FORTINET

Regulatory Drivers for Operational and Cyber Resilience for Financial Services in EMEA

How to Meet Business Requirements and Accelerate Compliance

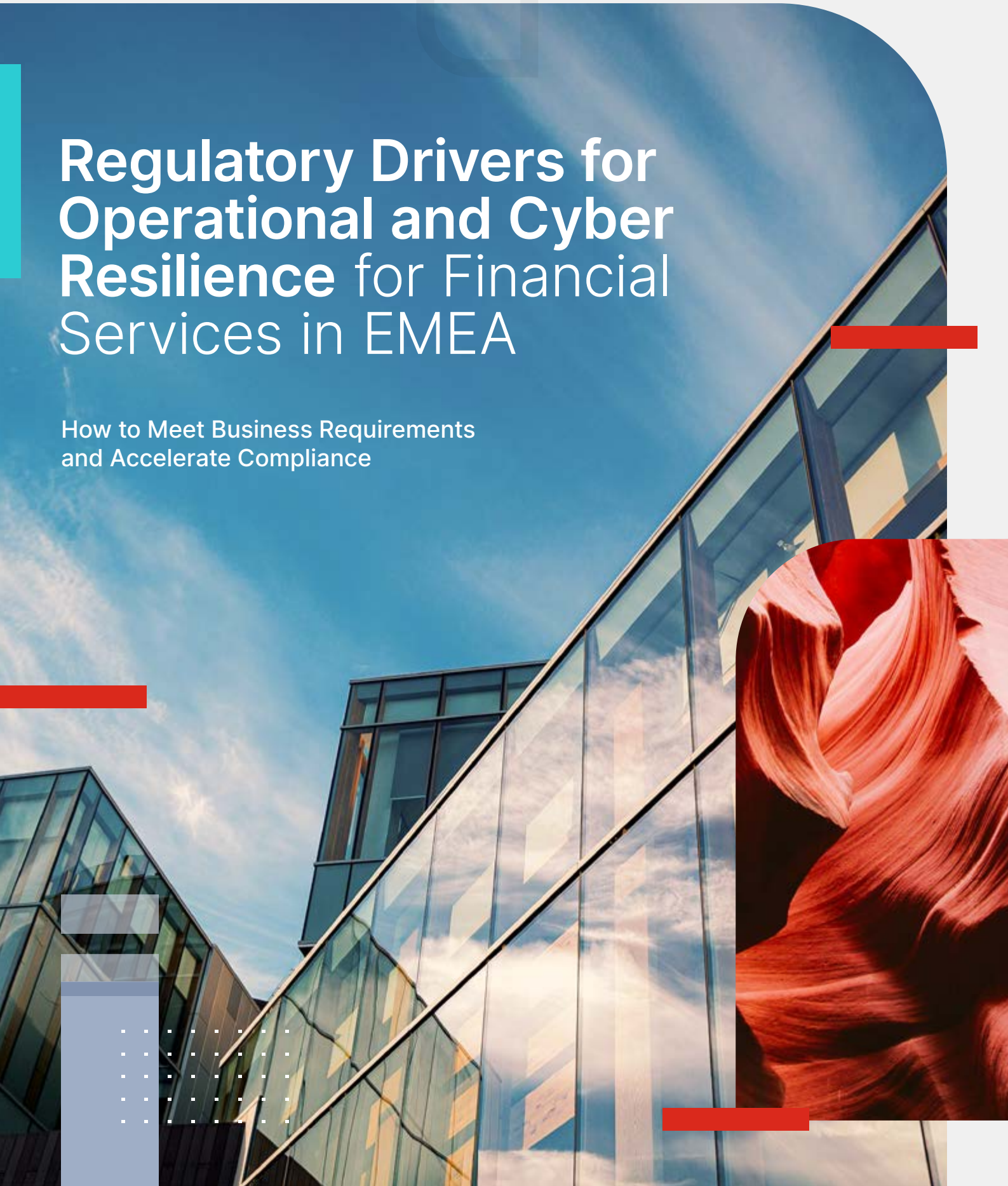


Table of contents

Financial services organizations are under more pressure than ever to strengthen their operational and cyber resilience.

Among the forces contributing to that pressure are fast-evolving technology, continually changing cyber threats,and an increasingly complex regulatory environment.

