Digital Banking Resilience: Emerging Norms and Strategic Considerations

The rise of digital banking and the consequent focus on operational resilience

Infosys® | Finacle

Inspiring Better Banking

www.finacle.com

Contents

Preface

In an era defined by rapid digital transformation, resilience in banking has emerged as a non-negotiable priority. With the rise of digital banking, financial institutions worldwide face a compelling mandate to fortify their operational frameworks. The increasing reliance on digital infrastructure, compounded by the growing threat landscape and evolving customer expectations, demands that banks build resilience at every level—protecting not only their financial standing but also for the broader stability of the financial ecosystem.

This report, **“Digital Banking Resilience: Emerging Norms and Strategic Considerations”**, explores the pivotal forces shaping the focus on resilience in today’s digital banking landscape. Part one examines the drivers of digital operational resilience (DOR), from technology reliance and cyber threats to regulatory pressures and customer expectations. This section provides insight into why resilience is critical to sustaining trust and continuity in financial services.

In part two, we delve into the potential consequences of faltering resilience—not only for individual banks but also for their customers, the financial system, and the economy at large. This segment underscores how disruptions, financial losses, and regulatory scrutiny can erode trust and financial stability, emphasizing the imperative of robust resilience strategies.

Global convergence around DOR priorities is discussed in part three, where we outline the emerging commonalities across cybersecurity management, information and communication technology related risks management, incident response management, business continuity requirements, and third-party oversight. In the discussion, we examine the key areas where the standards are aligning across the banking sector, spotlighting shared priorities and practices.

Part four casts a spotlight on key legislations, emergent norms and regulatory guidelines, such as the Digital Operational Resilience Act (DORA) - Europe, the cross-industry prudential standard CPS 230 operational risk management (CPS 230) from Australian prudential regulation authority (APRA), principles for operational resilience - Basel committee on banking supervision (BCBS). We examine their applicability, core recommendations, and impact on resilience planning. These examples provide context on how leading regulatory standards are shaping operational resilience practices around the globe.

Finally, in part five, we present a holistic approach to digital resilience management, structured around three critical pillars: cyber resilience, platform resilience, and force majeure preparedness. We also introduce Infosys Finacle’s strategy, designed to empower banks in achieving digital resilience through a layered approach at the organizational, product, and process levels. This approach highlights the essential role of an integrated security and resilience posture, advanced system architecture, and robust continuity planning—all vital to safeguard against today’s complex threat landscape.

By providing a comprehensive understanding of digital resilience imperatives, this report aims to guide banks and financial institutions in strengthening their operational frameworks, fostering trust, and ensuring stability in a rapidly changing environment.

1

Factors amplifying the focus on digital resilience in banking

The banking sector, once primarily reliant on physical infrastructure, has undergone a profound transformation, becoming increasingly digitized. This digital evolution, while offering numerous benefits, has also introduced new vulnerabilities that necessitate robust digital resilience measures.

A confluence of factors is driving a heightened focus on digital resilience within the banking industry, which can be viewed through three distinct optics. First, technology-led factors highlighting the vulnerabilities that arise from a rapidly evolving digital landscape. Second, operational-related factors underscoring the need for banks to enhance their security measures and operational capabilities to ensure uninterrupted service. Lastly, the customer-centric and regulatory optic emphasizing the growing expectations from consumers for seamless access to banking services and the corresponding regulatory pressures that accompany these demands.

The following sections delve into the key factors, examining their implications for the industry.

Increasing reliance on technology and the interconnectedness

Banking has become highly digitized, with institutions also relying heavily on ecosystems of third-party technology vendors, service providers, and fintech companies. Systems are interconnected both within banks and with external platforms, amplifying vulnerability to cascading failures. Disruptions — whether from cyberattacks, cloud outages, or vendor failures — can have far-reaching effects, impacting not just individual institutions but the entire financial system. As banking becomes borderless, the need for digital resilience continues to grow to prevent destabilizing risks across the global financial landscape.

Complexities introduced by new technologies

New technologies such as AI, blockchain, cloud computing, and 5G are reshaping banking while also introducing new risks. While these innovations enhance efficiency and customer experience, they present challenges such as data sovereignty issues, algorithmic bias, and regulatory compliance complexities. Operational resilience is becoming increasingly vital as banks navigate the vulnerabilities associated with adopting advanced technologies. Addressing these complexities is essential for ensuring both security and continued customer trust.

Escalating cybersecurity threats

The rise of digital technologies, including increasing cloud adoption, has expanded the attack surface for cybercriminals. Banks, given their economic importance and the sensitive nature of the data they handle, are prime targets for cyberattacks. Regulatory bodies are becoming ever more aware of the systemic risks cyber incidents pose — not just to individual banks but to the broader financial ecosystem. The frequency of ransomware, data breaches, and distributed denial-of-service attacks is pushing cybersecurity resilience to the top of the sector’s priorities.

Surge in digital transactions

With banking services now available on-demand and across multiple channels, the volume of digital transactions has surged, including real-time and microtransactions. This exponential growth requires banks

to ensure their platforms can scale effectively to handle peak loads without disruption. Regulatory emphasis on robust scalability measures — including cloud elasticity, load balancing, and stress testing — is intensifying, underscoring the necessity for digital infrastructure that can maintain performance during periods of high demand.

Rising customer expectations and regulatory pressures for service continuity

Customers expect uninterrupted, 24/7 access to financial services, whether through online or mobile banking, or other digital access points of choice. Any disruption harms a bank's reputation and results in significant financial losses. Regulatory bodies, recognizing this critical demand, have introduced policies mandating that banks ensure operational continuity even in the face of unexpected events. Service availability is becoming a key component of both customer satisfaction and regulatory compliance.

Costs to customer trust and protection

Customer trust is the foundation of banking; however, the increasing frequency of cyber incidents threatens that trust. As consumers grow more reliant on digital banking, they face greater risks of identity theft, fraud, and data breaches. Regulators are tightening data protection rules, emphasizing the need for banks to implement stringent safeguards. Protecting personal information remains critical for maintaining customer confidence in the digital banking age.

In summary, while the six factors outlined above are instrumental in amplifying the focus on digital resilience in banking, adopting a proactive stance in risk management is becoming increasingly imperative. A shift from reactive to proactive risk management is rapidly emerging as a significant driver behind the development of new digital resilience frameworks. Historically, many institutions responded to disruptions only after they occurred; however, this approach is no longer viable in today's fast-paced digital landscape. Regulatory bodies now demand that financial institutions proactively identify potential risks, conduct regular resilience testing, and implement robust safeguards to prevent disruptions.

