Infosys®
Navigate your next

WHITEPAPER

THE RESILIENCE IMPERATIVE

Organizations are pursuing greater resilience, whether it is to satisfy regulators or offset the risks of an increasingly complex world. However, business continuity can provide more than just protection. With the right tools, preparing for disruption will help organizations increase revenue, improve efficiency, and better serve customers.

FUSION RISK MANAGEMENT

Infosys® | Knowledge Institute

The demand for greater business resilience has been a growing drumbeat for at least a decade. In 2020, it finally reached a crescendo. The pandemic has badly broken entire industries, upended supply chains, and shifted customer needs and behavior. The crisis has challenged the fundamental pillars of value creation worldwide, with only the most resilient able to weather these changes.

In the past several decades, increasing economic volatility, increasing market and customer complexity, rapidly increasing dependency on technology, and rising political instability yielded unprecedented levels of uncertainty. Non-financial and financial turbulence was so significant that our world is now known by researchers as VUCA (volatility, uncertainty, complexity, and ambiguity) and TUNA (turbulent, uncertain, novel, and ambiguous).

In response, many leaders focused on what was in front of them, leaving long-term value on the table. By the beginning of 2020, the pace of change was so swift that many companies focused on efficiency over providing new value to customers, favoring immediate gains over long-term results.

Then the pandemic hit.

The initial, acute phase of COVID-19 left organizations with many questions and few answers. In a March Gartner survey, just 12% of respondents said their companies were highly prepared for the pandemic.[1]

We identified and mapped, but it did not stand up to the test. We effectively had to go back. We had to create a new scenario around the pandemic and its cascading set of impacts ... lockdown, loss of people, working remotely. A lot of people had to change their scenario plan.

— Chief resilience officer for a global financial services institution

At Fusion, we have collaborated with thousands of organizations through this uncharted era, measuring the impact in the crisis's initial weeks and months. How did companies respond in the fog of war? How has the adversity opened new pathways to growth? How did companies try to see into the future — or at least further than the competition?

As we exit this global crisis, the stakes couldn't be higher. Companies that employ new agile ways of working are not only able to survive but thrive. Executives looking to compete must develop a new awareness of how customers are impacted when disruption occurs and how those disruptions are likely to happen. A new era of uncertainty demands that teams weave risk-awareness and resilience into the fabric of their organization — eliminating the silos, anticipating, preparing for, responding to, and learning from risks and events.

Short path from business continuity to growth

The path back to growth depends first on stabilizing the institution. For that, many have looked to business continuity planners, who were long charged with understanding relationships between critical processes and disruption.

That is a tall order for a domain under siege. Traditionally, companies recognized business continuity plans as necessary, but those documents had a tendency to gather dust on a shelf or were buried deep in a shared drive. Business continuity plans were too often viewed as little more than an insurance policy against disaster or a checkbox to satisfy regulators and shareholders. In either case, these plans offered little value unless the worst happened.

In spring of 2020, when the worst did happen, businesses globally struggled to adapt. EY's Global Board Risk Survey found that just 21% of the board member and CEO respondents believed their organizations were "very prepared" for an event like COVID-19.[2] After years of prosperity and relative stability, the world was clearly a much more dangerous place than previously thought. And those business continuity plans — designed to keep the world humming — were too static, dated, and unintegrated with how businesses really worked.

Now that organizations have seen one of their worst-case scenarios strike — a global recession triggered by the most severe pandemic in a century — business continuity plans are cast in a different light. When integrated with core operations of the business and holistically applied with strategic foresight (risk intelligence), the work of continuity can make the difference between weathering the storm and sinking entirely.

In uncertain times, business continuity efforts can provide foundational intelligence, particularly when applied in tandem with best practices in risk management, cybersecurity, third-party management, and crisis response and recovery. A detailed understanding of how a firm works and the critical elements necessary to serve its customers can be a competitive advantage — preventing disruption, enabling firms to respond quickly to shocks, catalyzing transformation, and fueling growth.

The adage "run the bank, change the bank" has rarely had more resonance. Forward-thinking firms are using the same business intelligence that protects and insulates their companies to serve the customer of the future. The result is new products and services, improved efficiency, and even the creation of new business models. The right plan and access to the data used to create it can become an offensive advantage as much as a defensive one.

