protiviti®
Global Business Consulting

TECHNOLOGY & CYBER RESILIENCE FOR UNINTERRUPTED BANKING

TODAY'S IMPERATIVE, NOT A FUTURE GOAL

Face the Future with Confidence®

TABLE OF CONTENTS

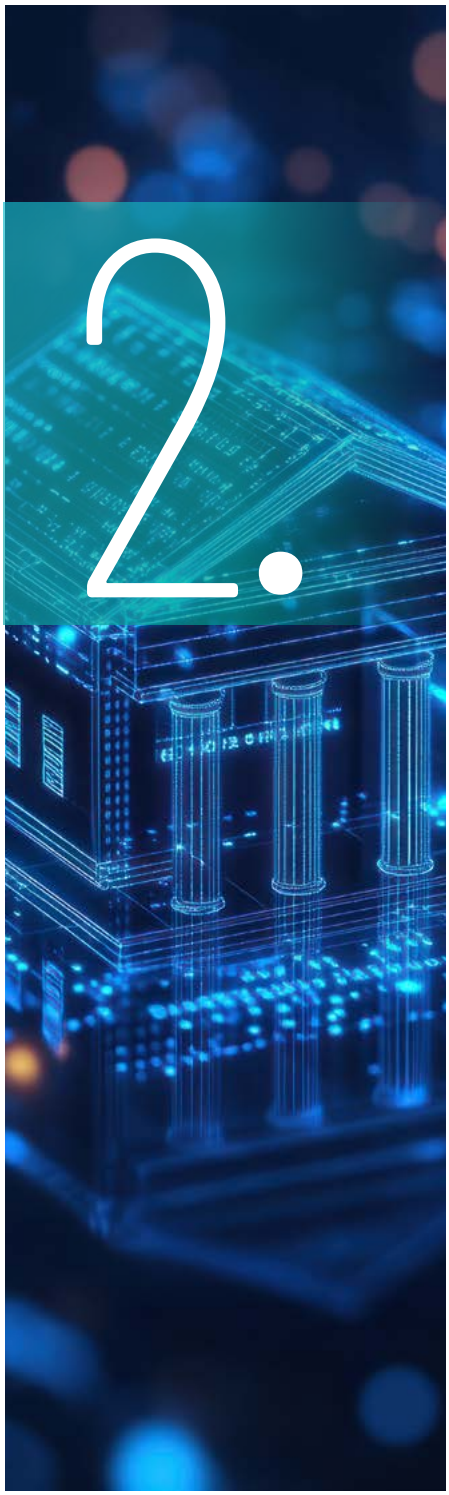
1. EXECUTIVE SUMMARY

As banks evolve into fully digital enterprises, it has become abundantly clear that Technology Resiliency is no longer optional; it's a fundamental business imperative. The ability to maintain uninterrupted operations in the face of disruption has shifted from just a technology consideration to a Boardroom priority. CIOs, are increasingly accountable not just for enabling digital transformation, but for ensuring the Bank can continuously operate uninterrupted.

Every customer transaction, interaction, and critical business process depends on the stability and performance of the Bank's underlying technology. Without a robust and reliable technology foundation, the Bank's ability to withstand disruptions — be it cyberattacks or system failures/human errors—is severely compromised impacting service continuity, customer trust, and **regulatory standing**.

Operational resilience ultimately means withstanding disruptions without interrupting the delivery of core services. This level of resilience is only achievable when technology systems are not just robust, but inherently reliable— designed to t**ransparently continue operations**. True technology resilience extends beyond simply keeping individual systems "up and running". It demands that the entire infrastructure stack—spanning compute, operating systems, middleware, applications, networks, and storage layers—remains consistently available, ensuring that services and data are always accessible in a stringent regulatory and security environment.

For CIOs and the Bank's leadership, this requires a shift from traditional IT Disaster Recovery (ITDR) mindsets, re-evaluating their approach to technology and cyber resilience with a proactive lens. It means dedicated investment in resilient technologies and architectures, alongside a commitment to re-engineer systems for fault tolerance and the elimination of single points of failure, all with continuous availability as the paramount goal.