2

The negative consequences of faltering digital resilience

In the rapidly expanding digital banking landscape, faltering digital operational resilience can have profound and far-reaching consequences. With numerous factors and forces at play, the ability of banks to maintain robust and secure digital operations is crucial not only for their own stability but also for the broader financial system and economy. When banks experience digital failures, the impacts extend beyond immediate operational challenges, influencing financial losses, regulatory scrutiny, and even eroding public trust. The rest of the discussion will explore what this means for the bank, the customer, the financial system, and finally, the overarching implications on the economy.

For the bank (s):

Financial losses from cyberattacks, outages, and data breaches can be severe for banks, encompassing both direct costs such as remediation, fines, and legal fees, and indirect costs like lost revenue, customer churn, and reputational damage. Operational disruptions from digital outages further exacerbate these losses by impeding critical banking services, hindering customer transactions, payment processing, and internal operations. This results in decreased productivity, heightened customer frustration, and a decline in overall business efficiency. Non-compliance with digital operational resilience (DOR) regulations can invite regulatory scrutiny, leading to investigations, fines, and potential operational restrictions that tarnish the bank's reputation and disrupt its operations. Additionally, security incidents and operational failures erode public trust, causing customer churn and making it challenging to attract new clients, which hampers the bank's growth prospects.

For the customers:

Service disruptions caused by outages can prevent customers from accessing their accounts, making payments, or conducting transactions, leading to significant inconvenience and frustration while hindering their ability to manage finances effectively. Cyberattacks pose further risks by granting unauthorized access to customer accounts, resulting in fraudulent transactions and financial losses. Data breaches also expose sensitive information, increasing the risk of identity theft and financial fraud. Such security incidents and disruptions can severely erode customer trust in the bank's ability to protect their information and assets, prompting them to seek more reliable competitors.

For the financial system:

A widespread cyberattack or IT outage at a major bank can create systemic risk, triggering a domino effect that impacts other institutions dependent on its services. This can destabilize the financial system and disrupt critical financial flows. Furthermore, incidents at a single bank can lead to a broader loss of market confidence, which may cause financial instability and heightened market volatility.

For the broader economy:

Instability and declining confidence in the financial system can significantly reduce investment from both businesses and consumers, ultimately hindering economic growth. Additionally, outages that disrupt critical services, such as payment processing, can impact the ability of businesses and individuals to conduct everyday transactions. This disruption creates a ripple effect, further affecting economic activity and stability across various sectors.

3

Digital operational resilience priorities are converging, globally

Across the banking industry, digital operational resilience laws are increasingly converging to address the growing complexities and risks in a highly digitalized environment. Despite regional variations, these laws share common objectives: making sure banks can endure, react to, and bounce back from disruptions that threaten their operations. From things such as governance and oversight, to managing cyber threats, third-party risks, prudent ICT management and several such critical areas, the banking sector faces a unified regulatory push to enhance resilience. The convergence highlights a collective recognition of the critical role that operational resilience plays in safeguarding financial stability, customer trust, and regulatory compliance across the sector. In the following discussion, we explore key areas where norms are unifying globally, highlighting shared priorities and practices.

Collective considerations on information and communication technology (ICT) risk management

The management of ICT risks is essential for organizations to ensure operational resilience, particularly in an era of increasing digitalization and interconnectivity. As ICT risks evolve, there is a clear convergence across global frameworks that guide banking institutions in safeguarding their technology systems and processes. This convergence revolves around key areas such as establishing a comprehensive risk management framework, ensuring strong governance and oversight, maintaining accurate inventories and mapping of ICT assets, and conducting thorough risk assessments and prioritization. Additionally, there are converged practices related to testing, ICT operations security, project and change management, network security, among others. The common interests, and the key considerations include:

- **A well-rounded ICT risk management framework creation** that encompasses all operational aspects of an organization's digital systems. This framework provides a structured approach to identifying, mitigating, and responding to risks that could affect business continuity or compromise data integrity. The framework addresses risks across various dimensions, including internal processes, external threats, and third-party service providers.
- **Governance and oversight norms** that plays a crucial role in managing ICT risks by ensuring that the risks are prioritized at the highest levels of the organization. Strong governance ensures that ICT risk management is integrated into the broader operational strategy and that leadership takes direct responsibility for overseeing the organization's resilience efforts.
- **Creation of a detailed inventory of all ICT assets.** This includes hardware, software, networks, and data systems, as well as third-party resources and cloud infrastructure. Accurate asset mapping is essential to identify vulnerabilities, assess dependencies, and prioritize protection efforts.
- **Risk assessment related guidelines** that form the backbone of ICT risk management by enabling banks and financial institutions to evaluate the likelihood and impact of potential risks. Through regular and thorough assessments, banks can identify the most critical vulnerabilities in their systems and prioritize resources to address the high-impact risks.

- **Stress testing and scenario planning related norms.** Entities should simulate various types of disruptions, from cyberattacks to system outages, to test how their ICT systems will respond under pressure. This proactive testing helps uncover potential weaknesses and prepare for real-world incidents.
- **ICT operations security norms** that include implementing cybersecurity measures to guard against data breaches, unintended access, and various other cyber related threats. It encompasses securing networks, ensuring encryption, and maintaining stringent access controls.
- **Project and change management guidelines** for implementing new technologies, updating software, or migrating systems.
- **Norms related to securing network infrastructure** for protecting sensitive data and ensuring the uninterrupted operation of ICT systems.

Global emphasis on cybersecurity as a core priority

Cybersecurity has emerged as one of the most critical aspects, with regulatory frameworks around the world increasingly converging on this shared priority. As banks continue to rely on digital infrastructure to deliver essential services, they face rising threats from cyberattacks, data breaches, and fraud. This has prompted global regulators to enforce stringent cybersecurity measures to ensure banks can safeguard sensitive financial information, maintain the integrity of their systems, and protect the interests of customers. The common requirements include:

- **Adopting robust security protocols** to prevent unauthorized access to systems, data, and networks. Laws typically mandate encryption, multi-factor authentication, and advanced monitoring tools to detect and respond to potential breaches in real time.

