DXC TECHNOLOGY

The New Banking Paradigm: Orchestrating 24x365 Operational Excellence

The gold standard for operational resilience in banking

These days, customers expect access to banking services at all times, driving the need for 24x365 banking operations.
However, this doesn't mean simply extending service hours. It requires a fundamental shift in how banks operate and deliver services.
Continuous banking operations are essential for customer satisfaction, operational efficiency and competitive advantage.

Customer expectations

The demand for round-the-clock banking is driven by the increasingly globalized and digital nature of business and personal finance. Customers expect the convenience of managing their accounts, conducting transactions and accessing customer support at any time of the day or night, irrespective of time zones.

Competitive advantage

Banks that offer 24x365 services can differentiate themselves from competitors by providing superior convenience. This can lead to increased customer loyalty, higher satisfaction rates and a stronger market position.

Enhanced customer satisfaction

Constant availability ensures that customers can perform transactions and resolve issues at their convenience, leading to higher satisfaction levels and trust in the banking institution.

Increased revenue streams

Extended operational hours can lead to increased transaction volumes and the potential for new revenue streams. For example, continuous access to trading platforms or investment services can attract a broader customer base.

Operational efficiency

24x365 banking operations can streamline processes and reduce the burden on traditional branch hours. Automated systems and digital platforms can handle routine transactions, freeing up staff to focus on more complex customer needs.

IBM Geographically Dispersed Parallel Sysplex® (IBM GDPS® CA)

GDPS CA provides geographically dispersed, high-availability and disaster recovery capabilities for IBM z/OS and zLinux systems.

This solution ensures no downtime, continuous operation and zero data loss during site failures by utilizing synchronous replication and automated failover.

The IBM GDPS (Geographically Dispersed Parallel Sysplex) CA (Continuous Availability) solution is part of IBM's disaster recovery and resiliency software suite for IBM Z systems. It is designed to provide near-continuous availability and disaster recovery capabilities across multiple sites. Here are some key features:

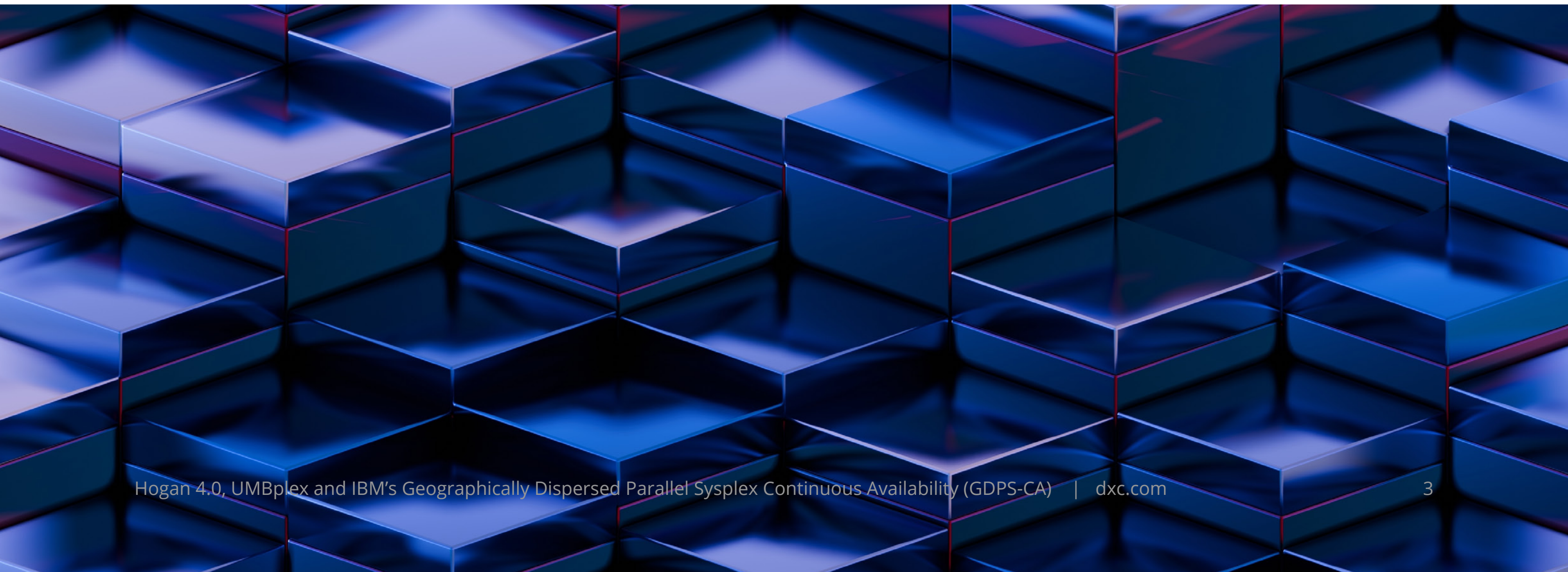
Near-continuous availability: Ensures that systems can remain active and workloads can continue to run even in the event of site or storage failures.