To provide these benefits, businesses need to transform the way they

Figure 1. Know your business inside and out

SERVICES
Key functions provided to customers or the broader economy

PEOPLE
Workforce composition and behavior

THIRD-PARTIES
Multitier visibility at the supplier, site, tier, product, and service level

SYSTEMS
Benefit to business, service continuity, reputation, security, infrastructure

DATA
Loss, corruption, cost of managing, availability, compliance, breach, vendor lock-in, integration, remanence

PROPERTY
Liability, legal, partnerships, climate change

PROCESS
Infrastructure, IT, human error, workplace safety, process quality, mechanical failure

GEOGRAPHY
Concentration, weather hazard, geopolitical

Source: Fusion Risk Management

think about managing day-to-day operations. They require a robust understanding of firm dependencies, risks, and alternatives, with an eye toward better serving the customer of today and of the future. A prepared firm is a confident one. And through better risk intelligence and well-rehearsed continuity capabilities, institutions can more comfortably navigate the risks necessary to run, protect, change, and grow the business.

Regulatory directives: A customer-first view

In December 2019, the Bank of England, Financial Conduct Authority, and Prudential Regulation Authority introduced new guidance on managing risk and fully integrating business continuity with operations.[3] Operational resilience is the ability of firms and the financial system as a whole to absorb and adapt to shocks, rather than contribute to them.

European guidance established five key activities needed to manage business resilience, focused on the concept of critical services and managing to impact tolerances.

1. Identify your key services from a customer perspective. What are the important tasks your customer expects from your firm? We have heard them described as the "I wants." "I want to access cash." "I want to make a payment on a credit card."
2. Map the delivery of services end-to-end. Visualize what it takes to make the service a reality. This could include critical systems, third parties, people, sites, and processes. Understand dependencies, relationships, and the order of actions needed to complete tasks.
3. Understand the impact if one element of services — a third party, a system, a team, a site, or a process — suddenly became unavailable. Based on impact, establish the maximum amount of time your customer, the economy, and the market could withstand the disruption.
4. Devise severe, but plausible, scenarios and make a plan in case they occur. Test your response as if it were a live event. Learn and iterate.
5. Create governance and communication strategies that can integrate into the fabric of your firm.

These steps summarize best practices and point the financial services industry in a specific direction. But they also leave room for the ingenuity and know-how of individual firms. This guidance can solve three important challenges.

1. **The problem of prioritization** — Businesses should define criticality in the context of the larger economy and consumer impact. By viewing criticality from a customer perspective, firms have a sharper understanding of where to put resources in times of calm and times of stress.

2. **The problem of mapping** — Mapping an entire organization — every process, every capability — is a nearly insurmountable task that yields questionable benefits. Companies are constantly shifting. Ascertaining what is critical allows them to focus on mapping only the things that matter to the customer, to the market, and to the firm's existence.

3. **The problem of measurement** — Establishing benchmarks for operations allows a firm to more effectively measure what is actually good, determine the boundaries of what customers will withstand, and effectively manage the business to those constraints.

In the end, operational resilience is simply good business management.

Regulation and best practices: Building trust

After the U.K. directives, many regulators elsewhere followed with guidance of their own — notably the Basel Committee in August and the Federal Reserve's summary of sound practices of operational resilience in late October. Many regulators see this as an opportunity to align on a common operationalized view of a more resilient financial sector.

Let's not waste this opportunity, even though it came out of a pretty dark tragedy, for us to take the steps [toward] a true alignment of operational resilience, [putting] us in a better position to strengthen resilience against all sorts of hazards very likely to occur in the not-too-distant future on a more regular basis.

Art Lindo

— Deputy director for policy in the Federal Reserve Board's Division of Supervision and Regulation

Institutional trust can take decades to build — sometimes centuries — but can vanish overnight. Implementing the right operational muscle to detect, monitor, address, and learn from disruption is not optional.

Salesforce's 2020 study of global financial services trends found that the "last global recession diminished customer trust in FSIs. Although the causes of the current crisis are different, the mandate to strengthen customer confidence nevertheless takes on urgency in the face of economic uncertainty."[4]

Improving customer trust moved from fifth to second among corporate priorities. Eighty-two percent of customers said a company's trustworthiness matters even more this year than last, according to the Salesforce research.

Leaders view the impact of risk and resilience as beyond improving existing operations. Their companies implement resilience to find new value streams as their initiatives mature.

An outside-in and inside-out approach

From regulatory and best practices perspectives, planning just isn't enough. Business continuity plans can become outdated even before they are complete. Organizations, just like the risks that affect them, are not stagnant. Business intelligence must evolve to stay ahead of threats and provide guidance on how to respond before and after an impact.

> Not being able to make quick, well-informed decisions is a big risk for businesses today

One of the biggest risks that organizations face today is an inability to rapidly make well-informed decisions. Take away the real-time nature or accuracy of insight, and the decision is too late, ineffective, or both.

Our cohort of financial leaders reported that only 5% of their pandemic continuity plans were followed as written in the acute phase of the crisis. What helped those that were able to follow their plans?

- Integrated situational monitoring that sensed and signaled changes in the external operating environment and in the firm's operational capability.
- A deep understanding of the complex web of their firm's service delivery processes, operational dependencies, risks, and capabilities.
- A well-practiced set of responses, such as connecting from a remote setting, switching to a backup third-party technology provider, or routing calls to an alternative service center.