- **Incident response plans** to ensure that banks have the ability to contain and mitigate the impact of cyber incidents swiftly.
- **Continuous cybersecurity testing** to regularly conduct penetration tests, vulnerability assessments to evaluate their preparedness for various types of cyber threats. This ensures that cybersecurity protocols are not only implemented but are also effective in the face of evolving risks. Regulatory bodies expect these tests to be comprehensive, identifying both internal vulnerabilities and external threats posed by cybercriminals.
- **Vendors to meet the stringent cybersecurity standards** and regularly undergo security assessments.
- **Cybersecurity linked with broader data protection laws,** reflecting the convergence of operational resilience with privacy concerns.

Consistent approaches to incident management

Incident management has become a cornerstone of digital resilience frameworks across the global banking industry, with regulations converging on the critical need for effective reporting, timely notifications, and transparent disclosures. As operational disruptions, cyber incidents, and system outages increasingly threaten the stability of financial institutions, incident management processes are being strengthened to ensure rapid response and limit the impact on banking operations and customers. The focus areas include:

- **Timely incident reporting** wherein banks are typically mandated to report significant operational or security incidents to relevant regulatory authorities within a specific timeframe. This prompt reporting ensures that regulators can monitor the impact of the disruption, assess any systemic risks, and coordinate responses where necessary.
- **Notification requirement norms** wherein banks must notify not only regulators but also their customers and affected parties in the event of a major disruption, especially if it compromises sensitive data or impacts key services. These notifications are designed to maintain transparency, allowing customers to take necessary precautions or make informed decisions.
- **Emphasis on incident disclosures** wherein financial institutions are often required to disclose the nature of the incident, its root cause, and the steps being taken to rectify the situation and prevent future occurrences.
- **Root cause analysis and post-incident review norms** requiring banks to conduct detailed analyses following an incident to identify its underlying cause and take corrective actions. These post-incident reviews are crucial for improving future resilience.
- **Testing and scenario planning norms** covering proactive measures like testing response plans and running scenario exercises to gauge incident response readiness.

- **Collaboration with regulators and industry bodies** which requires banks to share insights from their incidents with industry peers and authorities, to support a collective understanding of risks and vulnerabilities.

Common foundations of business continuity and disaster recovery

Business continuity and disaster recovery management is a foundational component of digital resilience in banking, with regulatory frameworks worldwide recognizing its critical importance. There is a strong regulatory push to ensure continued service delivery, maintain customer trust, and safeguard financial stability. Key focus areas include:

- **Conducting thorough business impact analysis** requiring banks to identify critical functions, assess potential disruptions, and quantify the financial and operational impacts of these interruptions. It allows banks to prioritize resources, design recovery strategies, and allocate adequate funding to the most essential services, ensuring a clear understanding of how interruptions could affect both operations and customers.
- **Comprehensive business continuity planning (BCP)** that involves outlining steps to maintain key banking services in the event of a disruption, including establishing alternative work arrangements, backup facilities, and redundancy measures. This ensures that banks can continue core operations even during major disruptions, minimizing the impact on clients and the financial ecosystem.
- **Disaster recovery (DR) planning** that specifically focuses on restoring IT systems, data, and infrastructure following an interruption. Banks are required to implement DR strategies that include data backups, failover systems, and alternate site arrangements.
- **Ongoing training and simulations** that stresses the need to ensure readiness for BCP-DR activation. Accordingly, banks must conduct regular drills and scenario-based training to test their plans, help staff understand their roles during incidents and validate the effectiveness of continuity and recovery procedures.

- **Assessing the resilience of third-party vendors** as part of the BCP-DR efforts. Given banks' reliance on external service providers, particularly for cloud-based and outsourced operations, understanding vendors' continuity and recovery capabilities is highly essential. It includes assessing vendors' BCP-DR policies, establishing contractual recovery time objectives (RTOs), and ensuring that third parties are held to the same resilience standards.
- **Continuous testing and planning the updates** in response to new threats, technological advancements, and organizational changes.

Aligned practices for managing third-party risks

Effective third-party risk management is crucial for digital operational resilience in banking, with global regulatory standards underscoring the importance of strong controls and comprehensive oversight of vendor relationships. As banks increasingly rely on third-party providers for critical services, they face heightened risks around data security, compliance, and operational continuity. To mitigate these risks, regulatory frameworks insist focus on several key areas, that includes:

- **Conducting comprehensive due diligence** before entering into relationships with third-party providers. This due diligence typically involves evaluating vendors' financial stability, security measures, data protection practices, and disaster recovery capabilities.
- **Setting up effective contract management** as it sets out the terms and expectations for service delivery, data handling, security protocols, and incident response. Regulatory guidelines most often mandate banks to establish clear service level agreements (SLAs) - whether business, IT, or both as applicable, also define recovery metrics, and include accountability clauses.
- **Ensuring third-party providers' adherence to regulatory requirements and internal policies.** It involves continuous monitoring of vendors' compliance with relevant laws, such as data protection regulations, and cybersecurity standards. Regulatory frameworks also emphasize the need to regularly review vendors' compliance status, conduct audits, and demand certifications when necessary, reinforcing both legal and operational accountability.
- **Performing risk assessments** to evaluate the evolving risks associated with vendors' operations, technology environments, and geopolitical factors that may impact service delivery.
- **Taking stock of incident response management** to ensure that vendors have robust incident management processes, timely notification protocols, and clear communication channels in case of disruptions.

Harmonized tactics for governance and reporting practices

Governance and reporting have become central pillars of digital resilience frameworks within banking, with regulatory standards worldwide placing a strong emphasis on structured oversight and clear accountability across organizational levels. Effective governance ensures that banks can proactively manage risks, respond to incidents, and foster a resilient culture. The recommendations include:

- **Establishing board-level oversight** wherein boards play a critical role in setting the strategic direction for digital resilience and are accountable for ensuring the institution's overall security and operational continuity. Regulations require board members to regularly review risk reports, approve resilience policies, and provide direction on key resilience strategies.
- **Ensuring management accountability** wherein management teams are responsible for implementing and monitoring resilience measures throughout the bank. Regulatory frameworks highlight the need for clearly defined roles and accountability within management, ensuring that specific individuals or teams are tasked with resilience-related functions. This accountability includes managing risks, ensuring compliance, and coordinating responses to potential disruptions.
- **Implementing enterprise-wide cadence and reporting.** Global regulations encourage banks to adopt standardized reporting cycles and use consistent metrics to assess resilience performance, enabling timely identification of risks and vulnerabilities.
- **Defining transparent, escalation protocols** that allow for swift responses to incidents. Banks are expected to establish pathways for escalating incidents from operational teams to senior management and the board, ensuring timely awareness and response to critical issues.