Disaster recovery: Provides rapid recovery from disasters with minimal data loss and downtime.

Multiple site management: Manages remote copy configurations and storage subsystems across various sites.

Automation: Automates operational tasks and failure recovery from a single point of control

This solution is particularly beneficial for enterprises that require high availability and robust disaster recovery capabilities, which are essential competencies for any bank.



The GDPS-CA sites concept consists of having two sites that are separated by virtually unlimited distances, running the same applications, and having the same data to provide cross-site workload balancing and CA and DR. This change is a fundamental change in thinking from a failover model to a CA model.

GDPS-CA does not use any of the infrastructure-based data replication techniques that other GDPS products rely on, such as Metro Mirror (PPRC) or Global Mirror (GM). Instead, GDPS-CA relies on both of the following methods:

Software-based asynchronous replication techniques for copying the data between sites.

Automation, primarily operating at a workload level, to manage the availability of selected workloads and the routing of transactions for these workloads.

The GDPS-CA product, which is a component of the GDPS-CA solution, acts primarily as the coordination point or controller for these activities. It is a focal point for operating and monitoring the solution and readiness for recovery.

Hogan Umbrella UMBPlex Services and IBM Sysplex enable true 24X7 operability

IBM Sysplex (System Complex):

IBM Sysplex (System Complex) is a high-availability, scalability and workload management architecture primarily used in IBM mainframe environments. It enables multiple IBM mainframe systems to work together as a unified entity, providing better performance, redundancy and failover capabilities.

Umbrella UMBPlex:

UMBPlex is a collection of services provided by the Umbrella system to enable all Hogan applications (deposits, loans, cards, customer management) and client applications written under the Umbrella system to:

- Run in a Sysplex
- Share data cached by the common data management facility (CDMF) across a Sysplex
- Share random tables across a Sysplex
- Share shared data groups across a Sysplex.

Benefits of GDPS-CA, Sysplex and UMBPlex

IBM's GDPS (Geographically Dispersed Parallel Sysplex) Continuous Availability, in combination with Hogan UMBPlex, offers several key benefits for businesses:

1 High availability:

GDPS ensures continuous availability of critical applications and data, minimizing downtime and maintaining business operations even during unexpected disruptions (**www.ibm.com/products/gdps**).

2 Disaster recovery:

It provides robust disaster recovery capabilities by automatically mirroring critical data across geographically dispersed sites. This ensures rapid recovery in the event of a site failure (**www.ibm.com/docs/en/gdps/continuous-availability**).

3 Workload balancing:

GDPS efficiently balances workloads between multiple sites, optimizing resource utilization and enhancing overall system performance (**www.ibm.com/docs/en/zos-basic-skills?topic=availability-benefits-parallel-sysplex-disaster-recovery**).

4 Data integrity:

The solution maintains data integrity across all mirrored sites, ensuring that data is consistent and reliable (**www.ibm.com/products/gdps**).

