DIGITAL OPERATIONAL RESILIENCE — FUTUREPROOFING OPERATIONS BEYOND THE REGULATORY SCOPE

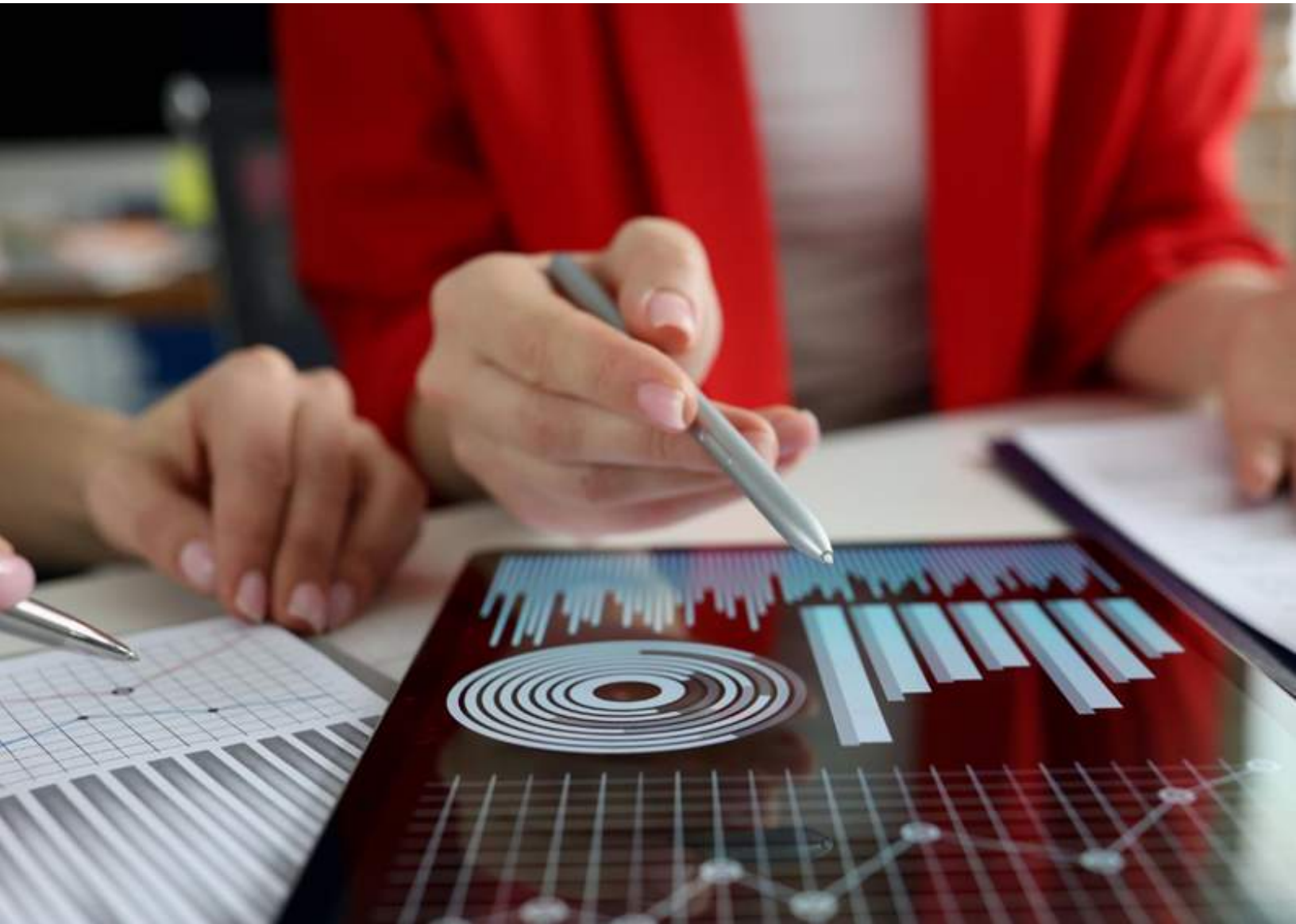
Author:

Maria Adele Di Comite

March 2022

An IDC Industry Spotlight sponsored by Nutanix

IDC #EUR148894722



Digital Operational Resilience — Futureproofing Operations Beyond the Regulatory Scope

Executive Summary

Customer demands for innovative and personalized solutions, along with the enormous pace of regulatory change and high operating costs, are forcing European financial entities to reinvent their operating models. These are characterized by a high degree of interconnectivity and are geared towards offering hyper-personalized, top quality, and high-speed or even real-time services. Digital resilience is a key paradigm for Financial Services and Insurance (FSI) providers to navigate today's increasingly data-driven, virtualized, and ecosystem-centric operating model. FSIs must manage digital operational resilience by looking at their internal systems and operations as well as the augmented space that covers the interconnections with all stakeholders. Customers' omnichannel access and employees working remotely in a hybrid workplace are expanding financial entities' cyber-attack surface. The need to optimize cost efficiency and scalability has led to many financial entities adopting cloud services, and now they need to be in control of the proper functioning of their operations that rely on external IT resources. Risk management approaches must consider the blurring boundaries of operational responsibility, moving towards a holistic approach of end-to-end digital operational resilience.

AT A GLANCE

KEY TAKEAWAYS

- The proposed EU regulation for digital operational resilience for the financial sector (DORA) is addressed at both the financial entities and their ICT and cloud partners.
- ICT and cloud third-party service providers will be under the direct supervision of one of the financial services' European Supervisory Authorities (EBA, ESMA, EIOPA).
- Collaboration among trust partners with info sharing is encouraged to foster the resilience of the whole financial industry.
- Existing mandatory ICT-related incident reporting procedures will be harmonized to streamline FSIs compliance obligations.

EU regulators recognize the growing dependency of FSIs on information and communication technology (ICT) and cloud service providers. Indeed, in a recent IDC survey 94% of the FSI confirmed that they leverage cloud services[1]. There are concerns that the prominent role of the critical ICT providers is leading to a possible systemic risk, therefore regulators are moving toward active involvement. With the new DORA regulation proposal[2] , one of the financial services' European Supervisory Authorities (EBA, ESMA, EIOPA) will directly supervise ICT service providers to mitigate the risks stemming from financial entities' dependency on them.

To future-proof financial entities, EU regulators are asking them to review the "*ICT risk management framework supporting the financial entity's business strategy (…) defining a holistic ICT*

[1] Source: IDC Industry Acceleration Survey, April 2021 (n=197 FSI)

[2] Proposal for a Regulation of the European parliament and of the council on digital operational resilience for the financial sector and amending Regulation (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

multi-vendor strategy (..) showing key dependencies on ICT third-party ICT service providers"[3]. To counter the systemic risk of interconnected digital operations, regulators have decided to expand the European Supervisory Authorities oversight to cover the designated third-party ICT service providers of the FSI industry, acknowledging that this is a deeply integrated and interconnected sector. The upcoming EU regulation proposal requires financial entities to adopt a holistic approach to the digital operational framework, widening the scope of ICT risk management to include their ICT services providers and to undertake end-to-end digital testing. The EU regulation proposal provides the direction towards the harmonization of mandatory incident reporting requirements across Europe to streamline the fulfilment of this compliance obligation. Besides mandatory incident reporting, regulators are also supporting voluntary information sharing among trusted partners.

Given the new operating models, there is no need to wait for the regulation to come into force. It is already time for financial entities to review their ICT risk management framework along with, and possibly together with, their technological partners. Financial entities and ICT vendors' joint undertakings to improve the overall ICT-risk management must, however, include compliance with the upcoming digital operational resilience requirements among their key business priorities. These priorities range from improving the bottom line with enhanced cost efficiency and scalability to providing customers with personalized services and improved customer experience, thereby improving revenues. Other measures include supporting the hybrid workplace, enabling business continuity to ensure security and privacy. The power of data and intelligence sharing across the ecosystem is a powerful way to foster industry resilience, giving FSI and ICT providers the opportunity to find new ways to collaborate for social good.

