Deloitte.
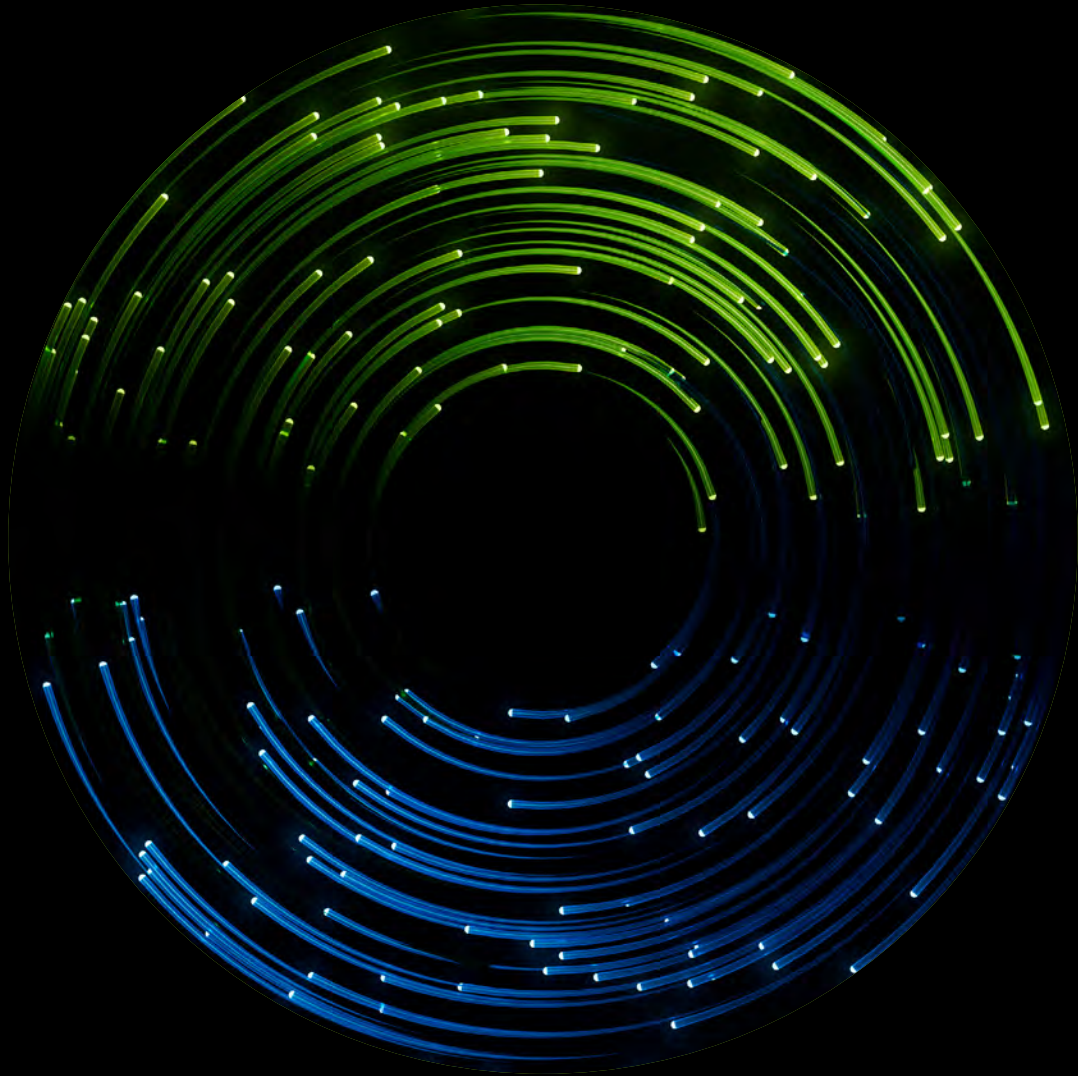
Building a proactive culture of resilience:
Empowering enterprises to thrive

Technology resilience is the ability of a system to continue operating and recover swiftly under adverse conditions. **Resiliency has become more crucial as we navigate an era marked by increasing complexity—due to distributed architectures, multi-hybrid cloud environments, thousands of microservices, and interconnected systems.**