To be resilient in a new era of unpredictability, organizations must think more strategically about gathering and processing information. A nearly unimaginable amount of digital data has already been created, and the volume is increasing by multiples. IDC predicted that the amount of digital data in the world would increase from 33 zettabytes in 2018 to 175 zettabytes by 2025.[5] Organizations have two hurdles to clear when it comes to all this data:

How do we capture it? And once we have it, what do we do with it?

In many cases, firms are not struggling with the volume of data. Instead, it's a filtering problem.

An optimal system understands both internal and external data and uses it to identify areas of friction, single points of failure, and the most serious risks. This would create a framework that adapts to a shifting landscape and offers ways to minimize or prevent disruption.

Organizations need to know what is approaching and the resulting financial, reputational, legal, and regulatory effects. How will a storm or cyberthreat or political dispute or health crisis affect an organization, its employees, and customers? And how will that system allow leaders to make the most effective decisions? How does a firm's risk topology influence economic, market, and consumer risk? How does the firm's risk posture invite regulatory intervention? Looking at the system holistically, as opposed to parts, can yield benefits for consumers, the global economy, and firms alike.

The power to perceive, think, and act

Business continuity plans have traditionally lived in Word documents and Excel spreadsheets. Employees spent significant time and effort entering data about their organization into static files. However, the real value comes from understanding the relationships among the firm's assets, their processes, and their people's ability to deliver a service.

During a mapping exercise, one of Fusion's financial services clients uncovered a critical, aging legacy system that was unpatchable. It required an exorbitant service contract just to keep it running. By mapping critical business services, it was determined that if the system were to fail, it would have brought down four critical business lines. The company had no choice but to replace it or risk a catastrophic shock to the business.

A spreadsheet can list all the applications used in a company. But it can't immediately inform a manager of exactly which customers would be affected if an app or system failed, if there were backups available, how they affect other processes or services, and impacts on the broader economy. A static risk management system requires staff to review documents scattered throughout the company, wasting productivity and money.

Figure 2. Initial activities for operational resilience

Step 1
Step 2
Step 3
Step 4
Step 5

Step 1 - Identify services

Organizations need to identify and document the critical or important business services that have considerable systemic impact internally and externally.

Step 2 - Map resources

Service dependencies need to be mapped using processes as the center point – critical resources are systematically brought to the surface for analysis and consideration.

Step 3 - Set impact tolerance(s)

Impact tolerances are set (based on specific impact categories) leveraging the most critical data fed from the mapped resources and continuous monitoring.

Step 4 - Scenario testing and validation

Organizations must test their ability to remain within impact tolerance for each critical or important service – this helps to validate the confidence level on the resilience of services.

Step 5 - Response and communication

Impact tolerance testing and analysis should focus on the response and recovery actions organizations would take to continue the delivery of critical or important business services.

Source: Fusion Risk Management

Without critical automation, firms often wither away in manual effort and delays while trying to stay on top of risk and operational priorities. One global manufacturer spent more than 50,000 hours each year updating static plans. The move to an automated system reduced the effort by 75%.

Imagine the impact from a critical data insights perspective — a task that previously took weeks, now accomplished in a fraction of the time. Manual systems introduce risk by delaying important insights and creating knowledge silos.

Automation can make real-time insights accessible to everyone, from the front line to the boardroom, and mean the difference between stagnation and growth, instability and security.

Connecting the dots

No matter how companies operate, their organizational risk is not siloed. Risks in one area ripple outward toward other departments and then to the company as a whole.

Another company in our cohort found that its critical service center operations were concentrated in a geopolitically unstable region. High levels of absenteeism and civil instability required them to diversify the delivery of these crucial services.

The most advanced systems integrate internal and external data to make connections that weren't previously known or understood. This can be like the difference between treating the symptoms and treating the illness.