FSI key Business Priorities for 2022 and Beyond

The key business priorities of financial entities rely heavily on ICT and cloud services, though to achieve these objectives the technology must be properly combined with people management and process design.

Maximize business value through improved ROI, lower cost of operations, and higher efficiency: Infrastructure modernization and cloud adoption allow FSIs to reduce operational costs, avoiding oversized ICT infrastructure and providing the needed flexibility and scalability to take advantage of sound and secure technologies. The modernization of ICT systems has led most of the FSI industry to adopt a multivendor and multicloud architecture to achieve their priorities, improving the bottom line thanks to enhanced efficiency and cost optimization. The trend to leverage modern cloud-based architectures and innovative ICT solutions to gain higher efficiency is well consolidated. This trend has been confirmed in a recent IDC survey on the FSI major areas of IT technology investments for 2021: 27% were planning to invest in collaborative cloud platforms; 28% were planning to expand public cloud platform adoption (through IaaS, PaaS, or SaaS solution); and 44% were planning to devote recovery funds to infrastructural cloud

[3] Art.5 Proposal for a Regulation of the European parliament and of the council on digital operational resilience for the financial sector and amending Regulation (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

migration and adoption[4]. The pandemic fundamentally reshuffled business priorities; cost and efficiency (26%)[5] and performance (31%)[6] are top of the list. Growing attention is paid to value economics, looking at benefits related to cost optimization. On the revenue side, new ways and opportunities for business growth are made possible with data-driven innovation, data management, and artificial intelligence. Financial entities must undertake modernization efforts to transform their infrastructures, moving to more flexible, scalable, and powerful systems. They need, however, to remain in control of the proper functioning of ICT systems, internal and third-party, and of the quality of the services they offer to the public.

Provide customers with a personalized services offering based on data-driven innovation to improve service quality and speed. The benefits of cloud adoption and the modernization of the ICT systems are important in terms of cost efficiency and revenue growth. Financial entities are exploiting data-driven innovation to provide customers with more personalized and better services with shorter time-to-value, thereby improving revenues and customer engagement. In a recent IDC survey, 29% of financial entities stated that they would invest in data analytics as a priority to improve decision making and 40% stated that they run data-rich digital applications on external clouds. Indeed, the overwhelming amount of data to be processed requires extensive cloud resources, innovative technology, and modern architectures. These technological enablers have a positive impact on the revenue side of the financial entities supporting them to ensure fast delivery of innovative solutions generating new revenues.

Banks have changed their operating models, moving closer to their customers. With a proliferation of interaction points, and a huge amount of data available in the ecosystem, banks are undertaking efforts to integrate edge, core, and cloud data to gain real-time insights and leverage data-driven innovation. In a data-rich environment, the industry is also leveraging external data available in the ecosystem. ICT system modernization, combined with collaborative ecosystems, leads to better customer services and improved customer experience. For example, it's expected that by 2024 the use of shared industry cloud data will improve decision time on commercial loans by 50%[7].

The relevance of data-driven innovation and the benefits of collaboration are also witnessed by the fact that 59% of financial institutions are already actively involved in digital ecosystems and 26% are planning to move into collaborative ecosystems[8].

