company contributes to resilience. In every project, resilience must be taken into account from the outset and tested in productive operation.

The implementation of resilience in established processes and systems is often very complex. Following a company-wide analysis with regard to so-called "quick wins", a business-oriented approach should be adopted. The most important customer services should be reviewed as a matter of priority and made more resilient. In addition to specific analyses, it is also necessary to search for missing resilience concepts in the domains. These are good indicators of a low maturity level. Since low-resistance support processes pose a threat to resilient core processes, focus should not be exclusively placed on core processes.

How well and quickly the resilience maturity can be increased depends on the following success factors:

Culture is a cornerstone of resilience, as changes are part of everyday life in the age of digitalization and networking. Employees must be empowered and supported to actively shape such changes. Management also has to conduct a rethinking: Increasing resilience means consciously accepting financial inefficiencies. Operational processes that are already fully utilizing their capacities under normal load are very susceptible to disruptions and thus endanger the company.

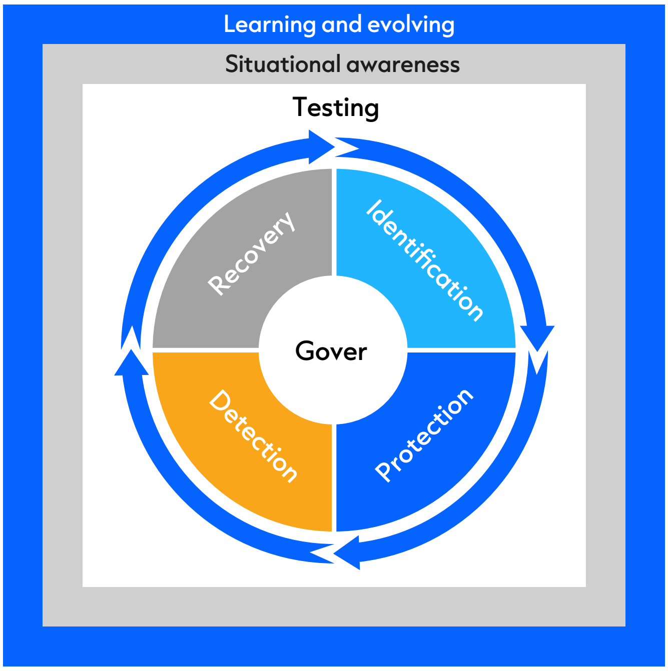
Leadership support is essential due to the far-reaching consequences. Enterprise Risk Management offers a direct starting point for this. In view of the conscious financial inefficiencies, measures to increase resilience must be supported by top management.

For **new projects** resilience must be integrated from the beginning. Weaknesses in individual areas can quickly affect the entire company due to close cooperation and complex dependencies. Therefore, clear, company-wide competence regulations are of key importance. With long decision-making paths, resilience can often no longer be guaranteed.

Tests, practicing & review of the measures are important instruments to ensure resilience in the event of an emergency. In many cases, measures are only formally implemented. Substitutions that can only carry out the most necessary tasks, or replacement servers that are not up to date, cannot be used in an emergency. The financial expenditure for corresponding tests can be reduced by automation and an appropriate periodicity.

CROE Inspiration nicht nur für Finanz-marktinfra-strukturen

High security standards are mandatory in the financial market. In the past, it was usually sufficient to limit security measures to regulated or commercial applications, such as SOX 404 or the Payment Card Industry (PCI).
Dominik Moser



Structure CROE

Financial Market Infrastructures (FMI) with their services for trading, settlement, processing and safekeeping of securities form the backbone of an efficient and functioning capital market. In addition, they are an essential link for the international networking of capital markets and capital movements.

Due to numerous attacks, which spanned far beyond the theft of financial figures and payment card data, the requirements for operational resilience and integrity were extended to all systems. In view of the increasing use of cloud and IoT solutions, defense measures limited to the perimeter are becoming increasingly ineffective. This makes a holistic and sustainable cyber risk management indispensable. Existing industry standards and best practices are helping organizations manage cyber security risks. The core problem, however, lies in the implementation of these frameworks, as they have to be adapted to the security requirements of their own industry and company. The financial market infrastructures (FMIs) in the Eurosystem also faced this problem when they were confronted with the "Guidance on Cyber Resilience for Financial