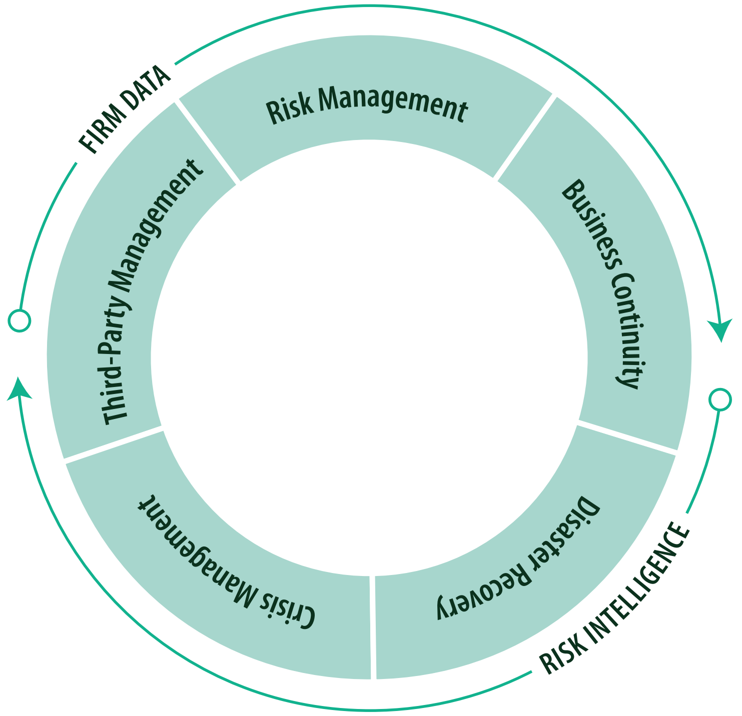
A U.S. consumer and commercial lender, with branches nationally, achieved integrated operational resilience in just six months. The bank consolidated continuity plans, mapped the organization, and completed comprehensive risk assessments of 350 of its most critical vendors. Now, the lender has a complete picture of its most important third-party operational risks and how they might affect the delivery of key services to bank customers.

The best risk management systems and approaches provide visibility into all the interconnected effects. Your risk will never be zero, but companies can narrow the range of unknowns and respond more quickly when they are known.

From risk to mitigation to strategic foresight

Mitigating risk, as it is traditionally understood, is an important goal but not the only goal. Companies pursuing greater resilience and agility should consider what managing risk can also accomplish. At its simplest, it prepares an organization for some future contingency. However, risk management can also solve current, invisible problems, such as inefficiencies and missed business opportunities.

Figure 3. Redefine resiliency



BREAK DOWN traditional silos that keep information segregated by department

Create **ONE DATA SET** that **INTEGRATES** with your existing systems

Gain **POWERFUL INSIGHTS** into operational performance and success metrics

Source: Fusion Risk Management

By cataloging and understanding all business processes from a customer perspective, leaders can see their companies in new ways. Companies will find new products, services, or business models in these illuminating moments.

As we've seen as a result of the global pandemic, customer needs and value creation assumptions can change overnight and irrevocably. The future depends on companies developing strategic foresight as a core competency of business excellence. Organizational mapping, scenario planning, testing, and other tools allow organizations to map their ever-shifting futures with greater confidence and fidelity. Scenario planning and other tools allow organizations to map their ever-shifting territory.

Strategic foresight enables executives to identify risks and opportunities, amplifying their ability to mold their organizations' future. Moments of crisis hold great commercial and innovative potential, even for the largest and most mature firms.

The world is too complex to take a one-dimensional approach to risk and resilience. It must still execute the fundamentals well but also supply business intelligence. To do that, a system needs to thoroughly understand the organization it protects.