Protect the integrity of operations and data with appropriate data governance and best in class security features including encryption, identity management, and strong customer authentication. The pandemic has boosted digitalization with an exponential growth of data to manage and protect. The overwhelming amount of data has created a data-rich ecosystem to be exploited for business growth with hyper-personalized services. Considering that data is core to delivering satisfactory customer experience and designing innovative services, the importance of

[4] Source: IDC Industry Acceleration Survey, April 2021 (n=197 FSI)
[5] Source: IDC Industry Acceleration Survey, April 2021 (n=197 FSI)
[6] Source: IDC Industry Acceleration Survey, April 2021 (n=197 FSI)
[7] Source: IDC FutureScape: Worldwide Corporate Banking 2022 Predictions, November 2021
[8] Source: IDC Industry Acceleration Survey, April 2021 (n=197 FSI)

sound and consistent data governance and secure data protection is clear. The European strategy for data[9] sets out four pillars — data protection, fundamental rights, safety, and cybersecurity — as essential prerequisites for a society empowered by data. FSIs and their ICT third-party service providers must deploy all means and technologies to support a sound data governance and ensure the consistency of data managed in their ICT systems, which are often fragmented and stratified. They need to guarantee data integrity and secure, controlled access to data. Data governance and the protection of access to data is important to ensure that only people that have a need to know have the right to access some sets of data, which requires the deployment of all authorization and access control features. Data protection is also key in the fight against external malicious agents that are willing to penetrate ICT systems to perpetrate fraud or cyberattacks. Data is also an asset to protect customers against fraud and can be exploited well leveraging artificial intelligence and machine learning. It is therefore of paramount importance for the FSI to select third-party ICT service providers that commit to keeping up with the best available security features and standards to preserve the confidentiality, integrity, and availability of data.

Ensure business continuity and optimize workforce transformation in a hybrid work environment. Financial entities have been adopting business continuity and disaster recovery plans for many years and are used to complying with the regulatory requirements that define their obligation to design, implement, test, and pen-test their procedures. Over time, FSIs have adopted comprehensive risk management procedures to ensure their compliance with multiple regulations. There are now two new aspects of ICT risk management that financial entities consider. The first is linked to the hybrid work environment that has been boosted during the pandemic, and the second is linked to the extension of compliance obligations along the supply chain. With the upcoming DORA regulation, to have "*sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks*"[10], each critical ICT third-party service provider to financial entities will undergo the direct supervision of the European Supervisory Authority that will act as lead overseer. The direct obligation of the ICT third-party service provider reinforces end-to-end digital operational resilience covering a significant part of the ICT risks along the supply chain of the modern distributed architectures of the financial entities. To enhance end-to-end digital operational resilience, the DORA regulation proposal also foresees that "*where ICT third-party service providers are included in the remit of the threat-led penetration testing, the financial entity shall take the necessary measures to ensure the participation of these providers.*"[11]

In addition to traditional disaster recovery and business continuity plans, there is special consideration for hybrid work environments. New workplace models have become possible

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, A European strategy for data, COM (2020) 66 final.
[10] Art.30 Proposal for a Regulation of the European parliament and of the council on digital operational resilience for the financial sector and amending Regulation (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595
[11] Art.23 Proposal for a Regulation of the European parliament and of the council on digital operational resilience for the financial sector and amending Regulation (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

thanks to digital tools, and these have shown to be valuable when unforeseen events such as a pandemic or other external shocks disrupt the business-as-usual operational models. The pandemic has pushed FSIs, like many other enterprises, to leverage digital tools to enable remote working and thereby guarantee business continuity. Hybrid workplaces, together with multichannel customer interactions and overall digital transformation, have augmented the cyberattack surface and require additional workforce education to improve the cybersecurity awareness and skills that are very relevant when operating remotely.

Collaborative tools have enabled financial services business continuity and have become an integral part of risk management to achieve digital operational resilience. The introduction of collaborative tools based on cloud infrastructure has been dramatically important for social resilience under the pandemic restrictions and has allowed the financial industry to support corporations and citizens under stress. The workplace will remain hybrid. It is therefore time to move to a strategic approach to build a future-oriented digital workplace. This augmented FSI operational space will be carefully addressed as part of risk management policies and in business continuity procedures. The hybrid workplace should be considered, at the same time, as a wider vulnerability to be protected as well as a business continuity tool to be leveraged.