4

Towards a resilient future: Exploring key frameworks guiding digital banking operations

This chapter offers an overview of the changing dynamics of digital operational resilience in the banking industry, emphasizing key frameworks that are shaping practices, and policies. As financial institutions face mounting pressures from technological advancements and regulatory expectations, these frameworks offer valuable insights into the foundational efforts aimed at enhancing resilience. By exploring the key aspects of these guidelines, we will shed light on the ongoing initiatives that aim to fortify banks against potential disruptions and ensure a secure and reliable banking environment.

The Digital Operational Resilience Act (DORA), Europe

The context behind the promulgation of DORA

The DORA is a pioneering regulation by the European Union, crafted in response to the growing dependence of the financial sector on digital technologies and the mounting threat of cyberattacks. In recent years, cyber incidents targeting financial institutions have surged, leading to substantial financial losses and severe reputational damage. These events exposed significant vulnerabilities and underscored the need for a comprehensive, coordinated approach to cybersecurity and operational resilience. DORA was designed to address these concerns by establishing a robust framework for managing ICT (Information and communications technology) risks, aiming to fortify the resilience of the financial sector in Europe.

- One of the main reasons behind DORA is the increasing reliance of financial services on technology. From digital payments and online banking to data analytics and trading platforms, the financial sector's integration with digital infrastructure has introduced unprecedented efficiencies but also heightened its vulnerability to ICT-related disruptions. This dependence necessitates stringent measures to ensure that financial services remain reliable and uninterrupted, even when facing technological challenges. DORA's framework provides institutions with the structure needed to secure their operations against a wide range of digital vulnerabilities.
- Another critical factor is the growing sophistication and frequency of cyber threats. Cybercriminals are using several advanced tactics, including distributed denial of service (DDoS) attacks, ransomware demands, and phishing attacks, which present significant risks to financial institutions, their customers, and the wider economy. DORA's emphasis on robust cybersecurity practices helps financial institutions strengthen their defenses and stay ahead of these evolving threats, thereby safeguarding consumers and businesses from potentially devastating cyber incidents.
- Furthermore, DORA addresses the lack of regulatory harmonization across EU member states. Before DORA, financial institutions faced a fragmented landscape of cybersecurity and resilience regulations that varied from country to country, making it difficult to maintain consistent standards. By unifying these regulations, DORA promotes regulatory consistency across the EU, which simplifies compliance for financial institutions and enhances the overall coordination and effectiveness of ICT risk management across borders.
- Perhaps, DORA also represents a shift from reactive to proactive risk management. Traditional approaches often focused on containing and

responding to threats after they occurred. In contrast, DORA emphasizes prevention, early detection, and swift response, encouraging institutions to anticipate and mitigate risks before they escalate into full-scale incidents. This proactive stance helps build resilience within financial institutions, enabling them to minimize disruptions and maintain continuity.

DORA is set to enhance the operational resilience of the financial sector in Europe. This regulatory framework equips financial institutions to manage digital threats effectively, protecting both consumers and businesses from the financial and operational impacts of cyberattacks and other ICT-related disruptions. As a forward-looking initiative, DORA ensures that the financial sector remains robust in an increasingly digital world, fostering a safer, more resilient digital financial ecosystem across Europe.

The scope of DORA

The DORA applies across various financial and digital service providers, ensuring an elevated standard of operational resilience in the financial sector against ICT risks. The regulation specifies an extensive list of entities it governs, referred to collectively as “financial entities.” These include traditional financial institutions and a range of service providers that support digital and financial operations.

- Financial institutions covered by DORA encompass credit institutions, payment institutions (including those exempt under EU Directive 2015/2366), electronic money institutions, and account information service providers. Investment firms also fall under this regulation, as do crypto-asset service providers authorized under the markets in crypto-assets related regulation. Additionally, DORA extends to central counterparties, central securities depositories, trade repositories, and trading venues, all of which play critical roles in financial transactions and asset handling.

- DORA's scope further includes investment and fund managers, such as managers of alternative investment funds and management companies. Service providers related to reporting of data are also within its remit, as are insurance and reinsurance undertakings. In addition, DORA applies to institutions providing occupational retirement provisions, as well as insurance intermediaries, reinsurance intermediaries, and ancillary insurance intermediaries. Other entities such as administrators of critical benchmarks, credit rating agencies, securitization repositories, and crowdfunding service providers are also covered by DORA, reflecting the regulation's comprehensive approach to resilience in financial markets.

- Significantly, third-party service providers of ICT are also directly covered by DORA, given the integral role they play in supporting the digital operations of financial entities. This inclusion highlights DORA's proactive stance on managing third-party risks that could impact financial stability.

However, DORA excludes certain entities from its scope. These include certain insurance and reinsurance undertakings as per Directive 2009/138/EC, managers of alternative investment funds referred to under Article 3(2) of Directive 2011/61/EU, and occupational retirement provision institutions with pension schemes of 15 or fewer members. Other exempted groups include specific natural or legal persons exempted under Directive 2014/65/EU, smaller insurance intermediaries (such as SMEs, microenterprises), and post office giro institutions under Directive 2013/36/EU.

Lastly, member states have the option to exclude additional entities from DORA, specifically those referenced in points (4) to (23) of Article 2(5) of Directive 2013/36/EU, if based within the respective member state. Member states exercising this option must however inform the European Commission, which will then make this information publicly available.

Overall, DORA's extensive applicability highlights its intent to create a uniform standard for digital resilience across the EU's financial ecosystem, spanning both traditional financial entities and the ICT providers essential to their operations.

The 5 core pillars of DORA

The European Union's DORA has set out a framework with five key pillars. Together, they address both internal and external risks, mandating stringent controls and collaborative efforts that promote resilience, transparency, and uniform standards across the EU's financial sector. They include the following:

- **ICT risk management:** This is a foundational pillar that requires financial entities to establish a comprehensive framework for managing technology-related risks. It involves identifying and assessing risks associated with their ICT systems, implementing strong internal controls, and conducting continuous monitoring. The goal is to minimize operational disruptions by proactively managing potential vulnerabilities in digital infrastructure. DORA mandates that entities formalize risk management processes, such as ensuring secure data

handling, access controls, and risk reporting. By doing so, financial institutions are better equipped to withstand cyber threats and maintain continuity.