5 **Scalability:**

GDPS can scale to meet the needs of large enterprises, supporting complex and high-volume transaction environments (www.ibm.com/products/gdps).

6 **Security:**

Integrated security features protect sensitive data and ensure compliance with industry regulations (www.ibm.com/products/gdps).

These benefits make GDPS Continuous Availability a powerful solution for organizations looking to enhance their resilience and maintain uninterrupted operations.

Benefits of Parallel Sysplex and UMBPlex

In summary, a Sysplex operating environment with Hogan Umbrella UMBPlex support provides 24x365 availability, scalability, workload management and data-sharing capabilities for mainframe systems.

It’s a powerful solution for all banks that require high reliability and performance in their computing infrastructure and need to meet regulatory requirements.

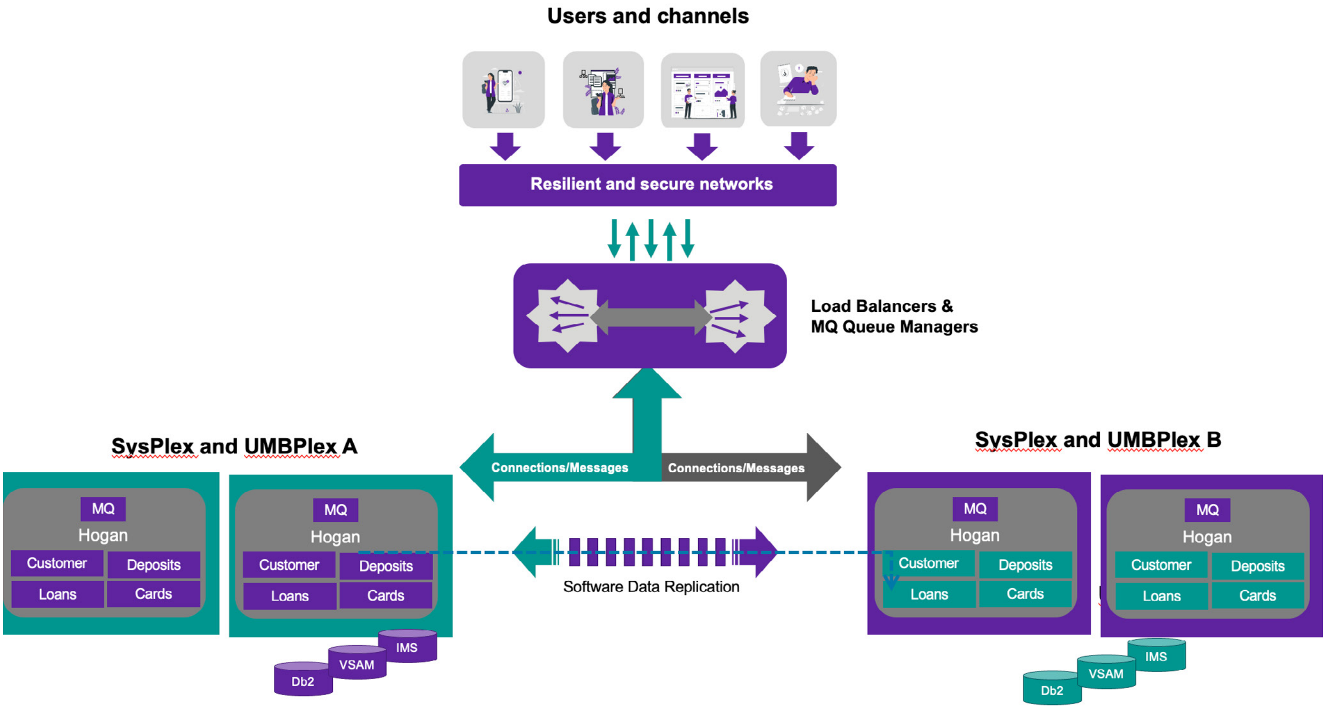


Figure 1: Hogan 4.0 and GDPS-CA

Are you preparing for quantum computing?