Enhance resilience and improve risk management with collaborative digital resilience procedures and information sharing: In the highly interconnected financial industry, collaboration in the ecosystem is also important when it comes to enhancing resilience. Two kinds of information sharing foster industry resilience, leveraging data to the benefit of the whole industry. The first is linked to mandatory collaboration of the FSI with supervisory authorities, and the second is based on voluntary information sharing among trusted partners.

- Harmonized mandatory incident-reporting enhancing digital operational resilience with consistent policies and procedures is a goal FSIs must pursue for its own sake. Moreover, sharing data about ICT-related incidents can benefit the whole industry since it allows the improvement of detection and reaction capabilities, especially in the case of large-scale cyberattacks. Mandatory incident reporting is a requirement foreseen in many regulations, and it is often fragmented or inconsistent across multiple jurisdictions. These issues are well known to the FSI industry, which copes with them every time they must comply with ICT-related incident reporting obligations. Thanks to the upcoming digital operational resilience regulation, this FSI compliance obligation will benefit from harmonized mandatory incident reporting frameworks.
- Voluntary info sharing is a great opportunity for social good and to enhance overall digital operational resilience, reducing systemic risk. The EU regulators support the opportunity to leverage the data-rich ecosystem, joining arrangements for voluntary information sharing among trusted entities. In recent years, collaboration based on voluntary info-sharing has proven to be successful at sectorial and/or national level to enhance defensive capabilities and threat detection techniques. Under the DORA regulation proposal, these collaborative arrangements are encouraged to foster the resilience of the whole financial industry. Collaborative digital resilience procedures and information sharing reduce systemic risk, enhance resilience, and improve risk management,

protecting society from large scale cyberattacks. The regulators have recognized the value of data-driven innovation and, in addition to a more harmonized mandatory incident reporting, are foreseeing the possibility to adhere to voluntary info sharing arrangements, overcoming some general data protection regulation (GDPR[12]) restrictions and allowing FSIs to share relevant data on ICT-related incidents among trusted partners to foster financial entities' defensive capabilities. Data management that integrates multiple data sources can support better risk management processes. Leveraging data analytics, financial entities can improve their ability to promptly detect malicious activities representing significant cyber threats.

Focus on Key DORA Regulation Requirements

Operational Resilience is no longer a "nice to have", but DORA will take resilience to the next level

European regulators have recognized the major role of ICT third-party service providers as an infrastructural backbone to the financial industry and are aware of the risks related to the reliance of the EU financial sector on ICT providers. There is a shift in regulations from indirect control to a direct ESA supervision over relevant designated ICT third-party providers, implying the need to:

- Encompass ICT and cloud providers within revised risk management procedures considering the expanded oversight scope of the financial industry European Supervisory Authorities (ESAs) that directly cover the designated ICT third-party service providers.
- Foster the resilience, business continuity, and availability of ICT systems with state-of-the art ICT technology and processes to manage security, minimize risks, and ensure data protection.
- Undertake appropriate testing and penetration testing with the ICT third-party service providers.
- Enhance data-driven operational resilience with voluntary info sharing arrangements and advanced data analytics.
- Streamline compliance obligations for financial entities thanks to the move towards the harmonization of multiple and fragmented mandatory incident reporting requirements.

Actionable Recommendations for Financial Institutions

Key considerations for FSIs to futureproof their organization

- Enhancing hybrid workplace tools and processes: FSIs deploying hybrid workplaces to ensure business continuity under adverse circumstances should move from a tactical to a

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data: https://eur-lex.europa.eu/eli/reg/2016/679/oj

strategic approach, implementing performance measures and looking at ways to attract, reskill or upskill, and retain talent in a hybrid work environment.