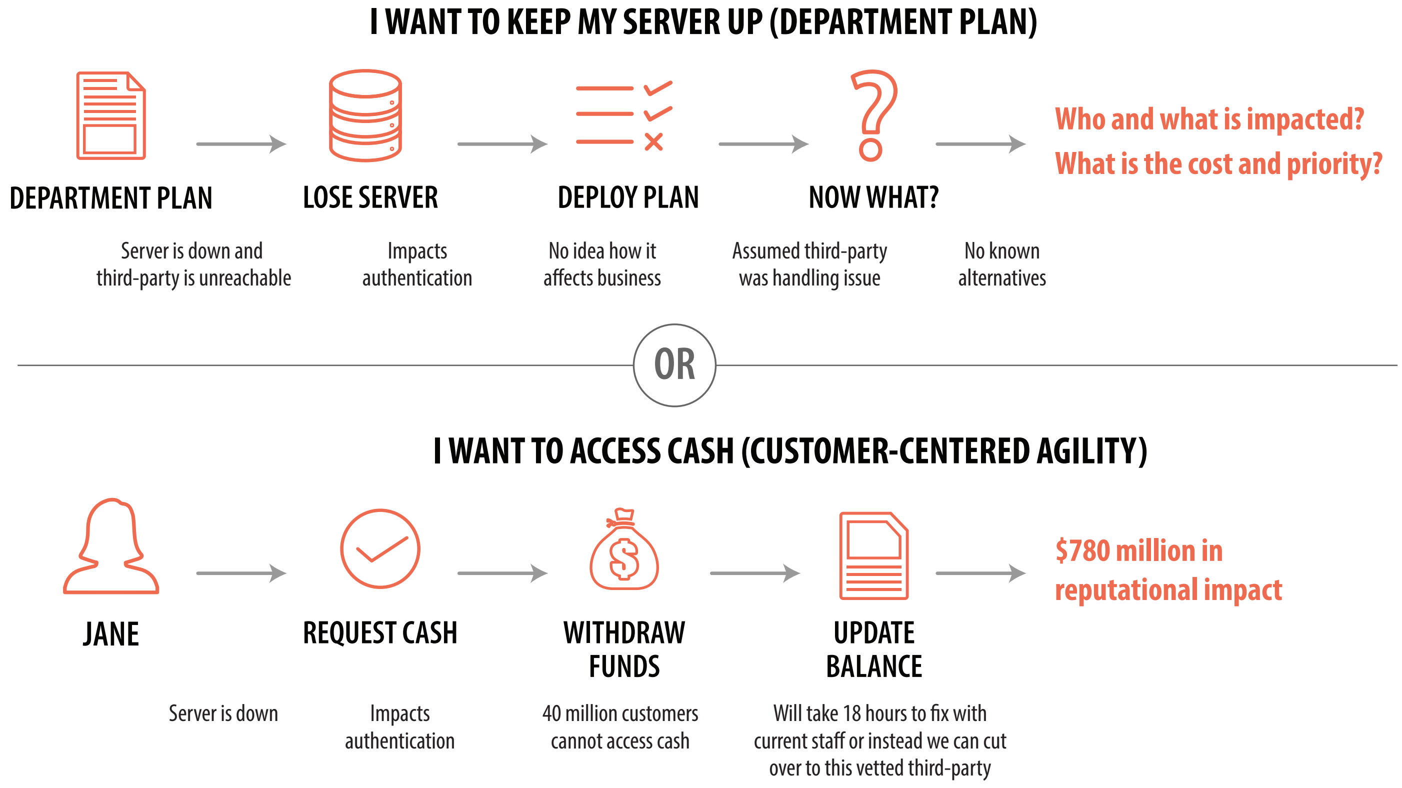
Creating exceptional experiences

If the Great Recession tested the liquidity of financial institutions, today's crises are a stress test of their ability to create new customer experiences. A wave of autonomous financial innovations is threatening incumbent institutions. Their digital transformations are on trial, forcing companies to improve their technologies. However, startups are already disrupting financial sectors and services, such as lending, payments, wealth management, and property and casualty insurance. COVID-19 and its cascading effects only accelerated the existing market dynamics.

> Companies should leverage systems that help them connect right data-driven insights to the right people

The right capabilities not only allow firms to get ahead of strategic risks, such as fintech disruptions, but also identify new opportunities to innovate. By mapping the customer's service delivery process and understanding their lifetime journey, businesses

Figure 4. A customer-centric perspective on business operations


I WANT TO KEEP MY SERVER UP (DEPARTMENT PLAN)
DEPARTMENT PLAN
LOSE SERVER
DEPLOY PLAN
NOW WHAT?
Who and what is impacted?
What is the cost and priority?
Server is down and third-party is unreachable
Impacts authentication
No idea how it affects business
Assumed third-party was handling issue
No known alternatives
OR
I WANT TO ACCESS CASH (CUSTOMER-CENTERED AGILITY)
JANE
REQUEST CASH
WITHDRAW FUNDS
UPDATE BALANCE
$780 million in reputational impact
Server is down
Impacts authentication
40 million customers cannot access cash
Will take 18 hours to fix with current staff or instead we can cut over to this vetted third-party

Source: Fusion Risk Management

can solve emergent needs and find new efficiencies.

As in-person transactions shift online, financial services institutions have even greater stores of digital information at their fingertips. Companies can gain additional value by leveraging systems that tap into data and then connect the right insights to the right individuals. This turns data into an even greater asset.

Financial services leaders have long noted that organizations should be ambidextrous, in the sense that they need to use existing competencies while exploring new ones. Data and technology flexibility allows companies to envision a better-prepared future.

Five critical operational capabilities

COVID-19 has accelerated the race to keep up with change. Shifts that would have taken years are now happening in months. Companies must transform on the fly while managing unprecedented challenges and a struggling global economy.

Businesses increasingly prioritized resilience before the start of 2020. However, many companies were still trying to determine how best to build resilience into their organizations when the current crisis struck. Defining resilience is easy (survive, recover, thrive), but applying that definition to a complex structure and set of relationships is a higher level of difficulty.

A multifaceted approach is needed, one that weighs risks, discovers inefficiencies, and unearths growth opportunities. These new and better capabilities will help businesses prioritize decision-making for every business process. Rather than using resources, the right risk management can add value, with or without the worst-case scenario.

The capabilities of true operational resilience — not just a rebadging of business continuity — can be framed with five key pillars.

Business continuity and disaster recovery

Traditional business continuity strategies focus on developing contingency plans in case disaster strikes. But these plans don't flexibly account for assumptions that change between when they are written and when they are called into action. We are living a real-time example: a global pandemic that sent millions home to work and learn — disrupting assumptions and sending aftershocks that affected the entire global supplier and third-party infrastructure for at least the next year. A contingency plan is only as effective as the underlying data that supports it.