Fortinet provides robust security solutions that enable businesses in the finance sector to navigate these complexities. This helps to strengthen resilience, cybersecurity, and compliance with regulations across different jurisdictions.

Why Operational Resilience is Important

Operational resilience describes how well an organization can manage disruptions and maintain critical operations. The disruption could be caused by anything from human error or an IT system failure to a cyberattack, war, or global pandemic.

Because the global economy relies on the stability and integrity of financial services, organizations in this sector have a vital need to ensure operational resilience. Disruptions in the financial landscape can lead to wider shocks across the economy. This is why financial services businesses must be diligent about being ready to prevent disruptions as much as possible, to act immediately to mitigate impacts when prevention isn't possible, and to work as quickly as possible to recover after incidents occur.

Furthermore, as a highly regulated industry, financial services must comply with numerous resilience-focused requirements. In addition to existing regulations, a steady stream of new requirements aims to minimize risks linked to emerging technologies and evolving business models. For example, digital banking grew rapidly in response to the COVID-19 pandemic, when many financial services organizations began migrating to cloud computing and software-as-a-service (SaaS) business models.

The Bank of England's Financial Policy Committee[1] explains the motivations behind growing regulation for financial market infrastructures (FMIs) in a March 2024 report: "operational resilience has become more important to maintaining financial stability, particularly as the financial system has become more digitalized and interconnected...". But the resilience of individual firms and FMIs alone may not be sufficient to ensure system-wide resilience: some additional vulnerabilities exist at the level of the entire system. These vulnerabilities include: interconnectedness, complexity and opacity; concentration; correlation and common vulnerabilities; and system-wide dependence on data.

The operational resilience polices set by the Bank, the PRA [Prudential Regulation Authority] and the FCA [Financial Conduct Authority] help to bridge the gap between firm-level and system-wide operational resilience." Although these comments are specific to the UK financial market, they apply equally to markets outside of the UK.

What this means is that businesses in financial services need a comprehensive strategy for operational resilience—one that can grow and change as their own needs and customer demands evolve, while also keeping up with fast-evolving tech innovations, managing risks, and ensuring compliance with a host of complex regulations.

What Types of Regulations are Mandating Operational Resilience?

There are numerous regulations across the UK, EU, and MENA currently driving the need for operational resilience in the financial services sector.

In the UK, for example, new mandates from the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) will come into force in March 2025. These rules require—among other things—that banks, building societies, insurers, and other financial services organizations set impact tolerances for important business services, establish plans for regular scenario testing across each of those services, and exercise response and recovery plans for potential disruptions.These regulations, which put a special focus on cyber resilience, are part of a wider UK strategy to enhance resilience and stability in the financial sector in light of recent disruptions such as the COVID-19 pandemic.

In the EU, the Digital Operational Resilience Act (DORA) aims to harmonize operational resilience requirements across the financial sector.

Coming into effect in January 2025, it addresses the industry's increasing dependence on digital technologies and third-party technology service providers, along with the risks created by this dependence. DORA requires organizations to conduct digital operational resilience tests, monitor third-party service providers, and report information on cyber threats and incidents.

Another EU regulation, the General Data Protection Regulation (GDPR), applies to any type of organization that collects or processes information about people based in the EU. In effect since 2018, it has had a large impact on financial services because of the large volumes of personal data that the sector deals with daily. There is also the EU's Network and Information Systems 2 (NIS2) directive for updated cybersecurity controls, which applies to organizations that provide critical services.

Other rules affecting the sector in different jurisdictions across the UK, EU, and MENA include the Single Euro Payments Area (SEPA), which—starting in 2025—will require payment service providers to be able to send and receive payments in no more than 10 seconds. The global Payment Card Industry Data Security Standard (PCI DSS) governs the handling and storage of personal data related to payment cards. There are also France's Monetary and Financial Code (MFC); various rules on anti-money laundering (AML) and counter-terrorism financing (CTF), the EU's Artificial Intelligence (AI) Act, and the EU's Cyber Resilience Act (CRA)—which is aimed at updating cybersecurity and cyber resilience requirements for digital products. Complying with such regulations requires a combination of technology and non-technological solutions such as updated processes and procedures.