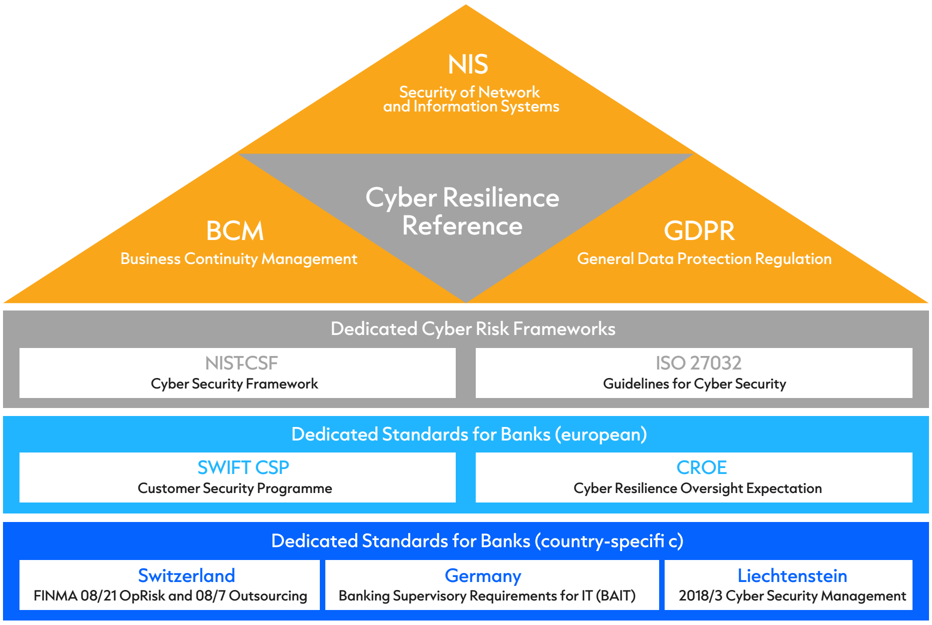
Market Infrastructures". It was published by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) in June 2016. The European System of Central Banks responded to the request for concrete implementation guidance by formulating the Cyber Resilience Oversight Expectations (CROE). This framework defines the expectations of the regulatory authorities for Cyber Resilience.

CROE has three main objectives:

- Specific instructions on how to implement the formulated expectations in order to lead to sustainable cyber resilience.
- Guidance for supervisory bodies on how to assess FMIs in their area of responsibility.
- The basis for a sound dialogue between the FMIs and their respective supervisors.

CROE is a comprehensive, state-of-the-art framework for critical infrastructures in the financial sector. It is based on the NIST Cyber Security Framework (NIST-CSF). The NISTCSF has a generic, cross-industry character and therefore requires industry and company-specific adaptation. As part of the process, CROE attaches great importance to governance and cultural change, which have some distinctive features in the banking sector.

In general you can see the relationship between dedicated frameworks like CROE in a hierarchical order: From common global requirements with a common reference to cyber resilience (CRS) to dedicated global cyber risk frameworks (NIST-CSF and ISO-27032) to industry and country-specific cyber security manifestations that ultimately lead to a company-specific implementation.



Various new regulations are in progress or have been enacted in recent years. In Switzerland, for example, FINMA Circular 08/21 “Operational risks in banks” dealing with cyber risks (under Principle 4, technology infrastructure). This is just the beginning. It can be assumed that in the short and medium term national and international authorities will set the framework for their application even narrower. This will result in regular checks of compliance by official authorities.

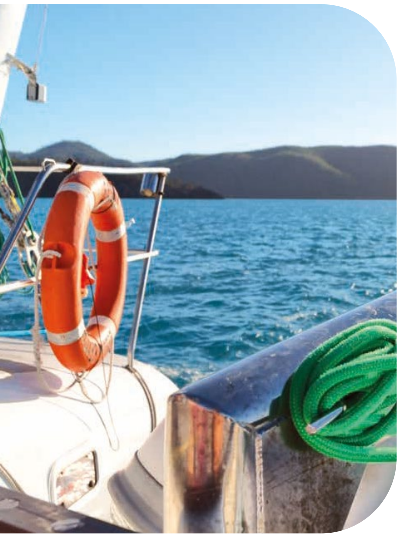
Key Standards of Cyber Resilience

Who should implement CROE and what can others learn from this framework?

CROE is the concrete design of various frameworks for the (small) segment of financial market infrastructures, such as NIST-CSF. Therefore, a complete, dogmatic implementation of CROE makes little sense for other industries.

It is important to realize from practical experience that it is preferable to rely on an industry-specific framework than to adapt a framework such as ISO-27032 or NISTCSF to one's own company. CROE provides valuable information on what such a design looks like, and on what level of detail it is based.