- **ICR related incident reporting:** The framework requires financial entities to develop structured procedures for identifying, handling, and reporting significant ICT incidents to ensure swift responses and transparency. When a major incident occurs, institutions must notify regulatory authorities within a specified timeframe, detailing the incident's nature, impact, and any mitigation efforts underway. This process not only helps manage individual crises but also enables authorities to gather insights into systemic threats affecting the sector across the region. By enforcing timely reporting, DORA aims to improve industry-wide awareness, coordination, and resilience against ICT threats.
- **Digital operations resilience testing:** This requires financial entities to regularly evaluate the robustness of their ICT systems against potential cyber threats, primarily. This involves a comprehensive suite of assessments, including vulnerability scans, continuity exercises, and penetration testing to identify and address weaknesses proactively. DORA mandates threat-led penetration testing (TLPT) for critical systems, simulating real-world attack scenarios to ensure systems can withstand advanced cyber threats. These tests help financial institutions strengthen defenses, protect critical functions, and ensure their operational stability.
- **ICT third-party risk management:** It emphasizes the importance of managing risks associated with outsourced ICT services, which are critical to the operations. This requires financial entities to thoroughly assess and monitor the security and resilience of third-party providers, especially for essential services such as cloud based operations, data processing, and cybersecurity. It mandates that institutions include risk-related clauses in contracts, covering aspects like data security, incident response, and service continuity. Additionally, financial entities must regularly review the performance and risk profiles of these providers, ensuring they can uphold the same resilience standards as in-house systems.
- **Information sharing:** This pillar promotes collaboration within the sector by encouraging institutions to share insights on cyber threats, vulnerabilities, and best practices. The exchange aims to build a collective defense against ICT risks, allowing entities to proactively address emerging threats and avoid common pitfalls. Financial institutions are also encouraged to form alliances or such arrangements, participate in industry forums, and contribute to a broader knowledge base on cybersecurity resilience. By fostering transparency and open communication, DORA helps the financial sector enhance its preparedness, mitigate risks collectively, and create a more unified response to cyber threats.

The timeline

The DORA outlines a clear timeline for implementation and compliance. It officially came into effect on January 16, 2023, marking the beginning of a transition period for financial entities across the EU. This period is crucial for institutions to prepare for the new requirements and implement necessary changes to their operational resilience frameworks. The act's full applicability will commence on January 17, 2025, at which point all financial entities, such as banks, fintechs, payment service providers and others, must comply with its stipulations regarding incidents management, overall ICT risk management, and third-party risk management. They should closely monitor the development and implementation of regulatory technical standards (RTS) and implementing technical standards (ITS) during the preparatory phase, prior to full commencement. During the transition period, organizations are expected to conduct thorough assessments of their ICT systems, establish risk management frameworks, and ensure incident response plans are in place. This timeline allows for a systematic approach to aligning existing practices with DORA's regulations.

The cross-industry prudential standard CPS 230 operational risk management (CPS 230), from Australian prudential regulation authority (APRA)

CPS 230, the standard from APRA for operational risk management, is a crucial regulatory framework designed to enhance operational resilience across APRA-regulated entities, such as in the banking, insurance, and superannuation sectors. By focusing on resilience, governance, and risk assessment, APRA aims to foster a more robust financial system that can withstand operational disruptions effectively.

The key objectives

The CPS 230 established by the APRA aims to enhance operational resilience among regulated entities, ensuring they can maintain operations and recover quickly from disruptions. The standard mandates the development of robust risk management frameworks for identifying, assessing, and managing operational risks effectively, while promoting strong governance and accountability at the board and senior management levels. CPS 230 aims to foster a culture of risk awareness, facilitate consistency across sectors, and ensure that risks associated with third-party service providers are adequately managed. It encourages continuous improvement in operational risk practices through regular testing and incident management processes. Ultimately, the standard aims to ensure compliance and transparency, strengthening the overall stability and resilience of Australia's financial sector to protect consumer interests and uphold confidence in the system.

The focus areas

The main aspects of CPS 230 include the following:

- **Operational risk management framework:** Entities are required to establish a robust operational risk management framework that includes policies, processes, and controls for examining, evaluating, managing, and monitoring operational risks. Also, the focus includes:
  - **Governance structure:** CPS230 emphasizes the importance of strong governance, requiring entities to have clear accountability and oversight for operational risk management at the board and senior management levels. This includes defining roles and responsibilities as appropriate.
  - **Risk identification and assessment:** Entities must implement systematic processes to identify and assess operational risks. This involves evaluating potential risks, their impacts, and the likelihood of occurrence to prioritize risk management efforts effectively. CPS 230 also mandates the design and implementation of effective controls to mitigate identified operational risks. These controls should be integrated into the entity's daily operations and continuously monitored for effectiveness.

- **Incident management:** A crucial aspect of CPS 230 is the requirement for robust incident management processes. Entities must have procedures in place for identifying, reporting, and analyzing operational risk incidents to learn from them and improve risk management practices.
- **Service provider management:** CPS 230 mandates robust service provider management practices. Entities must identify and assess material service providers, conduct due diligence, and implement effective oversight mechanisms. This includes ongoing monitoring, risk assessment, and contractual requirements to ensure service providers align with the organization's risk appetite and operational objectives.
- **Business continuity and recovery:** Entities are expected to develop and maintain business continuity plans and recovery strategies to ensure that critical functions can continue during and after operational disruptions.

Apart from the key aspects mentioned above, CPS 230 also encompasses several other important principles. One of these is testing and assurance, which mandates regular testing and validation of the operational risk management charter to ensure its effectiveness and readiness to respond to potential disruptions. Additionally, compliance and reporting are critical; entities must demonstrate adherence to CPS 230 and maintain transparency in their operational risk management practices through appropriate reporting mechanisms to APRA. Furthermore, CPS 230 emphasizes the need for a culture of risk awareness within organizations, encouraging employees at all levels to actively participate in risk management practices, and positively influence the entity's overall resilience.

CPS 230 timelines

APRA released the final CPS 230 framework in July 2023. The standard will come into full effect on July 1, 2025, for most APRA-regulated entities. Non-significant financial institutions (non-SFIs) have one additional year to comply with certain requirements, until July 1, 2026. APRA expects regulated entities to proactively prepare for implementation, rather than waiting until the last minute. Key milestones included identifying critical operations and material service providers by mid of 2024 and establishing tolerance levels for critical operations by the end of 2024.