Challenges like perpetual technical debt, rigid systems, shifting regulations, organizational complexity, technology disruptions, and delivery friction create significant gaps. The "shift-left culture," new regulatory requirements (e.g., DORA,[1] SEC,[2] OCC,[3] FFIEC[4]), and a changing regulatory ethos add complexity to resilience, necessitating a balance between regulatory and market-driven solutions. Additionally, the shared responsibility model with third parties such as vendors, hyperscalers, and heightened customer expectations for "always-on" services further complicates matters.
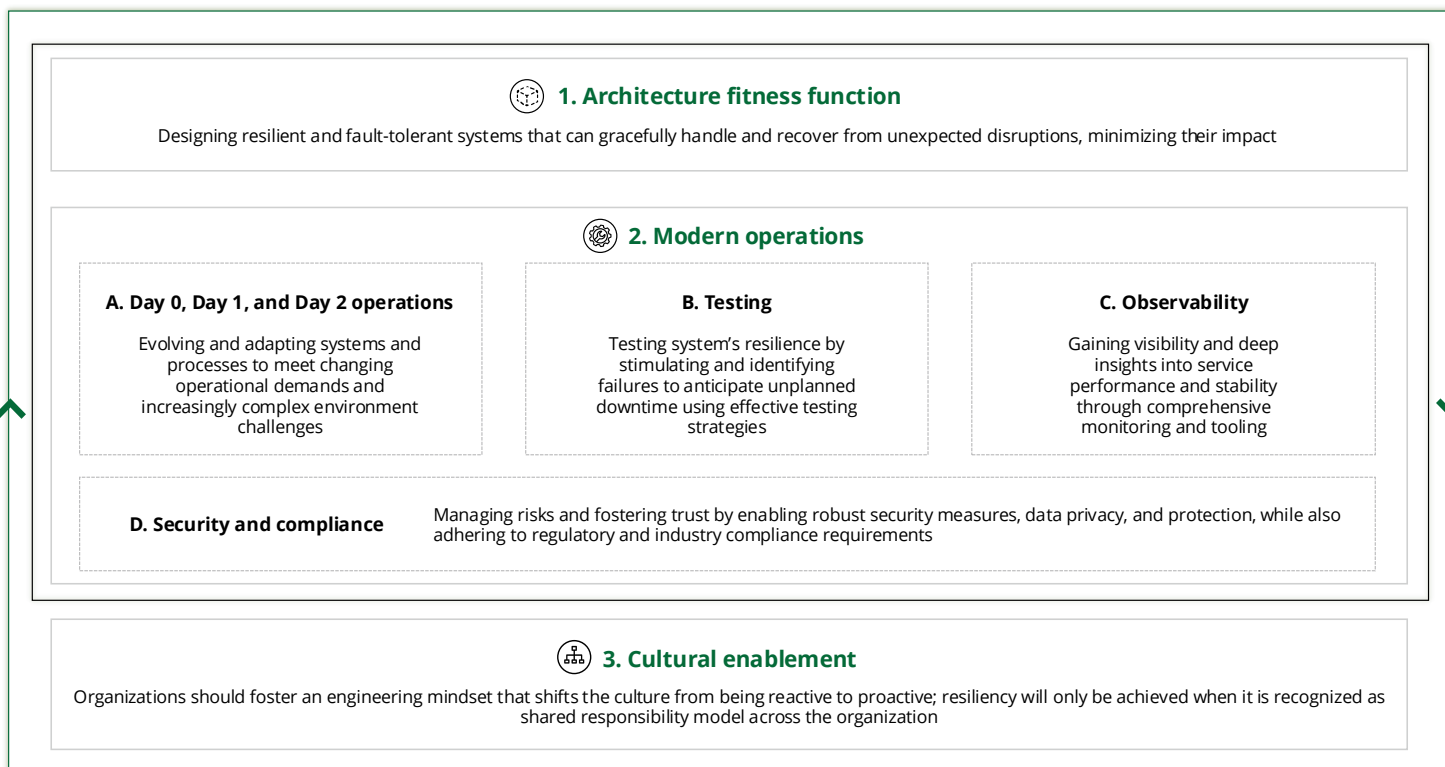
Resilience failures now carry severe consequences, potentially leading to competitive disadvantages and loss of customer trust. A recent faulty software update caused a major IT outage[5] worldwide, disrupting operations across sectors such as banking, airlines, and hospitals. This incident highlights the vulnerability of our interconnected world and the fragility of our technological environment.

Staying ahead of the curve: Deloitte's Enterprise Resiliency Engineering Framework

Deloitte's Enterprise Resiliency Engineering Framework provides **valuable guidance for building robust mitigation strategies, ensuring operational continuity during challenging times.** This framework fosters a proactive resilience culture, extending beyond mere availability and data protection, emphasizing preparedness and adaptability across architectural and operational pillars (figure 1).

Leaders must proactively mitigate resiliency problems to build reliable and robust systems and reduce the cost of fixing issues. Enabling organizations to assess their current state and recommending resilience improvement opportunities, such as implementing architectural patterns to remediate failures, or executing gamedays, ingrains a "resiliency-first" mindset and culture over time, marking a shift from how resilience is enabled today.