The potential benefits and risks of quantum computing are beginning to shape banks' future approaches to securing sensitive information and maintaining essential application and infrastructure integrity.

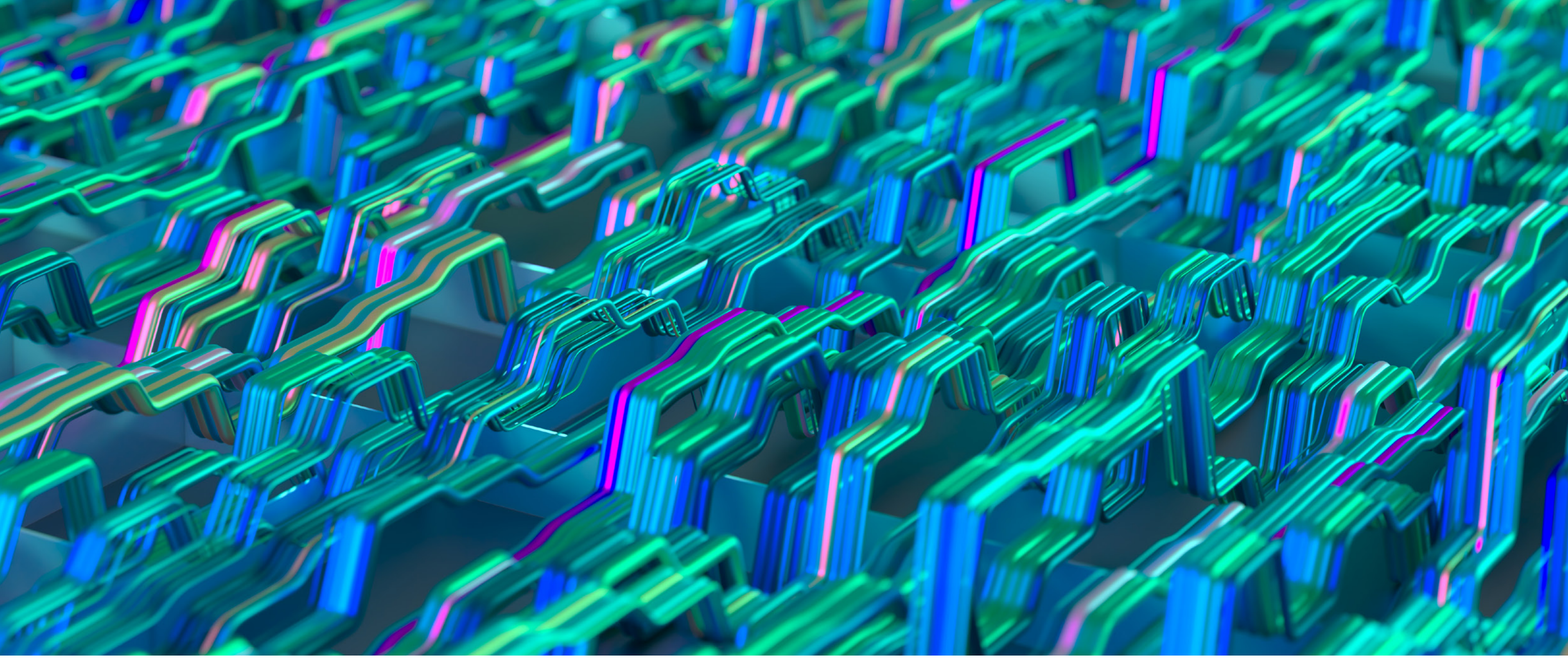
Practical quantum computing may be several years away yet. However, significant breakthroughs have recently occurred (e.g., the recent advances in **quantum teleportation** and **fractional excitons**). So, banks must develop quantum-safe cryptographic strategies while they still have time to prepare for quantum computing's business and social impact. One primary consideration is that integrating crypto-agility with system modernization will be a massive undertaking for top-tier banks. This transformation will impact the entire financial services landscape, involving standards bodies (e.g., **NIST**) and cross-industry cooperation at all levels.