Leveraging technology that maps how your firm works, how it breaks, how to put it back together again, and how to put it back together in new ways allows you to navigate volatility with agility and confidence. This is the fundamental underpinning of operational resilience — the ground layer of a top-down and bottomup approach to better business management.

Business impact analysis, undertaken as a part of continuity best practices, provides a rich perspective of an organization's inner workings — how they could plausibly be affected by external events, the likelihood of those things happening, and the impact should these events happen. The activities inherent in business continuity require teams to consider the consequences if the unthinkable happens, provide insight into the available alternatives, uncover single points of failure, and locate weaknesses in the value chain.

Further, business continuity connects plausible disruption to customer, market, economic, and business impact, allowing your teams to test and prioritize your response effectively. Creating services and products that are resilient by design only happens when you approach it with intention. It is said that only 15% of institutional risk is managed by risk and resilience teams.

There is an immense amount of information available to help organizations see around corners. We are swimming in data that can help us predict threats and opportunities, and the tools we use to analyze that flood of data are evolving too. Spreadsheets, text documents, emails, and meetings are solutions for a world that no longer exists. Weeding out unimportant information in order to surface insights that matter can be an immense task without the use of proper technology.

The problem is not information overload, it's filter failure.

Clay Shirky

— Vice provost of educational technologies at New York University

Technology that integrates data and allows businesses to visualize products and services from a customer perspective will set an organization apart. A map of the day-to-day operations within a business will keep it running smoothly.