Figure 1. Deloitte's Enterprise Resiliency Engineering Framework

1. Architecture fitness function

Designing resilient and fault-tolerant systems that can gracefully handle and recover from unexpected disruptions, minimizing their impact

2. Modern operations

A. Day 0, Day 1, and Day 2 operations

Evolving and adapting systems and processes to meet changing operational demands and increasingly complex environment challenges

B. Testing

Testing system's resilience by stimulating and identifying failures to anticipate unplanned downtime using effective testing strategies

C. Observability

Gaining visibility and deep insights into service performance and stability through comprehensive monitoring and tooling

D. Security and compliance

Managing risks and fostering trust by enabling robust security measures, data privacy, and protection, while also adhering to regulatory and industry compliance requirements

3. Cultural enablement

Organizations should foster an engineering mindset that shifts the culture from being reactive to proactive; resiliency will only be achieved when it is recognized as shared responsibility model across the organization

Source: Deloitte

2

Achieving proactive resilience may seem daunting, but a reference model can help organizations navigate challenges with confidence and adaptability. Ultimately, proactive resilience flips the script, driving businesses to thrive in an unpredictable world.

1. Architecture fitness function

At Deloitte, we thoughtfully assess and design resilient architecture for critical systems, recognizing that resilience is the backbone of robust systems, enabling them to **withstand and recover from unexpected failures.**

- **Resiliency patterns:** By implementing proven resiliency patterns, such as circuit breakers, time-outs, geographical redundancy, and active-active failover, traffic distribution helps prevent cascading failures in distributed systems maintaining their stability.

- **Deployment strategies:** Modern release management techniques, such as blue/green deployments and canary releases, ensure component resiliency and minimize downtime risks in production environments.

- **High availability and fault tolerance:** We advocate for redundancy across the technology stack, adopting availability zones, multi-regions, and modern data protection techniques and orchestration runbooks to facilitate quick recovery from significant failure events.

- **Policy-as-code:** By defining, enforcing, and codifying policies throughout the development life cycle, we help ensure application teams adhere to reliability standards.

- **Codify standards and hygiene:** Adhering to defined standards governing code quality and consistency reduces the likelihood of system failures due to code-related issues.

2. Modern operations

A. Day 0, Day 1, and Day 2 operations
Adopting site reliability engineering (SRE) practices requires patience and collaboration. A shift-left culture **integrates life cycle operations activities, such as planning and configuring maintenance tasks, earlier in the development life cycle,** fostering enhanced efficiency, collaboration, and reliability.

- **Resiliency practices:** Developing standardized and repeatable practices is crucial for driving SRE adoption.

- **Incident and problem management:** Implementing clear communication channels and standardized processes ensures that incidents are handled swiftly and effectively.

- **Release and change management:** Defining checks, tollgates, and standardized procedures throughout the software development life cycle (SDLC) aims to achieve stable releases with minimal risk to production environments.

- **Root cause analysis and post-incident reviews:** Establishing blameless procedures allows us to constructively identify incidents' underlying causes.

- **Automation:** Identifying opportunities for automation can significantly reduce routine tasks (e.g., infrastructure provisioning).

B. Testing

Building robust modeling, experimenting, and testing capabilities can help address challenges preemptively.

· **Failure mode and effects analysis (FMEA):** Establishing FMEA processes helps mitigate risks before they become issues.

· **Chaos testing:** Designing a library of chaos recipes for common fault injection patterns helps uncover vulnerabilities in a controlled environment.

· **Functional testing:** Comprehensive guidelines for functional testing are essential for maintaining a solid resiliency posture.

· **Nonfunctional testing:** Rigorous processes for non-functional tests allow us to accurately evaluate systems' speed, reliability, and performance levels.

· **Gameday and DR testing:** Regular gamedays and disaster recovery testing build muscle memory for real-world incidents.

C. Observability

Observability empowers organizations to **gain real-time insights into application health and performance.**

· **Telemetry:** Establishing a robust telemetry system provides comprehensive real-time system insights utilizing log management, time-series databases, and event correlation technologies.

· **Notification and alerting:** Configuring appropriate thresholds and alerts ensures critical incidents are promptly communicated.

· **Service level indicators and objectives (SLI/SLOs) and error budgets:** Collaborating with business and technology teams helps identify applicable SLIs and determine SLOs alongside error budgets.

· **Reporting and dashboards:** Integrating data from various sources into consolidated dashboards provides tailored real-time insights.

· **Intelligent ops integrating with development life cycle:** Integrating with the SDLC phases, we believe in observability that transcends traditional logging, monitoring, and metrics to offer a holistic view of an IT system's health, behavior, and performance.