Germany and DORA

In Germany, DORA aligns well with existing initiatives from the Federal Financial Supervisory Authority (BaFin), including MaRisk, BAIT, ZAIT, and VAIT.

This simplifies the integration of new regulatory requirements and ensures a high level of maturity in ICT security. BaFin President Mark Branson highlights the transformative potential of DORA[2]:

"The Digital Operational Resilience Act (DORA) provides an important opportunity. This regulation will make it easier for us to influence cloud service providers in future. Thanks to DORA, supervisory authorities in Europe will be much better placed to identify interconnections and market concentrations at service providers. And they will be able to monitor together critical service providers. All of this will increase the operational resilience of our financial system—which is key to successfully delivering the digital transformation."

How Organizations Need to Approach Operational Resilience

Operational resilience is a journey, not a destination. And the first step on that journey is for financial services organizations to identify which of their services are most vulnerable to disruptions that could threaten financial stability.

In its March 2024 report, the Bank of England notes, "Some operational incidents are more likely to have systemic impacts because of certain features of the financial system, such as interconnectedness or because the affected firm is systemically important. Operational incidents in systemically important markets could lead to widespread impacts because of interconnections between participants. Systemic impacts could also occur where internal disruptions are common across firms, such as functionality issues in commonly used software or a cyberattack that impacts multiple firms at the same time. Disruptions at third parties that provide services widely across the financial sector, or significant external shocks that impact much of the financial sector could also have systemic impacts."

After identifying the services most vulnerable to disruptions, businesses must then determine how much disruption these services could tolerate before stability is threatened—that level is called the service's impact tolerance. This factor could be measured by time, or by some other metric.

Keeping track of these critical services requires persistent monitoring, along with robust mechanisms for measuring performance, incidents, and response. Businesses also need to continually assess their services to ensure these remain aligned with their resilience objectives and impact tolerances.

Addressing operational weaknesses is also important. “Operational weaknesses can arise in all parts of a firm’s or FMI’s operations, including processes or governance procedures that are poorly designed, employees that are inadequately trained, business areas that are insufficiently resourced, poor culture, or third-party services that are inappropriately configured or overseen by a firm or FMI,” notes the March 2024 report from the Bank of England. “These weaknesses can result from a lack of understanding of new and evolving operational risks at various levels within firms and FMIs (from operators and managers to executives and boards) and from underinvestment in operational resilience. There can be large financial consequences for individual firms and FMIs when such weaknesses are exploited. For example, in 2012 the so-called ‘London Whale’ trader lost JPMorgan £4.4 billion from unauthorized trading activity.”[3]

Another consideration is data integrity. After any disruption, organizations will need a way to check data for critical processes to make sure that it is complete, accurate, and reliable. They also need to understand how that data-checking process could affect time to recover.

Finally, financial services businesses must be able to demonstrate how they can prevent or recover from a variety of potential disruptions. Based on these scenario tests, they will then need to ensure they have the right processes and operations operating to enable recovery. This requires them to have the appropriate strategies and technologies in place to make data-driven decisions, and to be able to apply those insights to support resilience. They must also be able to deliver reliable reporting and effective stakeholder communication based on those resilience metrics. This includes all required reporting to regulators.

ECB stress test

In 2024, the European Central Bank (ECB) introduced a pioneering cyber resilience stress test for 109 directly supervised banks. Rather than assess the banks’ ability to prevent cyberattacks, these tests will look at how they respond to and recover from such incidents.

In addition, the ECB will conduct an enhanced assessment for 28 of those directly supervised banks. Aimed at assessing the level of coordination with other supervisory activities, this will require those institutions to provide the ECB with additional information about how they coped with the stress test cyberattack. These banks were selected to provide a representative sample of different business models and geographies across the EU financial landscape.

Achieving all of the above requires financial services organizations to rethink how their infrastructure is built, maintained, and secured. This means embracing several strategies for enabling modern digital services that support resilience:

Cloud

Using the cloud enables businesses in the financial sector to offer a wide range of modern services with the flexibility, availability, and agility that their customers expect. But it also creates responsibilities for shared security. Cloud service providers are typically responsible for the security of their systems—security of the cloud—while their customers must take responsibility for how they use those systems and manage their data—security in the cloud. This means that financial services businesses must take appropriate cybersecurity precautions and stay alert to the potential for cyberattacks and other threats. Because many organizations in the sector also continue to maintain legacy systems, they must also pay attention to hybrid security measures that work across both on-premises and cloud infrastructures.