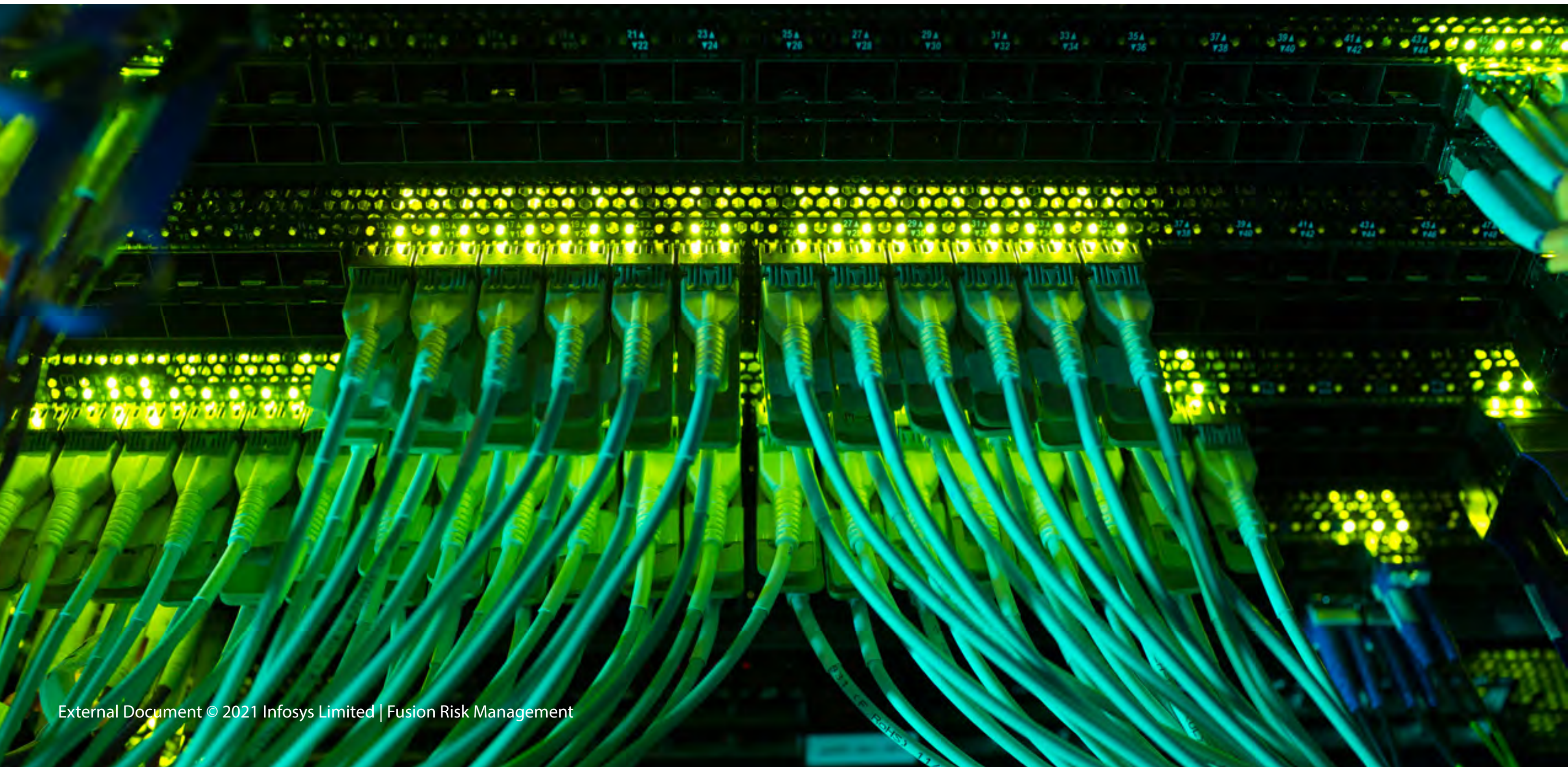
IT and cybersecurity

Trust is the true currency of financial services. Brands can take decades to build but can be destroyed overnight. Customer data is the lifeblood of brands and trust. Financial institutions must ensure the security, privacy, integrity, and confidentiality of customer data. In the face of growing threats, information security has raced to the top of virtually every board agenda. These events are increasingly seen as broadscale attacks on the wider ecosystem, and even where they may not impact your firm directly, you may be at downstream risk.

As a result of the robust interdependencies and network effects of cyberthreats and incidents, supervisory authorities have focused on risk to the ecosystem. But, beyond the ecosystem, your firm is responsible for the security and privacy of your customer data.

Risk-aware and resilient information security programs are often thought of as issues owned by IT. However, the repercussions of these attacks are lasting and affect every facet of the firm. Working collaboratively on strategies to better anticipate, prepare for, respond to, and learn from cyber risk and events helps companies design strategies that are more customer-centric and comprehensive than relying only on the IT perspective.

The proliferation of cybersecurity technologies, and threats, has made this task challenging. With unintegrated technology and quickly evolving threats, it's difficult to get a



sense of what is truly important for a business's health. Knowing that cyber risk and incidents directly affect the health of a company is an integral step to improving defenses.

> *I log in in the morning, all signals are red. I log out in the evening, all signals are red*
>
> *— CISO, large global financial services institution*

Understanding the connection back to the service has been effective in elevating the role of IT as a trusted business partner within the organization. Technology has helped IT interrogate their data through the lens of criticality, causing technology teams to rethink how they view the relationships between systems, data, people, and processes.

Operational risk management

COVID-19 has encouraged institutions industrywide to increase their integration of leading risk management practices. Boards are taking on a more active role in the oversight of financial, operational, and reputational risk. Increasingly, companies are fully integrating risk management into their operational and business functions.

With an increasing reliance on technology, cybersecurity has become a greater concern. Breaches have been surging in number and impact, with 90% of companies reporting more cyberattacks this year.[6]

Business ethics is another important regulatory focus, requiring teams to create a more risk- and resilience-aware culture. Compliance costs are skyrocketing, spurring many leading financial institutions to use their technology to more effectively demonstrate compliance and even stay ahead of regulations.

Effective risk management requires agile processes and nimble risk information technology systems. Combined, they allow firms to respond effectively to disruption and capitalize on opportunities that lie in the crisis's wake.

Third-party risk management

As organizations expand their third-party and supplier ecosystems, many are challenged with executing the core activities that make up critical services, risk topology, and compliance posture without compromising the quality of service delivered.

Control is a central challenge to managing third-party risks.

When considering your third party risks and building long-term resilience, your team must develop the visibility to:

- Understand your ecosystem.
- Know your critical risks.
- Employ strategies that help you reduce the ever-evolving landscape of threat and opportunity.

Understand your ecosystem

The financial services ecosystem comprises three primary categories of constituents: other financial services institutions, technology and other ancillary third parties not standardly governed by the same regulation, and public policy entities.

Each of these third-parties also has its own unique ecosystem of third-parties. Understanding the complex web of inner workings between your firm and others can help you mitigate issues before they develop into larger problems, and also capture opportunities more fluidly.

Understand your risk

Beginning with your list of core critical services and products, assess the risks involved in outsourcing this capability. Leveraging strategic foresight and what-if scenario planning, it is necessary to cast a more detailed understanding of your options and contingency strategies should that critical vendor fail or disappear overnight. It is inevitable that risks and events will occur. By isolating only the most critical of services, products, and scenarios in this way, teams are able to identify the signal from the noise, proactively managing the threats and opportunities most impactful to the firm. Leading with a customer-focused mindset, businesses are able to more completely address threats and capture emerging opportunities.