Implications of CPS230

APRA-regulated entities face increased regulatory scrutiny and potential enforcement actions for non-compliance with CPS 230. Implementing the standard can significantly enhance operational resilience and ability to withstand disruptions. This may necessitate strategic changes, including investments in technology, personnel, and processes. Careful assessment and management of third-party risks is crucial. Fostering a strong risk culture is essential for effective implementation.

Principles for operational resilience - Basel committee on banking supervision (BCBS)

The BCBS has established a comprehensive set of principles for operational resilience (POR), underscoring the importance of maintaining effective and reliable banking operations in the face of disruptions. In a rapidly evolving financial landscape characterized by increasing complexity and interconnectedness, these principles aim to equip banks with the frameworks necessary to anticipate, prepare for, respond to, and recover from adverse events. By emphasizing proactive risk management, robust governance, and the integration of resilience into business strategies, the BCBS principles serve as vital guidelines for banks striving to safeguard their operations and ensure continued service delivery amidst challenges. The POR principles aim to strengthen banks' ability to operate resiliently in the wake of adverse events, such as pandemics, cyberattacks, and natural disasters. These principles build upon the existing principles for the sound management of operational risk (PSMOR) and introduce a more comprehensive approach to operational resilience, focusing on critical operations, incident management, and business continuity planning.

The definition of operational resilience and its key considerations

The BCBS defines operational resilience as a bank's capacity to sustain critical operations during disruptions. This concept emphasizes the necessity for banks to not only survive adverse events but also to continue delivering essential services. A proactive approach is crucial; banks must anticipate disruptions by identifying potential threats and failures before they occur. The ability to act in response, adapt, and recover from disruptive events is central to operational resilience, which aims to minimize the impact of such events on critical operations.

In formulating their operational resilience strategies, banks should operate under the assumption that disruptions will occur. This assumption should shape their overall risk appetite and tolerance for disruption, which is defined as the degree of disruption a bank is prepared to tolerate under various severe yet reasonably likely situations. The concept of critical operations is central to this

framework, encompassing a broad range of activities, processes, and services essential for the bank's functioning and its role in the financial system. The determination of what constitutes critical operations is influenced by the probable material impact on the entity and systemic stability, acknowledging that this definition will vary based on each bank's unique characteristics, such as size, complexity, and role in the financial system.

To effectively govern operational resilience, the BCBS references a framework consisting of three lines of defense: business unit management, an independent operational risk management function, and independent assurance. This structure ensures clear responsibilities and effective oversight, allowing banks to implement operational resilience measures tailored to their specific contexts. Ultimately, the BCBS principles provide a comprehensive approach to enhancing banks' resilience, enabling them to safeguard critical functions and maintain stability in the financial system.

Guidance basis 7 key principles

The BCBS has outlined seven key principles for operational resilience. Directionally, the key considerations include:

- **Governance:** Banks should establish or leverage strong governance frameworks to oversee operational resilience, including clear responsibilities, risk appetite statements, and robust risk management processes.
- **Operational risk management:** Banks should have effective operational risk management practices in place to identify, assess, and mitigate operational risks that could impact their operational resilience.
- **Business continuity planning and testing:** Banks should develop comprehensive business continuity plans (BCPs) to guarantee the continuity of operations that are critical, in the event of disruptions. These plans should be regularly tested and updated.
- **Mapping the interconnections and interdependencies of critical operations:** Banks should map their critical operations to gain insight into their interconnections and dependencies, helping to identify potential vulnerabilities and likely resultant impacts.
- **Third-party dependency management:** Banks should manage their relationships with third-party service providers to ensure that they meet the bank's operational resilience requirements. This includes necessary due diligence, contractual arrangements, and ongoing monitoring, trade-off decisions.
- **Incident management:** Banks should have robust incident management processes in place to respond effectively to operational incidents, including timely detection, containment, and recovery actions.
- **Resilient information and communication technology (ICT), with due focus on cyber security:** Banks should invest in resilient ICT infrastructure and implement firm cybersecurity measures to safeguard their systems, and underlying data from cyber threats.

5

Banks and FIs need to take a holistic approach to managing emergent DOR expectations

Banks face an unprecedented demand for operational resilience to safeguard against disruptions, both anticipated and unforeseen. As digital transformation accelerates, the ability to maintain stability, security, and continuity has become critical—not only for protecting against cyber threats but also for ensuring robust platform performance and continuity during unforeseen events. To achieve this, banks must focus on three pivotal areas of resilience:

Defending against external threats – the cyber resilience factor:

Banks must stay ahead of evolving cyber threats by proactively defending against malicious actors. This demands a strong focus on advanced threat detection, rapid incident response, and ongoing cybersecurity enhancements. Prioritizing cyber resilience helps banks not only safeguard critical customer data but also align with regulatory requirements that protect customer trust and uphold the institution's reputation.

Ensuring platform integrity and continuity – the digital platform resilience factor:

Banks should focus on building an "unbreakable" digital infrastructure, ensuring continuous uptime and operational stability. This entails designing a reliable, scalable banking platform capable of handling high transaction volumes, agile maintenance, and uninterrupted deployment of new features. This level of resilience is vital to delivering dependable services and instilling confidence in customers.

Preparedness for uncontrollable events – the force majeure resilience factor:

Banks must be ready to operate through natural disasters, pandemics, and other uncontrollable events. By developing robust plans for continuity under extreme conditions, banks not only meet compliance and regulatory standards but also reinforce their commitment to maintaining reliable services, even in times of crisis.

Together, these pillars create a resilient and adaptive framework that empowers banks to withstand a spectrum of operational challenges—from predictable cyber threats to unpredictable global events. This strategic approach is both forward-looking and comprehensive, ensuring that the bank is well-prepared to meet current and future demands for digital operational resilience, safeguarding both customer trust and regulatory compliance.

So, what's recommended?

To ensure robust cyber resilience, banks should implement proactive threat intelligence and monitoring systems to identify and mitigate risks from malicious actors before they impact operations. This involves partnering with cybersecurity firms, leveraging threat intelligence platforms, and sharing information with industry groups to stay ahead of emerging threats. Additionally, designing a multi-layered security architecture that includes firewalls, intrusion detection systems, endpoint protection, and network segmentation can help contain

potential breaches and minimize lateral movement within the network. Comprehensive incident response plans, supported by detailed playbooks, are essential for swift recovery and communication during a cyber incident, with clear escalation paths and defined roles and responsibilities to ensure a unified response across teams. Regular employee training on cybersecurity best practices and conducting phishing simulations can reduce the risk of human error, fostering a security-first culture where all staff actively participate in safeguarding the bank's data and systems. Finally, conducting regular cyber resilience drills and penetration testing, will help evaluate the effectiveness of defenses and improve overall readiness for various threat scenarios.