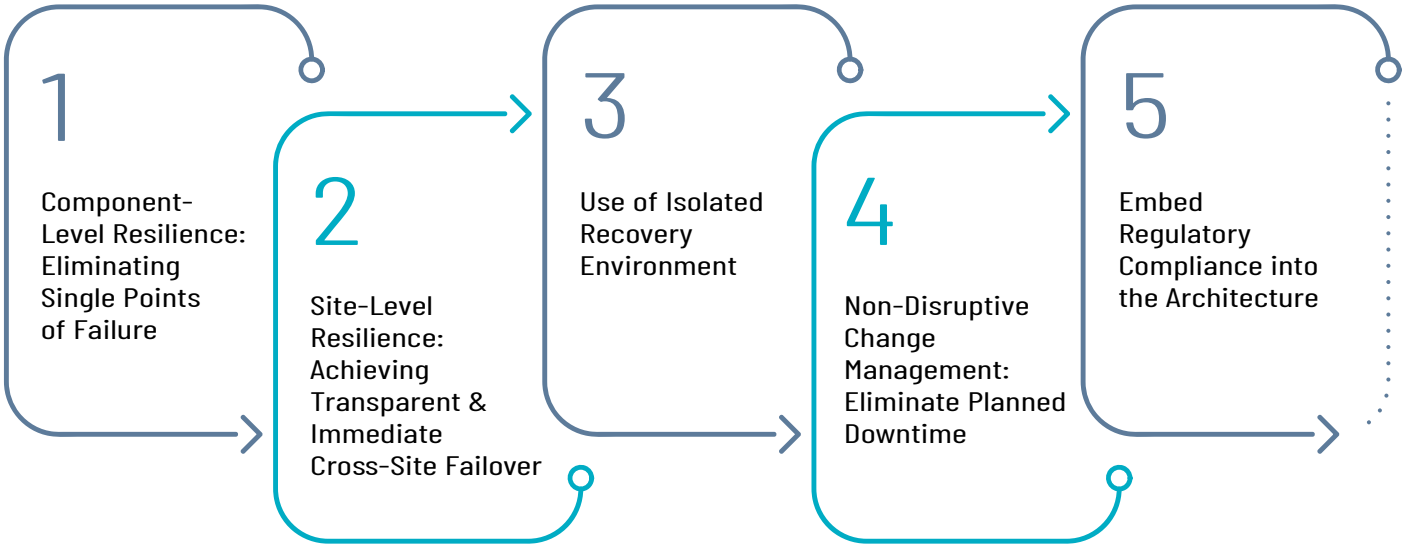
2. TECHNOLOGY & CYBER RESILIENCE: Principles and Foundational Requirements

Technology and Cyber Resilience represents an evolution beyond traditional ITDR, driven by core principles that guarantee continuous availability and rapid recovery. Unlike conventional DR, which often tolerates some downtime and relies on periodic backups and limited scope testing, resilient infrastructure focuses on eliminating single points of failure and ensuring transparent failover/failback for uninterrupted operations.

In the context of resilience, technology outages generally fall into three categories:

1. **Planned Downtime:** These are scheduled outages required for routine maintenance activities such as patching, bug fixes, upgrades, or other essential system tasks. Systems or data are taken offline intentionally and with prior notice.
2. **Unplanned Downtime:** These outages occur unexpectedly due to factors like human error, software bugs, hardware failures, or environmental issues. They are disruptive events that cannot be scheduled in advance.
3. **Cybersecurity-Driven Outages:** Outages resulting from cyber threats such as ransomware attacks, virus infections, or Distributed Denial of Service (DDoS) attacks. These are often malicious in nature and require rapid remediation response.

Both technology resilience and cyber resilience both aim to ensure the availability of technology systems, the distinction between the two stems from the causes of these disruptions. Technology resilience focuses on maintaining availability in the face of planned and unplanned outages. In contrast, cyber resilience is concerned with sustaining technology operations during and after malicious attacks. While both impact system uptime, technology resilience addresses operational reliability, whereas cyber resilience tackles intentional, security-driven threats to technology continuity. Together, they form a comprehensive approach and contribute to operational resilience.