Employ strategies to reduce risk and capture opportunities

Once you understand your broader ecosystem and isolate your most significant risks, you can devise systems and processes that anticipate, prepare for, respond to, and learn from third-party and ecosystem threats. Leading firms are migrating from models that focus on point-in-time assessments to continuous monitoring. Opening up new channels of communication and collaboration with third-parties, many are turning to end-to-end scenario planning and detailed testing measures. Those provide more assurance that their third-parties are prepared in the face of great ambiguity and change, able to surmount disruption, and deliver on their commitments to your firm, and in turn, your customers.

Incident and crisis management

While crisis management is important for all companies, the boards of financial services institutions face greater pressure from regulatory expectations and the unique role the industry plays in day-to-day lives. When a crisis arrives, banking regulators expect boards to evaluate the causes, determine how to respond in the near term, and decide whether changes are needed in the longer term.

In addition to regulatory expectations, nearly all crises can cause a company to lose the trust of its constituents. This risk is even more pronounced for banks, whose business model is entirely predicated on customer and public trust. Erosion of trust can quickly turn an otherwise isolated incident into an existential crisis for the organization. These kinds of threats have proliferated in the last year, heightening the need to be ready to move quickly, decisively, and thoughtfully when a significant crisis does occur.

2021: Renewal

Many in our cohort of financial services leaders see 2021 as a chapter of renewal, leading their organizations out of the rubble of a prolonged crisis and through a bubble of rapid transformation, ushering in a new wave of growth and potential.

The pace of change has never been this fast, yet it will never be this slow again.

Justin Trudeau

— Prime minister of Canada

It's one thing to recognize that disruption is happening across organizations, sectors, and geographies. But it's quite another to acknowledge we ourselves have been disrupted, and therefore our business strategies and tactics have to meet this current state — both opportunities and threats — as well as continuing transformational disruptions to come.

Are you prepared? It's insufficient to just talk about innovation or "digital." We also have to be able to run, protect, and grow the institutions that make up the very fabric of our global economic security.

How Infosys and Fusion are partnering to build more resilient enterprises

About Infosys

Infosys is a global leader in next-generation digital services and consulting. We enable clients in 46 countries to navigate their digital transformation. With nearly four decades of experience in managing the systems and workings of global enterprises, we expertly steer our clients through their digital journey. We empower the business with agile digital at scale to deliver unprecedented levels of performance and customer delight. Our always-on learning agenda drives their continuous improvement through building and transferring digital skills, expertise, and ideas from our innovation ecosystem.

About Fusion

Fusion's mission is to help companies prepare, manage, and act in any situation by equipping them with the software solutions they need to be successful. Fusion amplifies your organization's resilience through insights, workflow, and best practices automation. We leverage a methodology tested and evolved over a span of 15 years of experience, informed by the ingenuity and expertise of many of the world's most trusted, renowned brands. Fusion accelerates your progress toward a more prepared, unstoppable enterprise. And we're deeply integrated with your existing teams, your processes, your data, and your systems, so your organization is able to tap into the full value of your investments to get you further tomorrow.

Together, Infosys and Fusion bring unparalleled expertise and proven solutions to help organizations transform the way they work.

SET Index (SET)
Relative Strength Ratio
RSI(14) = 48.84

References

1 Gartner Business Continuity Survey Shows Just 12 Percent of Organizations Are Highly Prepared for Coronavirus, March 10, 2020, Gartner.

2 Nearly 80% of Board Members Felt Unprepared for a Major Risk Event Like COVID-19: EY survey, April 20, 2020, EY.

3 Outsourcing and third party risk management, Dec. 5, 2019, Bank of England.

4 Lessons from Nearly 2,800 Financial Services Leaders on Resilience in the Face of Crisis, Nov. 19, 2020, Salesforce.

5 The Digitization of the World, David Reinsel, John Gantz, and John Rydning, Nov. 2018, IDC.

6 Tanium Report Reveals 90 Percent of Organizations Experienced an Increase in Cyberattacks due to COVID-19, June 29, 2020, Tanium.

Producers

Paula Fontana

Senior Director, Value Creation & Delivery, Fusion Risk Management
pfontana@fusionrm.com

Jeff Mosier

Editor-At-Large, Infosys Knowledge Institute
jeff.mosier@infosys.com

Authors

Mohit Joshi

President, Infosys
mohit_joshi@infosys.com

Michael Campbell

Chief Executive Officer, Fusion Risk Management
mcampbell@fusionrm.com

About Fusion Risk Management

Fusion Risk Management is a leading industry provider of cloud-based software solutions for business continuity, risk management, IT disaster recovery, and crisis and incident management. Its products and services take organizations beyond legacy solutions and empowers them to make data-driven decisions with a comprehensive and flexible approach through one system. Fusion and its team of experts are dedicated to helping companies achieve greater operational resilience and mitigate risks within their businesses. Learn more about Fusion Risk Management at www.fusionrm.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

Infosys®
Navigate your next

For more information, contact askus@infosys.com

Stay Connected