AI

With the right artificial intelligence (AI) solutions, financial services businesses can enhance their cybersecurity across many processes. But AI can also be a double-edged sword, as the ECB notes: "When it comes to the interplay between AI and cyber risks, AI tools will enhance the capabilities of threat actors while also benefiting cybersecurity."[4]

A 2023 EY survey of European financial institutions found that 60% had already invested in generative AI (GenAI) technologies and 75% expected to increase their spending in that area in 2024.[5] Respondents cited such benefits as increased productivity and improved operational efficiency. Predictive AI is already used extensively to automate fraud detection. AI can also help to centralize incident management, automate threat responses, and enable rapid detection and response through advanced behavioral analytics. Newer GenAI technologies show promise for enhancing customer interactions while reducing costs. They also have the potential to accelerate the identification and remediation of threats; support complex queries during investigations; and adapt threat responses in real time based on evolving circumstances.

Cost Management

Even when dealing with limited budgets for cybersecurity, financial services organizations can improve their allocation of financial and human resources by relying on technology and service partners with advanced technology capabilities, including automation and AI.

UK and FCA/PRA

In the UK, the March 2025 deadline for the FCA/PRA mandates will require a proactive stance on risk management and significant investment to identify and secure critical business services. The FCA/PRA's nuanced approach underscores the importance of resilience by encompassing both individual institutions and the financial system at large.

Regular updates from the FCA and PRA will continue to shape the operational resilience landscape, requiring organizations to stay agile and responsive.

Digital Transformation Drives the Need for **Growing Resilience**

Cyber resilience is a critical component of operational resilience. The European Central Bank defines cyber resilience as "the ability to protect data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack."[6] That ability is more important than ever as financial services organizations digitize and modernize their services to keep up with customer expectations and evolving regulatory requirements.

The strategies for achieving cyber resilience and operational resilience are closely linked. Because business is increasingly digital, strong cybersecurity protections support both cyber and operational resilience.

Regulatory authorities looking to ensure the stability and integrity of the financial sector have recognized this by including strong cybersecurity elements in their rules on resilience. And organizations like the International Monetary Fund[7] warn that cyber resilience is essential to prevent threats to critical financial infrastructure and broader financial stability. Two trends are driving this need: the "unprecedented digital transformation" of the global financial system and the growing threat from malicious actors seeking to take advantage of that transformation.

France and GDPR

Financial services organizations in France must comply with GDPR requirements for stringent data protection measures, explicit consent for data processing, and prompt breach notifications.

In addition, businesses in the French finance sector must also secure their networks and information systems against cyberthreats to comply with NIS2, which has been incorporated into French law. They are also required to provide robust cybersecurity measures under the French Monetary and Financial Code (MFC).

What Developments are Driving the Need for Cyber Resilience?

The cyberthreat landscape is continually growing and changing, and the high value of financial services data makes organizations in this sector a leading target for criminals.

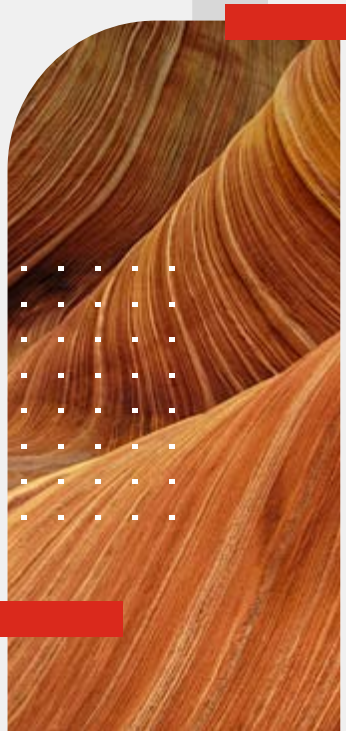
In addition to ongoing digitization of financial services businesses, other factors contributing to this are their growing dependence on third-party technology providers, a global shortage of skilled cybersecurity professionals, geopolitical tensions, and the emergence of new types of cyberattack strategies and technologies.