Core Principles of Technology & Cyber Resilience

1. **Component-Level Resilience: Eliminating Single Points of Failure**
   Resilience must be embedded at every layer—network, systems, middleware, and application. This is achieved by designing for redundancy at every level and eliminating single points of failure, so that localized issues never escalate into service outages.

2. **Site-Level Resilience: Achieving Transparent & Immediate Cross-Site Failover**
   Instead of depending on manual or delayed failover and failback mechanisms, resilient architectures leverage Active/Active configurations to enable seamless, real-time failover with no service interruption— a stark contrast to the often slower and manual recovery associated with traditional DR.

3. **Use of Isolated Recovery Environment**
   To enhance cyber resilience—especially against ransomware threats— leveraging an Isolated Recovery Environment (IRE) in addition to the traditional two data centers design. An IRE is a physically and logically separated facility designed to remain untouched during a cyberattack, ensuring the integrity of data. In ransomware scenarios, where both production and backup systems can be compromised, the IRE serves as a secure fallback, enabling clean recovery without reinfection risk.

4. **Non-Disruptive Change Management: Eliminate Planned Downtime**
   Resilient environments embraces techniques like rolling updates, blue-green deployments, and zero-downtime patching facilitate continuous release, allowing for frequent new versions and features without impacting service availability.

5. **Embed Regulatory Compliance into the Architecture**
   Resilient technology architectures allow for on-demand testing of failover and recovery mechanisms, enabling real-time assurance that regulatory expectations for resilience are consistently met.

Traditional ITDR vs Technology & Cyber Resilience

Aspect	Traditional ITDR	Technology & Cyber Resilience
Availability	Tolerates some level of outage	Zero-Downtime & Continuous availability with rapid, transparent recovery
Outage Threshold	Focuses on un-planned downtime only; planned downtime is excluded	Targets near-zero downtime; both planned & un-planned downtime are factored into RTO/ RPO metrics
Primary Data Center Usage	Operates mainly from a single, designated production site	Actively switches between main & secondary sites; secondary site runs BAU operations for prolonged duration i.e. ~6 months annually
Facility	Two data centres	Two data centres plus an Isolated Recovery Environment (IRE) for Ransomware Threats
Backup	Periodic backups with larger recovery windows	Continuous backup & rapid restore
Testing	Limited to internal organization	Extended to include third parties and live simulations

3. EMERGING REGULATORY LANDSCAPE: Key Expectations and Frameworks for Technology Resilience

Regulators are increasingly demanding that financial institutions demonstrate robust technology resilience, moving beyond traditional disaster recovery to ensure continuous operations. This evolving landscape presents several key expectations:

1. **Report on the Bank's current Technology & Cyber resiliency posture.** Banks are now expected to provide comprehensive, data-driven assessments of their current technology resilience capabilities, including dependencies and risk exposures. Regular assessments and documented posture reports are becoming foundational compliance elements.

2. **Outline a roadmap toward achieving Active/Active architecture** Supervisors are increasingly emphasizing the need for seamless, uninterrupted operations. A defined transition plan to Fully Active/ Active architecture is viewed as an imperative for critical infrastructure operators such as banks.