Implementation projects have shown that many discussions about the sense and purpose of an individual measure can be avoided if it is presented as part of a framework. In particular, the risk of unbalanced practical implementation, in which, for example, technical measures are over-emphasised and governance neglected, can be reduced in this way. In addition, a framework creates a balance between preventive and reactive measures. This not only raises the threshold for a successful attack, but also establishes systems and capabilities to quickly detect and respond to incidents. Another decisive advantage is the strategic control of the implementation program, which can be achieved by periodically checking the gaps to the framework.



Similar frameworks also exist in other sectors, such as the manual "General protection for Operational Technology in the Power Supply" published by the Association of Swiss Electricity Companies. However, a standard with the degree of concretization of CROE is still lacking in many industries. Cross-company initiatives - possibly supported by industry organizations or regulators - could quickly remedy this situation. Instead of a companyspecific design, an industry standard such as CROE would first be defined in such a situation. Due to the broad support, this would offer less room for debates as soon as the implementation measures become concrete and thus expensive.

Recommended approach for the implementation of CROE

CROE is not a "one size fits all" approach for the management of cyber security risks. Companies continue to be exposed to unique risks because they have different vulnerabilities and different risk tolerances. Accordingly, the practices in the framework must also be adapted to the specific needs of the company before implementation. Organizations can define activities that are crucial for the provisioning of critical services and prioritize investments to maximize their impact. Ultimately, the framework aims to reduce cyber security risks and continuously improve cyber resilience.

Open Banking as an opportunity Resilience for the Swiss finance center

Banks have always been expected to show a high degree of resilience. In the past, thick vault doors ensured the integrity of a bank and the assets entrusted to it, while today more and more complex measures in the area of cyber security are protecting the digital vaults. Regulators also draw up regulations aimed at ensuring the resilience of banks even in times of crisis.

Dr. Pascal Bettendorff, Stephan Gerber

Open Banking

Open Banking uses a collaborative model that enables financial institutions to provide the market with advanced banking information exchange capabilities through APIs. These functions allow third party providers to develop applications and services around the financial institution, and thus not only offer higher financial transparency to bank customers, but also provide new business models or additional services to financial institutions.

At present, traditional banks are also being challenged by a completely different kind of threat: Technology groups and neo-banks from Europe are pushing their way into the Swiss market as new players with innovative banking solutions, and are thus affecting the core business. Traditional banks have little chance of keeping pace with the agility and freedom of these new competitors and therefore need to find new approaches to remain competitive.

Open Banking offers banks an opportunity to open up their highly complex and specialized IT landscapes and offer future-oriented digital services together with third-party providers. In this way, traditional banks can open up new areas of business, benefit from the strengths of their new competitors and at the same time contribute their own strengths.

What changes with Open Banking?

The development of digital services and ecosystems often leads to cooperation with new partners, often also with young, innovative start-ups. Thereby, different corporate cultures collide, which in turn have a negative impact on the operational resilience. Looking at the dimensions of the operating models of the two partners, these differences become obvious.

People and Skills

A start-up employs other people with other skills than a bank. The product and the technology are clearly in the foreground here. It is important to inspire customers with innovative ideas. Further customer interests are rigorously subordinated to this goal. Flexibility and a high degree of adaptability are a matter of course for an innovative company, but they can overwhelm bank employees and customers. Small start-ups cannot understand how massively minimal adjustments to internal tools can affect the efficiency of hundreds or thousands of employees and lead to disproportionate implementation costs. On the other hand, a bank cannot afford to simply dispense with large existing customer groups by discontinuing broad access channels or high-volume products with no alternative. In the end, the average customer shows much less tolerance for incorrect account statements, incorrect postings or account blocks than a start-up company assumes.

A clear interface between the bank and the external service provider therefore makes sense. In addition, it also helps that a continuous readjustment of the fundamental core activities (protection of customer assets) and the surrounding shell of services with added value is available, which can be provided much more easily by partners. Both the innovation and the classical process thinking of the bank must be understood and included. Employees at the bank with an affinity for innovation serve as a bridge between the two worlds.

Organization and Governance

Organization and Governance could not be more different. In the "start-up-groove", young teams develop agile and self-organized innovative solutions without cumbersome organizational superstructures. The management is fully integrated into the development process and often possesses comprehensive technical know-how. On the other hand, there is the organization of established banking institutions with their clear processes and management structures. Regulatory, legal and financial requirements are omnipresent and have a considerable influence on the process handling.