To build a robust and resilient banking technology platform, banks should prioritize a comprehensive set of core tenets that collectively enable the platform to withstand disruptions while delivering reliable, high-quality services. Reliability and availability are essential to maintain uninterrupted access, ensuring systems are operational when customers need them most. Security safeguards customer data and protects against cyber threats, forming the foundation for customer trust. Strong performance standards ensure swift transaction processing and responsiveness, even during peak demand, while scalability allows the platform to grow seamlessly alongside expanding digital demands. Maintainability and modularity are crucial for efficient updates and isolated upgrades, minimizing disruptions. Resilience prepares the platform to withstand unexpected events, bolstered by robust disaster recovery and redundancy measures that enable swift recovery with minimal downtime. Comprehensive observability provides real-time insights into system health, allowing proactive issue detection, while interoperability supports seamless integration with other systems and partners, expanding service capabilities. Together, these tenets ensure that the banking platform is not only resilient but also adaptable to future challenges and innovations.

To prepare for unknowns, banks should establish geographically distributed data centers and cloud solutions to mitigate single points of failure caused by regional events, guaranteeing continuity during natural disasters or crisis of other sorts. Comprehensive business continuity plans (BCPs) are essential, covering extreme scenarios such as natural disasters, pandemics, and infrastructure failures. These plans should provide clear protocols for maintaining critical operations, ensuring employee safety, and facilitating effective customer communication. Additionally, conducting simulation exercises and stress testing helps assess preparedness for various force majeure scenarios, including environmental events like earthquakes and health-related crises. Evaluating the resilience of third-party and supply chain dependencies is also crucial; banks should confirm that key vendors have strong continuity measures and identify alternate suppliers when possible. Finally, proactive resource management and rapid mobilization of backup personnel, assets, and temporary facilities are vital to support critical functions during disruptions, including arrangements for remote work and communication channels to sustain essential services and operations.

Infosys Finacle offers reliable foundations for resilient banking operations

Today's complex digital resilience challenges demand a holistic, all-encompassing approach. With a strong cybersecurity posture, a robust system security design, and an advanced architecture, our platform is engineered to operate seamlessly at scale, empowering digital banking operations with exceptional resilience. We integrate security and resilience principles across every level—organizational, product, and process—ensuring that banks are equipped to navigate external threats and unexpected disruptions. Combined with our preparedness for force majeure events, we truly empower banks to maintain continuous, reliable service, no matter the circumstances.

The key highlights of Finacle's well-defined strategies and structured approach include the following:

- **Addressing and mitigating modern security challenges:**
  - A centralized business security advisory and support for our enterprise operations.
  - A cyber governance council with enterprise-wide policies and process frameworks aligned to industry standards, including the NIST Cybersecurity Framework.
  - A comprehensive organization wide information security management framework that encompasses:
    - Physical and information assets management.
    - Information security clauses in third party agreements.
    - Robust risk management processes in line with ISO risk standards and Infosys enterprise risk management methodology.
    - Certified in accordance with ISO 27001:2022 Information Security Management System (ISMS) practices.
- **Product level posture for secure and resilient performance entails the following:**
  - **Security design and related considerations:**
    - Finacle platform has incorporated a multi-layered security architecture with design considerations across various levels, including the following:
      - User and customer access layer
      - Integration and API layer
      - Application layer
      - Database and data layer
      - Infrastructure specific layer (cloud)
    - Secure practices and approach include:
      - Adherence to secure coding and testing principles throughout the software development lifecycle, and fully compliant with global security standards such as ISO 27001, PCI-DSS, FFIEC, COBIT, SOC2, others.
      - Compliance to Finacle's secure coding charter – a combination of guidelines from OWASP, SEI-CERT's secure coding standards, and further augmented with internal expertise.

- Static analysis of source codes, dynamic vulnerability analysis of applications using industry leading tools, penetration testing – both in-house and leveraging external expertise.
- Infrastructure security design considerations factoring in platform layer, transport layer and message level requirements.
- Key considerations related to emergent data security and privacy related norms have also been factored through the SDLC process.
- Release level testing based on applicable guidelines from a wide variety of standards such as ISO/IEC 27001-02, PCI-DSS / PABP, OWASP top 10, among other regional or country specific norms. Stringent assessments also include data privacy related checks.
- Other nuanced capabilities include -
    - Comprehensive capabilities to support zero trust security, with a range of access control mechanisms around authentication, and segregation of duties and entitlements for internal users as well as customers.
    - Build your own encryption, secrets, tokenization, data privacy, IP validation and more, empowering banks truly adopt security-by-design in their end-to-end operations.
    - Chaos engineering and resilience testing related considerations, and support enablers.

- Finacle offers a trusted security framework tailored for software-as-service propositions.
    - Preventive controls include key design considerations for identity access management, network protection, system protection, virtualization protection and data protection.
    - A host of responsive control enablers include an integrated monitoring center, with expansive focus on security information and event monitoring, availability and fault monitoring, web-integrity monitoring.
    - Periodic vulnerability assessments, and internal and 3rd party audits.
- In addition, Finacle clients can benefit from a wide range of cybersecurity services with pre-integrated third-party and homegrown security products offered by the Infosys CyberNext platform.

– **Application design and related considerations:**

- Finacle's composable banking platform is built on the foundations of a 100% open architecture, embracing true microservices architectural thinking – they enable higher degree of flexibility in terms of development, deployment, and performance management, including scaling. Fueled by domain driven design constructs, the platform offers right grained microservices tailored to the business domains they support.

Rooted in pattern language, the platform's microservices design ensures the delivery of efficient, precisely-tailored components perfectly suited to the unique requirements of each business domain.