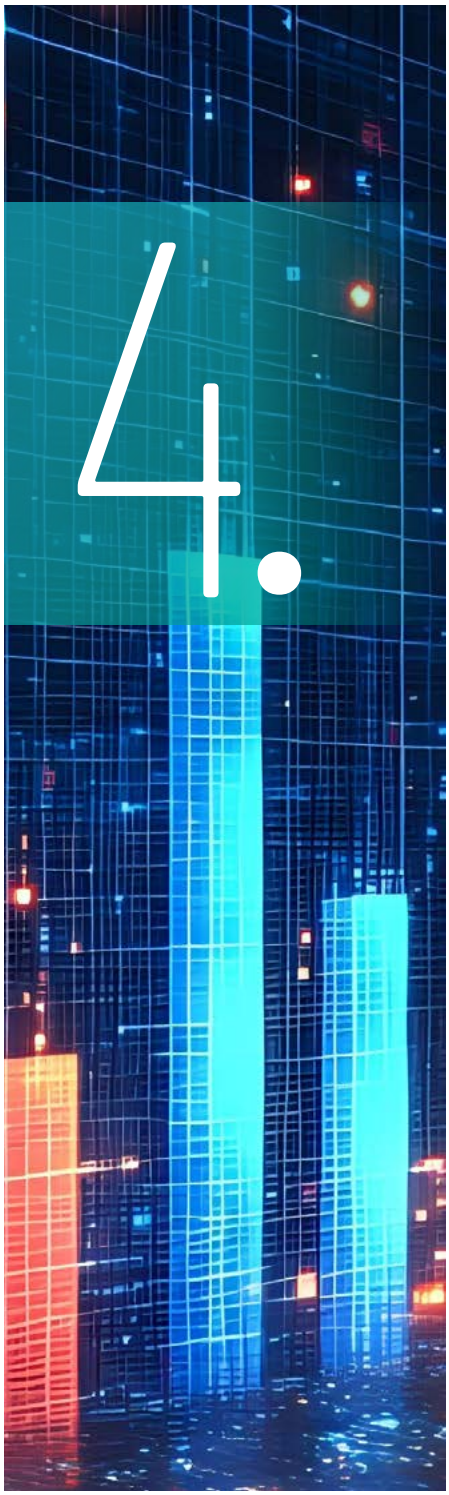
3. **Present the strategy for reducing RTO & RPO** Minimizing Recovery Time and Point Objectives aligns with regulatory goals for operational continuity. Authorities now require demonstrable efforts to shorten recovery windows through architectural improvements and automation.

4. **Define Minimum Viable Bank (MVB) requirements** Identifying and documenting MVB functions is essential to resilience planning. Regulators expect banks to clearly define minimum set of services and associated technology resources required to continue and sustain essential operations, ensuring core services can always be delivered to customers and the market.

5. **Establish a governance structure for Technology and Cyber Resilience**
   A formal governance model ensures accountability and oversight of resilience initiatives. Regulatory expectations now include clear roles, escalation paths, and board-level visibility over Technology & Cyber resilience risk.

6. **Adopt a unified framework for reporting and managing Technology & Cyber resilience risks across the bank**
   Banks are required to implement a standardized approach for identifying, assessing, reporting, and managing Technology & Cyber resilience risks across all business units and technology domains, fostering visibility and a cohesive risk posture.

7. **Regularly test failover & failback, including extended operations from the secondary site to ensure readiness**
   Supervisory bodies stress the importance of realistic testing to validate technology & cyber resilience readiness. Prolonged operation from alternate sites is now a best practice to ensure systems, staff, and processes are fully prepared.



4. THE MINIMUM VIABLE BANK (MVB): Prioritizing for Resilience

The Minimum Viable Bank (MVB), in the context of operational resilience, refers to the absolute set of essential business services, processes, underlying technology (IT infrastructure, applications, data), that a bank must maintain operational, even under severe and adverse disruption scenarios, to avoid causing unacceptable harm to customers and financial system.

In other words, a Minimal Viable Bank represents the leanest form of a digital bank, designed to deliver essential banking services even during crises such as catastrophic technology outages—ensuring near-zero downtime for the critical systems that support these core services.

The MVB concept is designed to serve three critical objectives:

1. **Harm Avoidance:** The foremost objective is to prevent unacceptable levels of harm to customers and the financial system in the event of severe disruptions.
2. **Focus on Essentials:** The MVB approach compels the bank to rigorously identify its Essential Business Services (EBS)—a central regulatory requirement—and determine the minimal set of resources necessary to sustain these services within pre-defined impact tolerances.
3. **Foundation for Resilience:** Once the MVB is established, it forms the foundation for all resilience planning. Investment, testing, and recovery strategies are prioritized to ensure the continued operation of these core MVB components under stress or failure conditions.