In order to combine the strengths of both organizations, governance cannot be based solely on contracts and SLAs, as this would deprive the start-up of its benefits. The content of the shared customer experience should be determined by the organization. All parties involved must be aware that the bank must retain responsibility for the content of their dealings with the customer. This has many concrete organizational consequences, such as data sovereignty.

Technology and Information

In the Technology and Information dimension, interfaces are a central element. The highly isolated, partly somewhat outdated, but highly stable and efficient applications of banks must be opened to modern cloud-based systems. Data and information can be exchanged with the new partners via technical interfaces. Each opening, however, holds potential risks for cyber attacks and leads to new technical dependencies.

Frequently different development processes collide thereby. Innovative companies bring innovations to users as fast as possible. This can quickly overwhelm a bank with a complex release management. In addition, bank customers have little understanding for regular maintenancerelated failures of their digital banking services, such as eBanking.

Integrations must therefore be developed with the awareness that any external service can fail at any time. Similar to the zero-trust concepts in cyber security, it therefore makes sense to turn away from maximum availability requirements. "Chaos Testing" of IT and business continuity anchors this new Credo in the organization.

The design of technical components must ensure their functioning without dependencies on external services. For example, if a system loses access to real-time data, local data must be available for approximation.

A clear service architecture is based on flexible interfaces and enables rapid exchange of technical components. With the help of microservices, applications are designed modularly, up to the ideal of interruption-free deployment - although this ideal state is not always desired. For example, stock market-related information or financial data must never be accessible to only part of the user in the context of a rolling deployment. API management allows for an easy integration of partners, with cleanly versioned interfaces and coordinated adjustments.

Partnerships

Young companies are often on shaky feet financially. They are founded quickly and liquidated just as quickly in the absence of success. It should not be assumed that such agile companies will be available as partners on a long-term basis. Especially in an initial or growth phase, losses are normal. It also happens that a formerly "hot" start-up is overtaken by even more innovative companies.

Accordingly, the question of multi-vendor strategies is constantly arising in Open Banking. For each partnership, it must be carefully evaluated which skills are to be developed internally or by other partners in parallel with the partnership. This must be adequately addressed through know-how management and appropriate training.

The question of intellectual property also arises during every cooperation. If this is not the responsibility of the bank, access to technical components or interface documentation should at least be regulated in advance via escrow mechanisms in the event of a total failure.

In order to stabilize the cooperation and develop it in a spirit of partnership, it is advisable to offer business coaching, especially for young companies. This enables more detailed control than, for example, supervision through presence on the Board of Directors.

Business processes

Start-ups quickly change unsuccessful business processes and models because they do not function along established value chains, but deliberately try to break them up or redesign them. Just like SMEs, start-ups operate in different cycles than traditional banks. This makes joint decisions more difficult.

The bank must be able to react at any time to changes in its partner's processes. Lean, well documented processes and well-trained employees increase the ability to react in such cases. At the same time, the bank must be in a position to compensate for missing provisions and, for example, undertake training courses or the production of manuals itself. In general, the insistence on contractual agreements is less expedient than spontaneously "rolling up the sleeves".

If a bank wants to benefit from the enormous opportunities offered by Open Banking, it must identify and control the risks arising from the partnerships. With a functioning release management system, technical and procedural risks can be addressed and reduced, for example.

It is important to align all measures in a way that ensures a gradual degradation of services in the event of a disruption in one dimension of the Operating Model. This means that the entire IT landscape can function just as reliably as an ATM, which only deactivates individual functions in the event of a malfunction and thus constantly offers the maximum possible customer benefit.

Future compe-tence An interview on the topic of Resilience with Dr. Thomas Rhomberg

→

SIX is the backbone of the Swiss financial industry and, as a key infra-structure provider, has stood for innovation and stability in the global financial markets since 2008. In an interview with Adrian Anderegg and Dr. Adrian Marti of Eraneos, Dr. Thomas Rhomberg who is the Head of Security Operations & Transformation at SIX, explained how SIX addresses the issue of resilience and how the company has achieved its current status in this critical domain.
Dr. Adrian Marti, Adrian Anderegg

Dr. Rhomberg, how does SIX define the term resilience?
Thomas Rhomberg: At SIX, resilience clearly spans beyond Business Continuity Management (BCM). I see this as the next development step, since resilience doesn't just integrate the planning element of BCM, but also other management disciplines, such as crisis management. In this context I really like the term resistance. A comprehensive approach to further drive the field of resilience is risk management.

One of the major factors for resilience is the economic ecosystem of a company. This includes suppliers and customers, as well as events that affect security or business continuity as a so-called "third party risk". Another key factor is the ability to further develop the enterprise in a volatile and disruptive business environment. In addition, resilience should also be considered from the perspective of organizational psychology for the individual, and thus at the level of the employee.