D. Security and compliance

In today's rapidly evolving digital landscape, the importance of security and compliance cannot be overstated.

· **Data privacy and protection:** Establishing and implementing data privacy and protection measures to securely handle personal and sensitivew information.

· **Third-party risk management:** Developing strategy to identify, assess, and mitigate risks associated with third-party relationships.

· **Regulatory and industry standards:** Adapting to regulatory and industry standards by defining a structured approach for continuous assessment and monitoring.

· **Continuous monitoring and validation:** Integrating real-time insights with regular security controls, policies, and compliance requirements assessments.

· **Auditability and traceability:** Maintaining auditability through robust audit trails and documentation practices enables us to demonstrate compliance effectively.

3. Cultural enablement

Fostering a culture of resilience requires a comprehensive cultural shift. SREs rely on metrics and data to make informed decisions and encourage **continuous improvement through regular reviews and updates to processes and tools.** This data-driven approach helps in identifying areas for improvement and implementing new practices that enhance overall resilience.

- **Operating model:** Embedding SRE roles throughout the SDLC.
- **Tooling:** Enabling and scaling the adoption of resiliency standards through practical tools and processes.
- **Communication management:** Clear and consistent communication is vital for any cultural shift.
- **Key performance indicators and key results areas:** Establishing ambitious yet measurable goals aligned with organizational objectives.
- **Training and incentivization:** Providing technical training on resiliency for all levels and developing mechanisms to reward desired behaviors.

By embracing these practices, we assist organizations in transitioning to modern operations, enabling them to **harness real-time insights and effectively manage error budgets.** This proactive mindset is crucial in safeguarding customer trust and maintaining organizational integrity in an unpredictable world.

Resiliency engineering framework in action: Use case

One of our clients faced significant reliability challenges with regular outages and needed to prepare for an influx of millions of new transactions on their platform. Despite establishing incident management processes, resiliency knowledge and skill gaps posed substantial challenges. The client sought our partnership to embark on their resiliency-bolstering journey.

By leveraging Deloitte's Enterprise Resiliency Engineering Framework, we empowered our client to adopt engineering practices, enhance IT resiliency, and seamlessly prepare for increased traffic. This transformation included:

- **Establishing an SRE operating model:** Clearly defined roles and responsibilities were set to ensure a structured approach to engineering site reliability.
- **Rolling out a robust SRE framework:** Implemented a comprehensive framework to guide resiliency practices across the organization.
- **Enabling precise SLIs/SLOs:** Defined and monitored SLIs/ SLOs to maintain performance standards.

Through proactive measures such as FMEA and chaos testing, we identified potential faults before they became issues. We also published resiliency software standards and upskilled teams to foster a culture of resilience.

The results were significant:

These efforts collectively contributed to enhancing system reliability and fostering a resilient organizational culture. This proactive approach ensured that our client was well prepared to handle the increased customer base and maintain operational continuity.

By collaborating with Deloitte and leveraging our Enterprise Resiliency Engineering Framework, the company mitigated most of its stability risks and built a robust foundation for future growth and stability.

Incidents were reduced by

25%

Duration of major incidents was reduced by nearly

30%

400+

failure modes were identified, and 60 were remediated across more than 100 critical path applications

These efforts collectively contributed to enhancing system reliability and fostering a resilient organizational culture. This proactive approach ensured that **our client was well prepared to handle the increased customer base and maintain operational continuity.**

By collaborating with Deloitte and leveraging our Enterprise Resiliency Engineering Framework, the company mitigated most of its stability risks and built a robust foundation for future growth and stability.

Why Deloitte?

In today's dynamic business landscape, resilience is essential. Embrace resilience engineering to ensure seamless operations and unwavering performance. Contact us to fortify your technology and lead with confidence.

For more information, please contact:

Chris Thomas
Principal
Deloitte Consulting LLP
chrthomas@deloitte.com
+1 (312) 486 1875

Nitin Gupta
Senior Manager
Deloitte Consulting LLP
nitingupta4@deloitte.com
+1 (412) 338 7535

Endnotes

1. Official Journal of the European Union, Regulation (EU) 2022/2554, EUR-Lex, December 27, 2022.

2. US Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations, "Cybersecurity and resiliency observations," February 27, 2025.

3. Jennie Clarke, "OCC to join regulatory rollout as it eyes operational risk requirements for banks," Global Relay, March 14, 2024.

4. National Credit Union Administration (NCUA), "Financial regulators revise Business Continuity Management booklet to stress to examiners the value of resilience to avoid disruptions to operations," press release, November 2019.

5. Sean Michael Kerner, "CrowdStrike outage explained: What caused it and what's next," TechTarget, October 29, 2024.

Deloitte.