A structured approach to defining the MVB includes the following key steps:

1. **Identify Essential Business Services (EBS):** Focus on Tier 0 and Tier 1 services that are essential to the bank's core mission and align with the Minimal Viable principle—those services that must remain operational under all conditions.
2. **Map End-to-End Dependencies:** Conduct a mapping of dependencies across technology systems, facilities, third-party providers, and other critical enablers that support the identified EBS.
3. **Determine Minimal Resources and Build Capabilities:** Establish the minimum set of resources—people, processes, technology, and infrastructure—required to maintain the delivery of essential services within defined impact tolerances. Develop targeted capabilities around these core elements.
4. **Operationalize Through a Governance Structure:** Embed the MVB framework within a formal governance model that ensures continuous oversight, accountability, testing, and iterative improvement.

The MVB concept plays a pivotal role in strengthening Technology & Cyber resilience and managing operational risk by:

1. Regulatory Alignment: MVB directly supports compliance with evolving regulatory expectations around operational resilience, including frameworks such as DORA (EU), PRA/FCA (UK) etc., It demonstrates the bank's capability to sustain critical services under adverse conditions.
2. Prioritization: MVB provides a focused framework for prioritizing resilience investments, resource allocation—both financial and human—and recovery strategies during crisis scenarios. It ensures that the Bank concentrates efforts on protecting the services that matter most.
3. Enhanced Communication: By clearly defining which services will remain operational and why, the MVB framework enables effective communication—both internally across teams and externally with regulators, customers, and stakeholders—during disruptive events.

In essence, the MVB is a blueprint for survival and continuity in the face of severe disruption, ensuring that a bank can fulfil its most fundamental obligations to customers and the financial system.

5. CIOs AND TECHNOLOGY RESILIENCE: Asking the Right Questions

In an era of mounting technology operational and cyber risks CIOs must challenge their teams and partners with the right questions to ensure their resilience strategies are comprehensive, forward-looking, and audit-ready.

Key Questions for CIOs to Ask:

1. How is fault tolerance implemented across the bank's infrastructure stack—compute, network, and storage?
2. Across the application landscape, what is the maturity level of the failover mechanisms in place, particularly in relation to data replication?
3. Given the scale and diversity of the bank's environment, how standardized and interoperable are the replication technologies, considering the organic evolution of the infrastructure over time?
4. In scenarios where the bank must operate from the secondary site under sustained live workload conditions, do we have sufficient capacity, performance headroom, and resource allocation to support business-as-usual operations?
5. Do our primary and secondary DCs exhibit true operational and architectural parity, encompassing not just infrastructure components but also consistent configuration management, patch levels, security baselines, and operational tooling to ensure seamless failover and failback without manual intervention?
6. What opportunities exist to simplify and streamline the bank's infrastructure to enhance resilience?
7. What is the design and readiness of the bank's ransomware recovery architecture, including the use of air-gapped or isolated recovery environments?
8. What is the depth and realism of bank's resilience tests and drills, covering full-stack failover and failback simulations, and extending to third-party dependencies?
9. Does the banks measure and report both the planned and unplanned downtime over the past 12 months, in terms of duration, cause, and impact?
10. At a high level, the bank is aware of applications with frequent failure incidents, have we performed analysis to understand the underlying patterns, and what remediation strategies are being pursued to address recurring failures to reduce RTO?

6. Challenges in Building a Resilient Technology Environment

Building a truly resilient technology environment within a large financial institution presents a formidable array of challenges. The journey from traditional disaster recovery to holistic technology and cyber resilience is fraught with complexities stemming from architectural legacy, resource limitations, and the intricate web of modern digital operations. CIOs and their teams must navigate these hurdles to forge a technology infrastructure capable of enduring an increasingly complex digital landscape.