Although we're looking ahead here, traditionally encrypted (e.g., public-key cryptography), wire-tappable communications are already at risk. "Harvest data now, decrypt later" (when quantum decryption solutions are finally realized) is an immediate cause for concern and appropriate action.

Regulations and operational resilience

The latest EU regulatory requirement, the Digital Operational Resilience Act (DORA), came into force this month and demands greater due diligence to address security and resilience challenges in an increasingly complex, digitally powered and global financial system.

DORA represents the most complete European regulations on operational resilience to date. It creates a binding, comprehensive information and



communication technology (ICT) risk management framework for the EU financial sector and non-EU banks with legal entities in the EU. The new act establishes technical standards that financial entities and their critical third-party technology providers must implement in their ICT systems by January 17, 2025.

The regulations apply to banks, financial institutions and critical financial-sector suppliers (third parties). This is the world's first framework that allows financial services supervisors to oversee critical ICT third-party providers (CTPPs), including cloud service providers (CSPs).

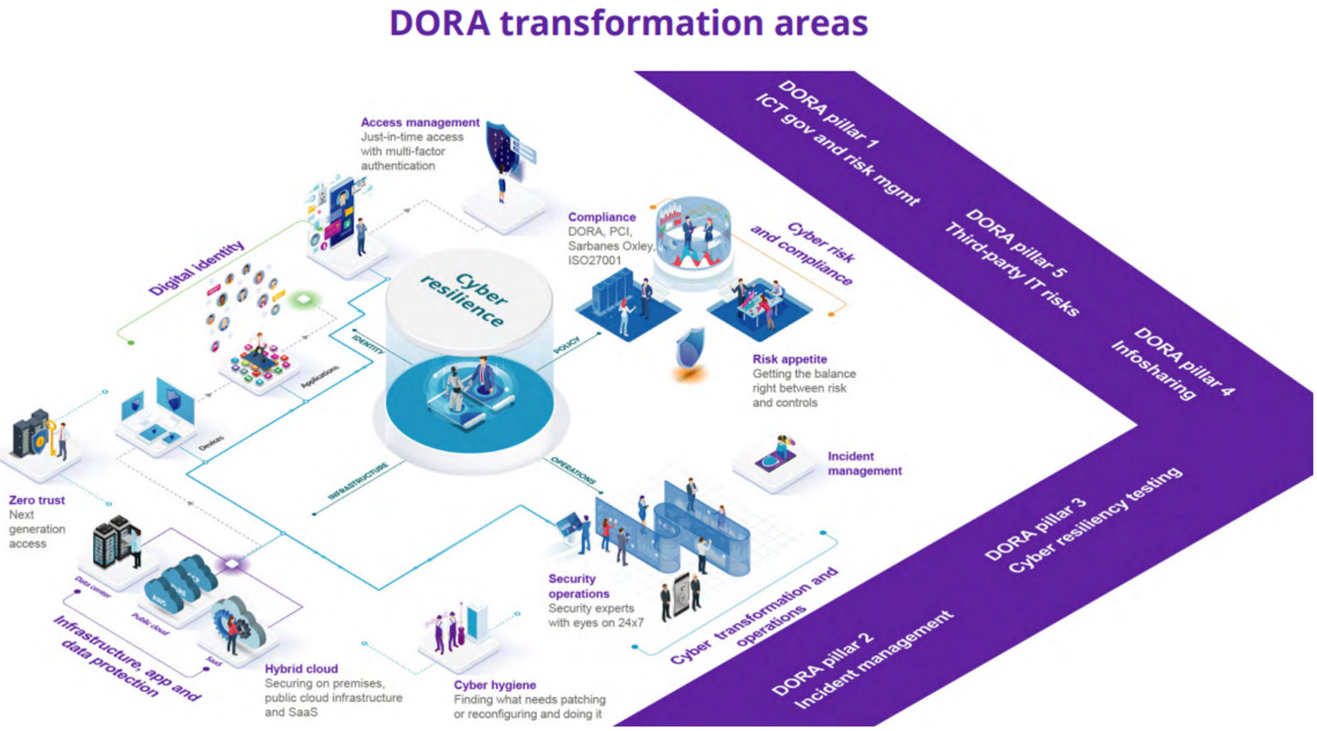


Figure 2: DORA transformation areas

Now, banks are aware of potential problems with noncompliance and could already have DORA programs running — some will be more adversely affected than others. Most banks were reasonably calm about GDPR compliance, but the rubber really hit the road when that first hefty fine was levied. So, are you leaving yourself open to a DORA fine (1% of your top-line turnover each day you're down, perhaps, not to mention the loss of reputation)?

REGULATORY SNAPSHOT

Financial Industry Mandates for Out-of-Region Disaster Recovery (DR)

In the financial sector, regulatory bodies enforce strict mandates on out-of-region disaster recovery to ensure operational resilience, data integrity, and business continuity. These mandates require geographically dispersed DR strategies to mitigate risks from natural disasters, cyber threats, and systemic failures.

Key Financial Regulations Requiring Out-of-Region DR

United States

- **FFIEC (Federal Financial Institutions Examination Council) Guidelines**
  - Requires financial institutions to have geographically dispersed backup and DR sites.
  - Must ensure resilience against regional disasters, including cyber incidents.
  - Tested failover capabilities for critical banking systems (e.g., payments, clearinghouses).
- **OCC (Office of the Comptroller of the Currency) & Federal Reserve SR 20-24**
  - Banks must maintain a second-site DR location at a safe geographic distance.
  - Periodic resilience testing to ensure recovery within two hours for critical operations.
  - Cyber resilience measures to protect against systemic risks (e.g., ransomware).