For me, however, resilience is not just a collection of classical skills, but rather an intrinsic characteristic of an organization, such as compliance, liquidity or governance. An organization should not be structured resiliently. More importantly, resilience should be the purpose of the organization.

What does SIX do to be resilient?
In recent years, we have set up our own Security Operations Center (SOC). From the very beginning, we have pursued the idea of also offering these services to our customers, since not every organization can operate such a "protective shield" service itself. Through this, we can also increase the resilience of the ecosystem to which SIX belongs and generate a clear added value for the financial market, in addition to our own resilience.

To ensure internal resilience, we have clear governance responsibilities and operate a risk management system that takes into account oversight expectations regarding cyber resilience, which is therefore the driver and catalyst for the necessary changes securing a highly available IT. In addition, the management of a robust control framework is also very important for us in this context.

Resilience is associated with a lot of effort. What are the drivers that have brought the resilience of SIX to its current state?
SIX is a joint venture and an infrastructure service provider for the financial market. Our primary endeavor to further develop resilience and continuously make existing processes more robust is derived from this fundamental mission. This is also the direct added value we generate. This is the only way we can function as reliable and highly available partner, entrusted with critical elements of the joint value chain. We also describe ourselves as a critical infrastructure for the financial market and, as a resilient company, want to make a conscious contribution to its stability, since the financial market is a crucial part of our economy that may not be allowed to collapse.

In concrete terms, risk management, i.e. our ability to identify and assess risks and derive appropriate measures, is the main driver. In addition, resilience within our corporate environment is an implicit expectation, and sometimes even a concretely addressed customer requirement. Ultimately, the driving force behind resilience also originates from the business strategy, in which change and transformation play a central role. Transformation in the sense of the ability to adapt one's own organization and business model flexibly at any time is becoming an increasingly critical success factor. The driving forces behind resilience at SIX are thus an interplay of various elements that together lead to the achieved, holistic status of resilience.

You have created a service out of your duty to be resilient, which can develop into a new business segment for SIX thanks to their SOC approach.
In my opinion, resilience is not a duty, but rather an aim that we at SIX address proactively. In this manner, we also proactively addressed the issue of cyber security about four years ago and asked ourselves what skills we needed to master in order to be better prepared for future challenges. The SOC is an example of how this pursuit has ultimately grown into a business opportunity.

Where should the responsibility for resilience be located?
If resilience is to be fueled from a central location, the responsibility for this is best handled by a risk organization. However, since resilience has different characteristics, it should preferably be founded on a decentralized approach. Individual skills, domains and organizational components with specific performance characteristics contribute to the overall organizational resilience. For me, this is therefore more of a bottom-up approach than a pure top-down approach.

What would you like to share with the readers regarding the subject of resilience?
I recommend every company that is integrated into an ecosystem of stakeholders of any kind to consider the issue of sustainability within the framework of resilience, and to think well beyond its own organizational boundaries. Today, many problems can only be solved through a joint effort with partnerships or alliances. This is the systemic perspective behind resilience that should be considered. SIX is already actively doing this and has, for example, carried out a scenario analysis of important trends in the area of business continuity with other system-relevant organizations in order to cooperatively drive the topic of resilience.

FinTech "Made in Switzerland"

SIX operates and develops system-relevant infrastructure services in the Securities & Exchanges, Banking Services and Financial Information business areas with the aim of increasing efficiency, quality and innovation along the entire value chain of the financial center Switzerland. SIX is owned by its users (120 banks) and in 2018, with around 2,600 employees and a presence in 20 countries, generated operating income of over 1.9 billion Swiss francs, and a net profit of 221.3 million Swiss francs.

www.six-group.com

eraneos

Experienced in a wide range of industries

Eraneos Group is an international management & technology consulting group that provides services from strategy to implementation. It has emerged from the alliance of Ginkgo Management Consulting, Quint Group, and AWK Group, as announced in 2021. The Group serves clients across three continents where some 1,000 dedicated and highly skilled professionals work jointly to unleash the full potential of digital. Services range from the development of digital business models and data analytics to cyber security, and from sourcing and IT advisory to the management of complex transformation projects. Eraneos Group has offices in Switzerland, Germany, Luxembourg, Spain, the Netherlands, China, Singapore, and the USA. In 2021, Eraneos Group realized a turnover of close to 200m EUR.

Contact us >

Our offices >

Visit our website >