Key challenges in building a resilient technology infrastructure

1. Heterogeneous Technology Stack
2. Diverse and Evolving Database Ecosystems
3. Intrinsic IT Infrastructure Complexity
4. Legacy Siloed Resilience Efforts
5. Application Volatility
6. Resistance to Operational Disruption
7. Vendor and Third-Party Dependencies
8. Financial Resource Constraints

Here are some key challenges in building a resilient technology infrastructure:

1. **Heterogeneous Technology Stack:** Overcoming the challenge of integrating and ensuring resilience across a diverse mix of disparate platforms, operating systems (e.g., Mainframe, UNIX, Windows, Linux) and myriad communication protocols.
2. **Diverse and Evolving Database Ecosystems:** Supporting recovery for traditional RDBMS like Oracle, MS SQL, and DB2 alongside NoSQL platforms (e.g., MongoDB, Cassandra, Hadoop).
3. **Intrinsic IT Infrastructure Complexity:** Interconnected applications, multiple facilities, layered networking, and hybrid environments significantly increase the difficulty of orchestrating resilient operations.
4. **Legacy Siloed Resilience Efforts:** Shifting from historical, isolated resilience focus areas (e.g., network-specific redundancy or single-layer virtualization) to an integrated, end-to-end resilience strategy that spans all layers of the technology stack.
5. **Application Volatility:** Legacy applications undergoing frequent changes often introduce instability that extends beyond the control of the underlying technology infrastructure.
6. **Resistance to Operational Disruption:** Business and technology teams often deprioritize resilience drills due to concerns over downtime, service impact, or customer disruption—limiting readiness for real scenarios.
7. **Vendor and Third-Party Dependencies:** Reliance on external providers, platforms, and system integrators as their resilience capabilities are opaque or untested.
8. **Financial Resource Constraints:** Securing adequate budget and financial investment for comprehensive resilience programs, often competing against other transformation priorities in a landscape of limited resources.

7.

ACHIEVING CONTINUOUS OPERATIONS:

The Technology & Cyber Resilience Transformation Roadmap

To achieve true resilience, banks must embark on a structured transformation journey. This requires systematically building capabilities across the entire technology and organizational landscape. Banks must proactively identify weaknesses and adequately invest in capabilities that ensure sustained performance even in the face of inevitable disruptions.

Below is a four-phased approach for Technology & Cyber Resilience Transformation to achieve continuous availability:

1. **Discover Resilience Blind Spots:** Initiate a comprehensive assessment of the current technology landscape to identify availability gaps, undocumented system dependencies, and weak points in failover and recovery coverage. This phase establishes a fact-based baseline to guide and prioritize subsequent transformation efforts.

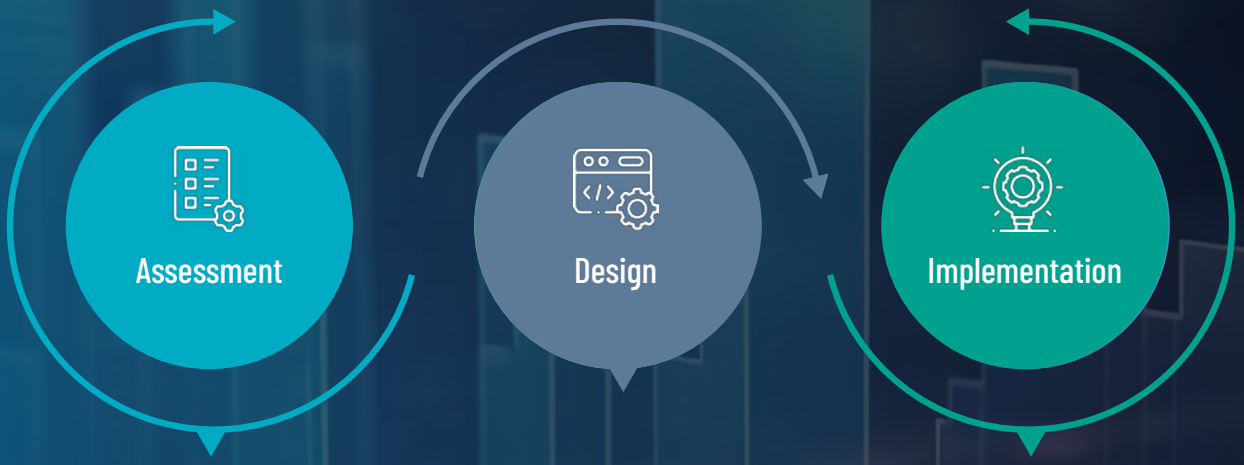
2. **Simplify and Re-engineer Technology Infrastructure toward Active/Active Architecture:** Modernize the infrastructure by eliminating architectural complexity, standardizing replication technologies, and transitioning to real-time, geo-redundant (Active/Active) configurations that enable seamless continuity across sites.