- The platform is built on a cloud-native, cloud-neutral architecture that ensures adaptability across diverse cloud environments – it exemplifies scalability and high performance, and is designed to meet the demands of population-scale banking.
- Leveraging advanced elastic scaling and dynamic load balancing capabilities, Finacle supports horizontal, vertical, and functional scalability to accommodate massive transaction volumes and data growth seamlessly. Through the scale cube model, the platform independently scales each core component – compute, storage, and database. This resource segregation enhances scalability and ensures that performance remains uncompromised as user demands grow.
- Finacle applications are designed to run in a containerized environment orchestrated by Kubernetes, supporting consistent deployments.
- The platform is designed for built-in redundancy ensuring high availability and reliability. Design considerations have factored in a host of support enablers such as auto backups in the cloud, automated failover through multi-AZ deployment.
- From application deployment perspective, Finacle has externalized the configuration through data hydration tool and configuration editor. Sidecar pattern ensures seamless induction of microservice and switchover in the least disruptive manner. Finacle DevOps Platform offers automation comprising CI-CD pipeline that is leveraged to provide capability of no-touch or low-touch updates to the independent microservices and related components. High availability during upgrades is supported through Blue-Green / Canary deployment architecture patterns.
- From a monitoring and observability perspective, Finacle has incorporated a seamless front-to-back service mesh – playing a key role in governing, intercommunications, observability and monitoring of the microservices. Several additional patterns including log aggregation based on the EFK stack, instrumentation through open telemetry and open tracing, performance monitoring through health check APIs are natively available.

- Finacle platform ensures low latency and high performance through advanced in-memory caching, asynchronous processing, and optimized load balancing with database sharding, enabling rapid data retrieval, lower response times, and seamless load distribution for high-throughput operations.

The architecture features highlighted above enables banks to streamline business continuity utilizing the composability features and limiting the downtime in case of business impact. It also empowers the bank to plan for efficient change management process with quicker business release cycles.

- **From a business continuity perspective:**
  - As a global ICT provider, Infosys Business Continuity Management Services (BCMS) maintains a comprehensive set of disaster recovery plans, support scenarios, and backup capabilities to ensure seamless business continuity.
  - Certified in compliance with ISO 22301:2019 Business Continuity Management System practices.

In summary, building resilient banks requires a holistic approach – And the time is now!

Banks must move beyond traditional compliance checklists and adopt a proactive, integrated approach to operational resilience. The interconnected nature of today's financial systems means that disruptions in one area can rapidly impact others, amplifying risks across the sector. To address these complexities, banks must implement a resilience framework that spans all domains of operation, from cybersecurity and ICT continuity to governance, data integrity, and incident response. This holistic approach requires banks to assess and fortify their critical systems, ensuring they can withstand a broad range of disruptions, whether they stem from cyber threats, operational failures, or vulnerabilities within third-party networks.

Furthermore, resilience is no longer a back-office function but a strategic imperative that must be championed by senior leadership. Accountability at the board and executive levels is essential, with resilience integrated into governance and risk management strategies organization-wide. This means developing clear resilience mandates, conducting regular testing, and establishing comprehensive risk assessments that are adaptive to emerging threats. Banks should invest in technologies like predictive analytics, automation, and continuous monitoring to enhance their ability to foresee, react to, and also recover from incidents swiftly. Importantly, banks need the right digital banking platform that supports these resilience operations. The platform should be designed with resilience in mind, incorporating features such as scalability, redundancy, security, and seamless integration with third-party systems. This ensures that the bank's digital infrastructure is not only capable of handling operational disruptions but is also built to support continuous innovation and adaptation in a rapidly evolving landscape.

Ultimately, by embedding resilience as a core competency, banks can position themselves to not just react to crises but also to thrive in an environment where resilience is a competitive advantage. A resilient bank is one that inspires confidence among clients and partners, capable of maintaining seamless services even in the face of global disruptions. This commitment to resilience aligns well with broader regulatory expectations and hence intrinsically also supports the stability of the global financial ecosystem.

As banks invest in building this robust foundation, including the right resilient digital banking platforms, they not only enhance their operational stability but also play an important role in nurturing a secure, reliable, and resilient financial future for all.

About Infosys Finacle

Finacle is an industry leader in digital banking solutions. We partner with emerging and established financial institutions to inspire better banking. Our cloud-native solution suite and SaaS services help banks engage, innovate, operate, and transform better to scale digital transformation with confidence.

Finacle solutions address the core banking, lending, digital engagement, payments, cash management, wealth management, treasury, analytics, AI, and blockchain requirements of financial institutions globally. Finacle's componentized structure allows banks to deploy and upgrade solutions flexibly as per their business priorities. Our solutions run in a containerized environment orchestrated by Kubernetes and can be deployed on a private, public, or hybrid cloud.

Report authored by

Sudhindra Murthy
Product Marketing Lead,
Strategic Initiatives,
Infosys Finacle

Diwakar Mandal
Product Marketing Manager,
Infosys Finacle

References

- https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- https://www.ibm.com/topics/digital-operational-resilience-act
- https://www.pwc.com/mt/en/publications/technology/dora.html
- https://www.dora-info.eu/dora/
- https://www.kroll.com/en/insights/publications/cyber/preparing-dora-guide-financial-institutions
- https://www.resolver.com/blog/digital-operational-resilience-act-dora/
- https://www.ey.com/en_lu/insights/wealth-asset-management/how-will-dora-impact-the-financial-sector
- https://www.apra.gov.au/operational-risk-management
- https://www.apra.gov.au/news-and-publications/apra-finalises-new-prudential-standard-on-operational-risk
- https://www.apra.gov.au/sites/default/files/2024-06/Prudential%20Practice%20Guide%20CPG%20230%20Operational%20Risk%20Management.pdf
- https://kpmg.com/au/en/home/insights/2022/09/apra-prudential-standard-cps-230-operational-risk-updates.html
- https://www.bis.org/bcbs/publ/d516.htm
- https://www.bis.org/bcbs/publ/d516.pdf

Why we exist

To inspire better banking so that billions of people and businesses can save, pay, borrow, and invest better.

How we do it

Our solutions and people help banks to engage, innovate, operate and transform better, so that they can improve their customers' financial lives, better.

What we offer

A comprehensive suite of industry-leading digital banking solutions and SaaS services that help banks engage, innovate, operate and transform better.

Infosys® | Finacle

Finacle is an industry leader in digital banking solutions. We are a unit of EdgeVerve Systems, a wholly-owned product subsidiary of Infosys (NYSE: INFY). We partner with emerging and established financial institutions to help inspire better banking. Our cloud-native solution suite and SaaS services help banks engage, innovate, operate, and transform better to scale digital transformation with confidence. Finacle solutions address the core banking, lending, digital engagement, payments, cash management, wealth management, treasury, analytics, AI, and blockchain requirements of financial institutions. Today, banks in over 100 countries rely on Finacle to help more than a billion people and millions of businesses to save, pay, borrow, and invest better.

For more information, contact finacle@edgeverve.com **www.finacle.com**