The rise of 5G networks and devices connected to the internet of things (IoT) brings an expanding number of potential vulnerabilities—as digitization increases, so does the risk of new kinds of cyberattacks. Another threat comes from emerging digital services such as money- laundering-as-a-service, which enables the movement of funds through cryptocurrency exchanges and hard-to-trace networks on the dark web. Meanwhile, continued innovation in AI provides new ways to launch cyberattacks while making it harder for targets to identify phishing and social engineering scams.

Digital currencies, especially Central Bank Digital Currencies (CBDCs) will add even more complexity to the threat landscape as they gain traction across different regions.

In the future, quantum computing could also bring unprecedented threats by making it possible to break today's encryption technologies. The Global Risk Institute's 2023 Quantum Threat Timeline Report[8] warns, "There's a high probability of quantum computers breaking public key cryptography within 15 years."

With all these developments, financial services organizations must prioritize cyber resilience no matter where they are in their digital transformation journey.

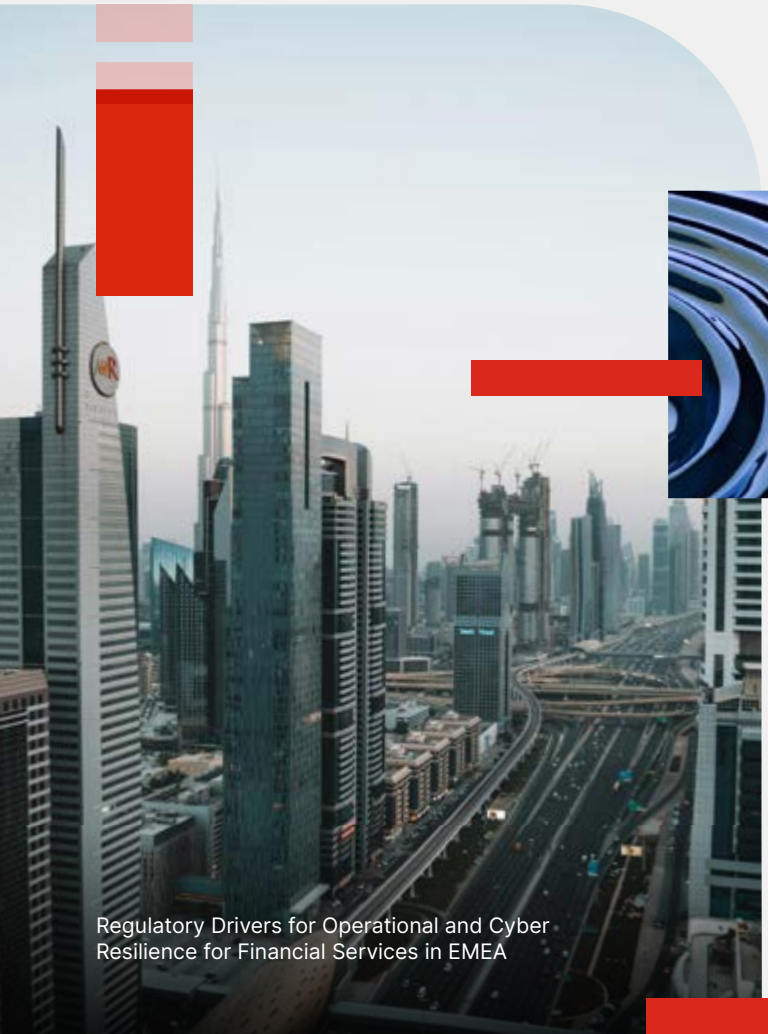


UAE and PCI DSS

The UAE's Central Bank plays a crucial role in maintaining the stability and integrity of the UAE's financial system.

Its comprehensive regulatory framework and proactive initiatives ensure the sector's resilience and competitiveness by enforcing such frameworks as PCI DSS. This requires continuous effort to provide network segmentation across cardholder information, cardholder data protection, vulnerability management, and access control.

Many financial services businesses in the UAE are pursuing transformation programs to address the impacts of such regulations. These efforts include reviewing compliance policies, hiring new experts, establishing change management committees, automating daily tasks, and adopting new technologies such as security orchestration, automation, and response (SOAR).