European Union

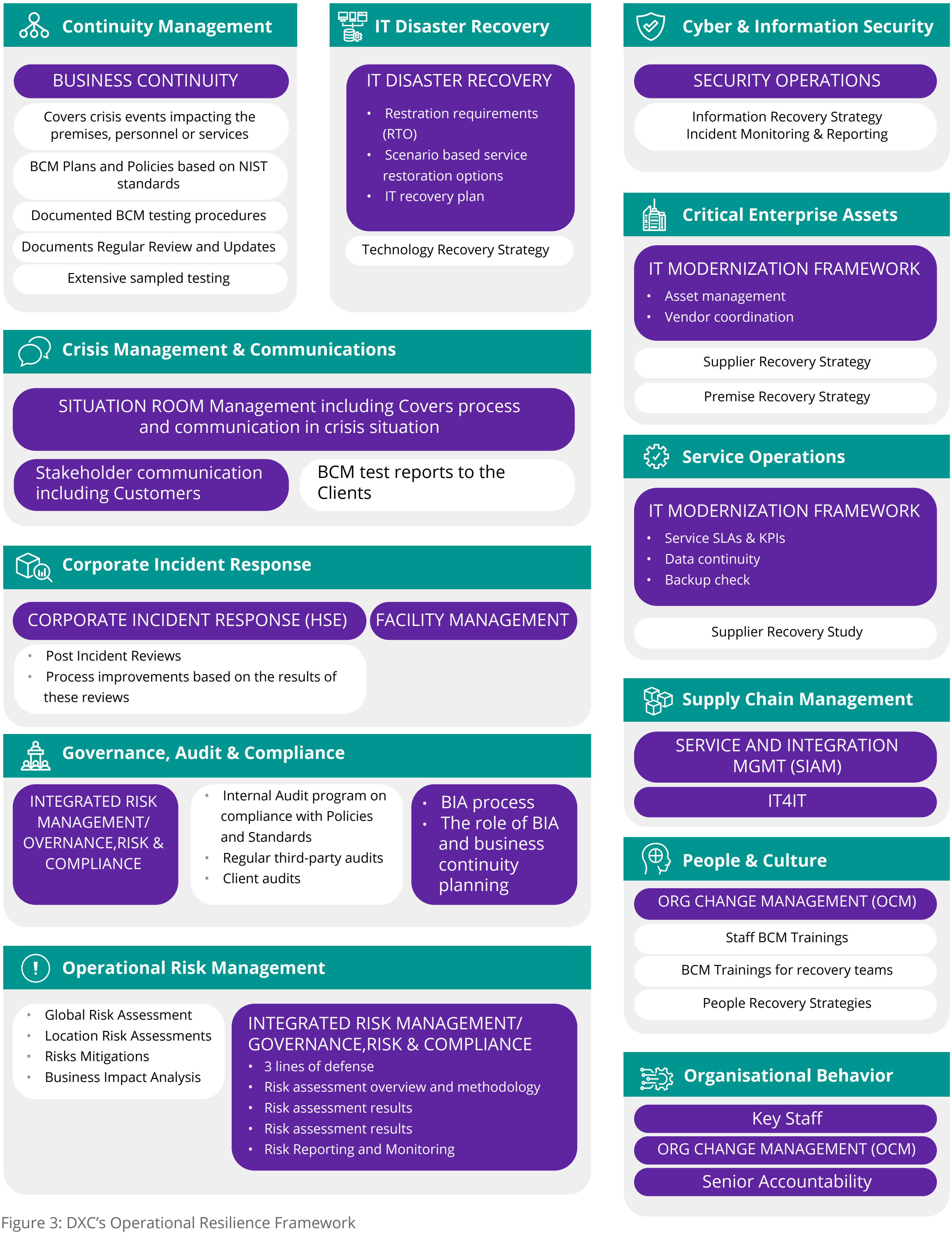
- **DORA (Digital Operational Resilience Act) – 2025 Compliance Deadline**
  - Financial entities must establish geographically redundant DR sites.
  - Requires periodic testing and adherence to maximum recovery times.
  - Cloud-based DR is allowed but must comply with outsourcing risk frameworks.
- **EBA (European Banking Authority) Guidelines on ICT & Security Risk Management**
  - Out-of-region recovery sites must be tested to ensure operational continuity.
  - Institutions must maintain near real-time failover capabilities for systemic functions.

United Kingdom

- **FCA (Financial Conduct Authority) & PRA (Prudential Regulation Authority)**
  - Banks and financial firms must implement geographically separated DR locations.
  - Impact tolerance & resilience testing is required for severe but plausible scenarios.

DXC’s operational resilience framework

This framework identifies 12 management disciplines that can be grouped in different ways to ensure appropriate operational resilience responses for different risks.



Continuity Management

BUSINESS CONTINUITY

Covers crisis events impacting the premises, personnel or services

BCM Plans and Policies based on NIST standards

Documented BCM testing procedures

Documents Regular Review and Updates

Extensive sampled testing

IT Disaster Recovery

IT DISASTER RECOVERY

- Restration requirements (RTO)
- Scenario based service restoration options
- IT recovery plan

Technology Recovery Strategy

Cyber & Information Security

SECURITY OPERATIONS

Information Recovery Strategy
Incident Monitoring & Reporting

Critical Enterprise Assets

IT MODERNIZATION FRAMEWORK

- Asset management
- Vendor coordination

Supplier Recovery Strategy

Premise Recovery Strategy

Crisis Management & Communications

SITUATION ROOM Management including Covers process and communication in crisis situation

Stakeholder communication including Customers

BCM test reports to the Clients

Service Operations

IT MODERNIZATION FRAMEWORK

- Service SLAs & KPIs
- Data continuity
- Backup check

Supplier Recovery Study

Corporate Incident Response

CORPORATE INCIDENT RESPONSE (HSE)

FACILITY MANAGEMENT

- Post Incident Reviews
- Process improvements based on the results of these reviews