3. **Implement Architectural Changes with Oversight and Validation:** Execute infrastructure and operational changes through a structured and controlled approach. Apply rigorous change management, validation processes, and stakeholder engagement to ensure a smooth transition with minimal operational risk.

4. **Establish and Sustain a Resilience-Centric Operational State:** Integrate resilience into day-to-day operations through continuous testing, enhanced observability, well-defined response playbooks, and strong governance. This ensures resilience becomes a measurable, sustained, and adaptive capability embedded within the organization.

8. HOW CAN PROTIVITI HELP

Protiviti can help you in various stages of your resilience maturity journey covering assessments to implementation.



Assessment

1. Technology & Cyber Resilience Posture & Maturity Review
2. Technology Resilience Compliance Review
3. Technology Incident and Change Analysis: Patterns and Root Causes
4. Technology Resilience Program Financial Planning
5. Technology & Cyber Resilience Scenario Testing & Validation

Design

1. Design & Development of Minimum Viable Bank (MVB) Framework
2. Resilience & Fault Tolerant Systems Selection
3. Full Stack Technology Infrastructure Solution Engineering & Re-Architecture
4. Point-Solutions Engineering & Design

Implementation

1. Resilience Automation
2. Technology Resilience Program Implementation Management
3. Technology Resilience Project Governance

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the Fortune 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. has served more than 80 percent of *Fortune* 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Key Contacts

Adib Ibrahim
Managing Director
Adib.Ibrahim@protivitiglobal.me

Shuaib Shafi
Managing Director
Shuaib.Shafi@protivitiglobal.me

Kumar Ritesh
Senior Director
Kumar.Ritesh@protivitiglobal.me

Our Offices in the MENA

Abu Dhabi
Emirates Real Estate Corporation
Building, 7th Floor, Office 707-711
Al Falah Street, Al Danah,
P.O. Box 32468, Abu Dhabi, UAE

Bahrain
Platinum Tower, 17th Floor
P.O. Box 10231, Diplomatic Area
Manama, Kingdom of Bahrain

Dubai
Office No. 2104, 21st Floor
U-Bora Tower 2, Business Bay
P.O. Box 78475, Dubai, UAE

Egypt
Cairo Complex
Ankara Street Bureau 1
First Floor, Sheraton Area
Heliopolis - Cairo, Egypt

Kuwait
Al Shaheed Tower, 4th Floor
Khaled Ben Al Waleed Street, Sharq
P.O. Box 1773, Safat 13018, Kuwait

Oman
Al-Ufuq Building, 2nd Floor
Office No. 26, Shatti Al Qurum
P.O. Box 1130, P.C. 112
Ruwi Muscat, Oman

Qatar
Palm Tower B 19th Floor
P.O. Box 13374, West Bay
Doha, Qatar

Saudi Arabia - Dammam
Q1-5, The Business Quarter
Salman Al Farisi St,
Al Khalidiyyah Al Janubiyyah, Dammam, Eastern Province, 32221,
Kingdom of Saudi Arabia

Saudi Arabia - Jeddah
King Abdulaziz Branch Road
Ash shati district , Building No. 7524 P.O. Box 3675, Jeddah 23412
Kingdom of Saudi Arabia

Saudi Arabia - Riyadh
Al-Ibdaa Tower, 9th & 18th Floor
King Fahad Branch Road, Al-Olaya,
Building No. 7906, P.O. Box 3825
Riyadh 12313, Kingdom of Saudi Arabia

Face the Future with Confidence®