The Middle East and KYC

Across the Middle East, the implementation of Know Your Customer (KYC) procedures in financial services is closely tied to cybersecurity, given the region's regulatory landscape and unique cultural and technological factors.

Arabic naming conventions differ significantly from those in the West and often include multiple components to reflect family lineage, which complicates identity verification. Variation in the transliteration of names also adds to complexity around KYC.

Every country in the Middle East has its own requirements for KYC and Customer Due Diligence (CDD), and financial services businesses must comply with these varied regulations to prevent financial crimes. For example, in the UAE, detailed KYC provisions are issued by the Central Bank.

The region is increasingly using technology such as e-KYC utilities to address these challenges. The Abu Dhabi Global Markets (ADGM), for instance, uses blockchain technology to streamline KYC processes and ensure data quality and compliance while also reducing costs and improving financial inclusion.

There is also growing adoption of GenAI for applications ranging from customer service chatbots to fraud detection and credit decision making. A 2023 PwC survey[9] found that 83% of respondents in the Middle East—including 92% in the UAE—planned to deploy GenAI tools for cyber defense in the next 12 months, compared to 69% globally.

How Organizations Can Strengthen Cyber Resilience

To maintain cyber resilience, financial services organizations must introduce a comprehensive set of cybersecurity strategies to ensure a 360° view of their cybersecurity landscape. A comprehensive, end-to-end approach is essential to deliver such capabilities. Among the elements needed are:

Strong Cyber Hygiene

This covers a range of best practices, from the use of secure access points and regular security updates to robust access management and safe email practices. Maintaining an infrastructure and culture of strong cyber hygiene helps to minimize risks while also supporting regulatory compliance.

Everyone in an organization has a role to play when it comes to maintaining good cyber hygiene. Financial services businesses must emphasize the importance of this and ensure that they train all employees on how to practice good cyber hygiene, particularly the essentials such as using multi-factor authentication and strong passwords, exercising caution when clicking on links in emails and always using the most up-to-date version of software. This training can help to prevent cyber incidents, but is also useful for mitigating and containing damage during cyberattacks.

Multi-Layer Defense

Also known as defense in depth, this involves the use of multiple security measures to protect data, infrastructure, and services. A multi-layered defense strategy considers potential vulnerabilities across hardware, software, and people. Such an approach provides protection through physical controls, network security controls, administrative controls, comprehensive security operations capabilities, and behavioral analytics such as AI-powered anomaly detection.

Actionable Threat Intelligence

This means not only identifying intelligence about active and potential threats, but being able to share and correlate that intelligence across an organization. Integrated security platforms are essential for achieving this.

AI-Driven Technologies

Advanced security technologies that use AI, both machine learning and generative based, are increasingly vital for cybersecurity. These help to provide holistic and integrated protection across an organization while accelerating threat detection, analysis, and responses.

SEPA

New Single Euro Payments Area (SEPA) rules on instant payments are aimed at bringing the speed of messaging apps to European financial transactions. The changes will affect 36 countries, including several that are not in the EU.

By providing immediate access to funds, the instant payment capabilities are expected to reduce the need for liquidity or pre-funding and support the introduction of new payment features such as the use of QR codes. Combined with Secure Real-time Transport Protocol (SRTP), instant payments could also increase efficiency and create new opportunities for automation, according to the European Central Bank.[10]

How Fortinet Enhances Resilience

Fortinet provides an integrated platform that covers all aspects of cybersecurity for financial services organizations.

This ensures consistent, continual, and proactive security protections across the business, which in turn supports compliance with today's complex regulatory requirements for operational and cyber resilience.

For example, Fortinet's services for risk assessment and management capabilities include helping organizations to identify their most important IT assets, understand the potential damage from threats, and determine the level of risk they are comfortable with.

These capabilities, as well as its services for incident response planning, are part of Fortinet's comprehensive platform to help companies stay resilient. This also helps organizations to navigate the complexities of EU-wide directives such as NIS2.

This revised version of the Network and Information Systems Directive is aimed at establishing consistent cybersecurity standards and practices across Europe. Other Fortinet services that enable financial services organizations to meet regulatory requirements for resilience include continuous monitoring, training and awareness programs, phishing simulations, and threat-led penetration testing.