Supply Chain Management

SERVICE AND INTEGRATION MGMT (SIAM)

IT4IT

Governance, Audit & Compliance

INTEGRATED RISK MANAGEMENT/ OVERNANCE,RISK & COMPLIANCE

- Internal Audit program on compliance with Policies and Standards
- Regular third-party audits
- Client audits

- BIA process
- The role of BIA and business continuity planning

People & Culture

ORG CHANGE MANAGEMENT (OCM)

Staff BCM Trainings

BCM Trainings for recovery teams

People Recovery Strategies

Operational Risk Management

- Global Risk Assessment
- Location Risk Assessments
- Risks Mitigations
- Business Impact Analysis

INTEGRATED RISK MANAGEMENT/ GOVERNANCE,RISK & COMPLIANCE

- 3 lines of defense
- Risk assessment overview and methodology
- Risk assessment results
- Risk assessment results
- Risk Reporting and Monitoring

Organisational Behavior

Key Staff

ORG CHANGE MANAGEMENT (OCM)

Senior Accountability

Figure 3: DXC’s Operational Resilience Framework

Banks must fully appraise operational resilience on an ongoing basis and devise a continual improvement strategy to address the subject holistically to avoid the dreaded reprimand. That's the real importance of keeping up to date with the latest applications, just as you would with all your other patches, browsers and security apps — they come with vital, enhanced features that support innovation and operational resilience.

In the United States, the regulator sets strong operational resilience guidance, but with increased cyberthreats, this is likely to become a mandate. Banks improve the customer experience by guaranteeing the tightest data security, developing faster, frictionless processes and providing innovative products and services that are easy to deploy and personalize.

Now, seduced by the benefits and challenged by the cryptographic threat of quantum computing, the ever-increasing computing power of IBM's z16 puts our banking clients in the security driving seat. Combine this with GDPS-CA, UMBPlex and Hogan core banking applications, and you have a best-in-class platform for operational resilience.

This is why so many Hogan clients are upgrading their systems and are doubling down on mainframe hybrid cloud to run their Hogan applications. Combining that with IBM's GDPS-CA and Hogan's UMBplex sets the gold standard for achieving 24x365 availability and operational resilience.

The IBM z16 provides extra protection by encrypting data wherever it resides — at rest, in flight or in use — with fully homomorphic encryption. Its robust data-processing capabilities and enhanced security features, such as fully homomorphic encryption, enable banks to protect data, ensure compliance and improve the customer experience through faster, frictionless processes.

Homomorphic encryption is a unique mechanism that resolves security and privacy issues. It allows third-party service providers to perform specific operations on the user's encrypted data without decrypting it. Homomorphic encryption accelerates our clients' innovation and collaboration with third parties without the risk of compromising sensitive information. In other words, it helps them deliver better outcomes for their customers.

The IBM Z Security and Compliance Centre, now an integrated capability of IBM z16, boosts compliance. It enables clients to be always compliance-ready. Banking compliance is viewed in near real-time via dashboards and reporting, which reduces the number of employees focused on audit preparations.

Banks improve the customer experience by guaranteeing the tightest data security, developing faster, frictionless processes and providing innovative products and services that are easy to deploy and personalize.

Now, seduced by the benefits and challenged by the cryptographic threat of quantum computing, the ever-increasing computing power of IBM's z16 puts our banking clients in the security driving seat. Combine this with GDPS-CA, UMBPlex and Hogan core banking applications, and you have a best-in-class platform for operational resilience.

- GDPS — IBM **https://www.ibm.com/products/gdps**

- GDPS Continuous Availability — IBM **https://www.ibm.com/docs/en/gdps/continuous-availability**

- Benefits of Parallel Sysplex: Disaster recovery — IBM **https://www.ibm.com/docs/en/zos-basic-skills?topic=availability-benefits-parallel-sysplex-disaster-recovery**

If you'd like to find out more **visit our website**
or contact **Duncan Alexander**

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.