- Reviewing operational processes, including the hybrid workplace, to enhance the resilience of all their operations, everywhere they take place, combining efficiency and security. FSIs must bear in mind that hybrid workplace operations expand the cyberattack surface and should address blurring boundaries with a structured approach.
- Extending operational resilience to the augmented financial institutions space covering end-to-end stakeholders including omnichannel customer interconnections.
- Improving operational resilience by fostering resilience across all key internal company operations with sound data governance and data sharing architecture: designing a robust data strategy to ensure that consistent data is available across operations, ensuring consistency, integrity, confidentiality, and data protection.
- Gaining additional benefits from tighter cooperation with ICT providers that can lead to innovative solutions and improved cost efficiencies, and even to design new procedures to enhance combined digital operational resilience.

To prepare for the introduction of the DORA regulations, FSIs should:

- Review their risk management procedures and compliance processes, with a focus on end-to-end digital operational resilience.
- Ensure also that their ICT third-party service providers fulfil the mandatory regulatory requirements and that they enhance their risk management procedures.
- Leverage the benefits of streamlined mandatory ICT-related incident reporting frameworks and review internal procedures; take advantage of voluntary info sharing, leveraging the data to improve resilience. Evaluate and join appropriate cyber threat information sharing agreements.
- Improve resilience beyond the individual FSI space through collaborative information sharing within the trusted ecosystems. FSI should be prepared to manage all the available data to leverage it to improve their defensive capabilities and threat detection techniques.
- Identify possible joint efforts with critical ICT providers to comply with digital operational resilience regulatory requirements. A long-term partnership can be established with trusted ICT third-party providers, given the high level of interconnections and interdependencies among them, to fulfil the digital operational resilience regulatory requirements.

Challenges

ICT third party providers and cloud service providers must provide their FSI customers with the best available security features and with robust business continuity policies and procedures. Nutanix is already committed to maintaining robust security and privacy management systems

in line with the security management ISO Standards[13], and will continue to do so according to the evolution of standards and certifications.

Since financial institutions rely on the visibility provided by the Nutanix Unified Control plane to detect incidents, Nutanix will also have to ensure through contractual arrangements its ability to provide 100% accurate visibility in real-time 24x7 to support mandatory incident reporting within stringent timeframes under different regulatory requirements.

Considering the shift in the regulatory evolution of end-to-end digital operational resilience, Nutanix will also have to review and fine tune its risk management procedures, adopting appropriate processes and procedures. Nutanix should be able to offer its customers service level agreements that are consistent with robust risk management policies, business continuity, and disaster recovery procedures.

ICT third-party providers and cloud service providers should review their role in the ecosystem since they have been identified as a relevant component of the financial industry and they can envisage formalizing long-term partnerships with customers to enhance operational resilience. Managing security with best-in-class solutions and keeping up with best practices, Nutanix should reinforce its positioning as a trustworthy ICT provider enabling business continuity and operational resilience.

Given the nature of its services, it is important for Nutanix to also have a closer look at regulatory evolution to get a clear understanding of how the regulators see the role of architecture orchestrators under DORA regulations. Nutanix should be ready to undertake joint efforts with its financial customers to identify ICT operational risks and to jointly manage the regulatory pressure and governance to mitigate them.

[13] ISO/IEC 27001:2013 Requirements for information security management systems
ISO/IEC 27017:2015 Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27701:2019 Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management
ISO 28000:2007 Specification for security management systems for the supply chain

MESSAGE FROM THE SPONSOR

Nutanix Enterprise Cloud and the Modern Financial Services Datacenter

Nutanix simplifies IT infrastructure while simultaneously providing the secure and cloud-like datacenter necessary for financial services digital transformation.

Download the cloud and datacenter brief.

About the Analyst

Maria Adele Di Comite, Research Director, European Financial Insights

Maria Adele is Research Director for the IDC Financial Insights European research team and is responsible for the IDC Financial Insights Corporate Banking Digital Transformation Strategies program. She has strong competencies in financial services strategy, cybersecurity, and regulatory evolution. She is an expert in B2B business strategy, with significant experience in financial services, system integration, and management consulting.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

Copyright and Restrictions