Key features of Fortinet's approach include:

Converged Security

Tight integration of network infrastructure and security architecture provides a single operating system for efficient operations, security, and a consistent user experience. This delivers end-to-end security, integrated threat intelligence, automated responses, and visibility across networks to ensure compliance and resilience.

Advanced Threat Protection

Using Fortinet's security operations solutions, financial services organizations can detect, prevent, and respond to threats in real time, helping them to meet the resilience requirements of GDPR, NIS2, DORA, and other regulations.

Cloud-Driven Innovation

Fortinet's comprehensive, cloud-based approach to cybersecurity simplifies security management for financial services businesses by integrating advanced solutions such as Zero Trust, Secure Access Service Edge (SASE) and AI-driven technologies. This unified strategy enhances resilience and eliminates siloed security practices. Fortinet's solutions also facilitate secure and compliant cloud adoption, ensuring adherence to critical regulations such as the CRA and EU Common Criteria.

Additionally, with its recent announced plan to acquire the AI-powered cloud security platform Lacework, Fortinet expects to integrate all of Lacework's critical Cloud-Native Application Protection Platform (CNAPP) services into its existing portfolio to help customers identify, prioritize, and remediate risks and threats in complex cloud-native infrastructure from code to cloud.

Leading AI Capabilities

With a portfolio of more than 40 AI-powered offerings,[11] Fortinet provides financial services businesses with unprecedented capabilities for threat investigation and remediation. These capabilities include rapid analysis of security incidents, support for complex investigation queries, real-time creation of threat remediation plans, and fast generation of playbooks for security architects. They are also essential for maintaining resilience as stipulated by FCA, PRA, and global standards.

For example, Fortinet Advisor (FortiAI), a GenAI assistant, helps security operations teams to rapidly investigate and remediate cyberthreats. Delivered through FortiSIEM—Fortinet's security information and event management solution—and FortiSOAR—Fortinet's offering for security orchestration, automation and response—FortiAI provides critical information within seconds, helping to reduce the mean time to detect and respond to incidents. It can suggest remediation actions, response playbooks, threat hunting indicators and more.

Comprehensive Compliance and Risk Management

Fortinet's solutions support comprehensive risk assessments and continuous compliance monitoring. These are essential capabilities for complying with GDPR, MFC, DORA, and emerging regulations like AML/CTF and the EU AI Act.

An Open Ecosystem

Fortinet's open ecosystem features hundreds of industry partners for technology, threat intelligence, DevOps tools, automation, and more.

Conclusion

Financial services organizations across EMEA must navigate an increasingly complex regulatory environment.

Fortinet provides them with the robust cybersecurity solutions and expertise needed to achieve and maintain compliance, manage risks effectively, and enhance overall cybersecurity resilience.

By partnering with Fortinet, financial businesses can confidently address current and emerging regulatory challenges, ensuring the protection of sensitive data and the integrity of their financial operations. Learn more about how Fortinet can help safeguard your operations and contribute to the operational resilience of your organization and a more secure and resilient financial future.

[1] Financial Stability in Focus: The FPC's macroprudential approach to operational resilience | Bank of England, march 27, 2024

[2] BaFin President Mark Branson: Learning the right lessons | Federal Financial Supervisory Authority, May 9, 2023

[3] The London Whale | Bloomberg UK, February 23, 2016

[4] The rise of artificial intelligence: benefits and risks for financial stability | European Central Bank, May 2024

[5] Majority of European financial services leaders expect Generative AI to significantly affect productivity and change | EY, October 25, 2023

[6] What is cyber resilience? | European Central Bank, June 2, 2022

[7] The Global Cyber Threat | International Monetary Fund, Spring 2021

[8] 2023 Quantum Threat Timeline Report | Global Risk Institute, December 22, 2023

[9] Digital Trust Insights Survey 2024, Middle East GenAI spotlight | PwC, December 3, 2023

[10] Work on instant payments in Europe advances | European Central Bank, May 24, 2023

[11] Meet Fortinet Advisor, a Generative AI Assistant that Accelerates Threat Investigation and Remediation | Fortinet, December 11, 2023

FORTINET

08 July 2024 1:56 PM
2774704-0-0-EN