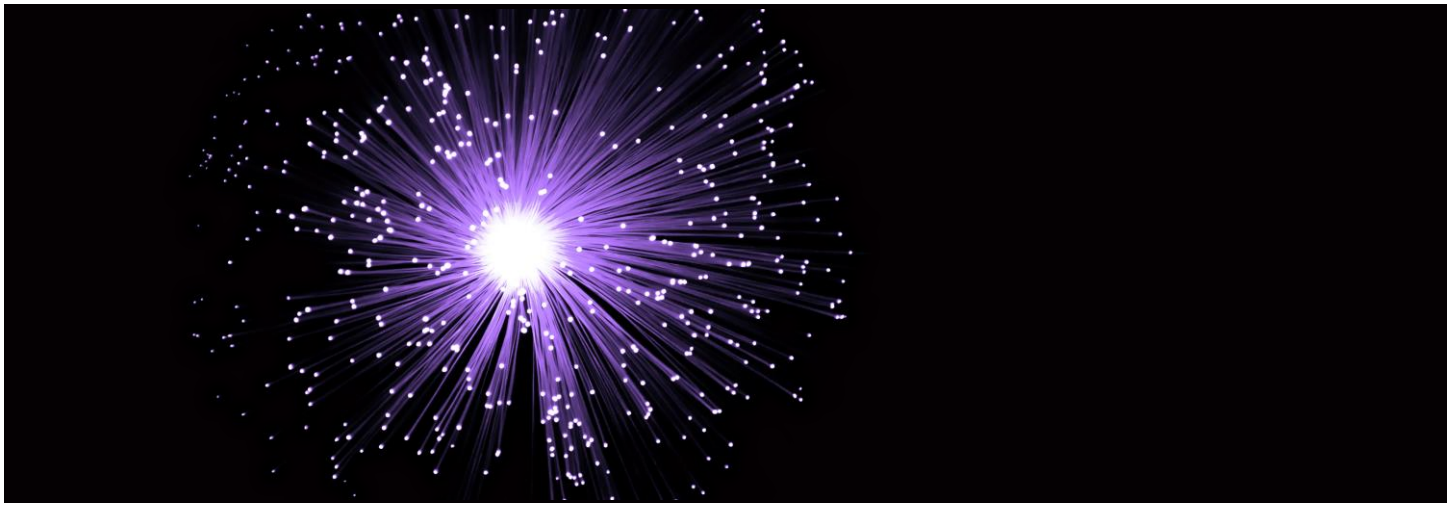
Deloitte.

amazon web services | Partner Network



Technical Resilience

Building the "always-on" enterprise with Deloitte Advisory and Amazon Web Services

Organizations spend millions of dollars on disaster recovery (DR) solutions that rely on tight interconnectivity, replication, redundancy, and open networks designed to support recovery from physical disruptions. During a cyber incident, these technologies can both complicate the recovery process and extend the adversary's reach.

Consider ransomware: Malware is planted in a production environment and the backup solution, working as designed, automatically propagates the infection to the recovery environment, rendering it unusable. Ironically, the most critical environments—typically equipped with the strongest recovery solutions—are often disproportionately impacted. The lack of clean and secure backups are the primary reason many companies are paying ransoms.

Although the purpose of disaster recovery investments is to provide for business resilience in the face of a technical failure, the architecture of many of these solutions—reactive in nature and focused on redundancy—has become an expensive liability. As threats become more complex and downtime becomes increasingly intolerable, a new resilience approach is needed.

Cloud computing, now widely used to revolutionize how business is conducted, offers the potential for new approaches to guarding against business disruption. Deloitte Advisory's Technical Resilience service, powered by Amazon Web Services (AWS), helps organizations establish a cloud-first, "always-on" strategy as part of a larger program to manage cyber risk in the growing digital economy. This approach shifts the paradigm away from reactive recovery measures toward a more secure, proactive, and resilience-centered one.

Through new risk management strategies, innovative architecture, and redesigned operating models, Deloitte Advisory's Technical Resilience leverages the power of AWS to help clients promote business continuity across their organizations, improve cyber risk postures, reduce costs, and increase operating efficiency.

No room for downtime

The notion of "acceptable downtime" that has underpinned traditional DR strategies is increasingly out of touch with the demands of customers, partners, and corporate directors, who expect technology to be always on. This is not unreasonable, given how technology-dependent society has become; technology brings ambulances to the right door in the least amount of time; it powers our national economy; it powers our supply chains; it keeps the lights on.

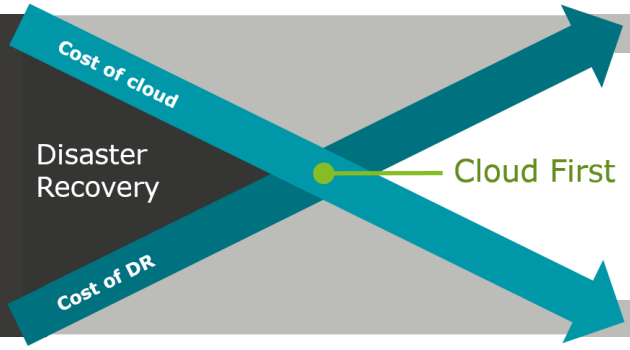
Downtime results in losses in productivity, public confidence, revenue and customer relationships—especially in an economy in which customer's other options are only a click away. Service level agreements can encourage acceptance of performance degradation at the component level, even though this suboptimal service may result in customer impacts similar to downtime itself. In addition, the very idea of acceptable downtime can result in a culture of complacency toward system maintenance and lack of interest in proactive forecasting that might help avoid future disruptions. The result can be repeated outages from predictable events.

Traditional DR: the risks are increasing

Legacy DR programs focus on redundancy as the primary approach to mitigating potential IT outages through data replication, high availability configurations, tight interconnectivity, and open networks. While these investments can shorten the time to recover from physical disruptions such as disk or interface failures, they were not designed for 24-hour news cycles and the never-idle digital economy. Many legacy DR solutions lag behind the degree of dependence on technology and are proving too expensive and outdated to provide appropriate mitigation of current and future technology risks. Current business trends exacerbate the problem:

- Rapid growth of digital business has created highly complex digital revenue streams that often lack manual workarounds needed to preempt or respond to potential disruption.
- Rapid evolution of cyberthreats has outpaced innovation in business resilience.
- Growing interconnectivity, driven by Internet of Things (IoT) adoption and technology interdependence, increases the probability and impact of disruptive events.
- Growing dependence on third parties and interdependence between entities increases the complexity of transactions, expands the potential reach of a single event, and increases the likelihood of supply chain disruption.

The total cost of ownership for cloud computing continues to decrease. As interdependency and business reliance on technology increase, the cost of traditional disaster recovery grows.



The time and money required to manage recovery needs is growing at an unsustainable rate. Redirecting DR spend to cloud infrastructure can increase technical resilience and total availability.

Cloud-first as a basis for Technical Resilience

As the number of endpoints grows (e.g., IoT), businesses and customers become more connected, technology interdependency increases, and the cost of traditional DR grows proportionally. The result is growing costs and a diminishing return on traditional DR planning and investment. Inversely, the cost of cloud is decreasing as productivity requirements grow, resulting in greater cloud adoption. In an economy that increasingly demands zero downtime, always-on can be the answer, inherently built into cloud solutions at affordable prices.

The cloud offers a logically-defined computing framework that is inherently scalable and responsive, allowing businesses to quickly adapt to changing conditions and fluctuating business cycles. But by itself, moving to the cloud will not allow you to realize these benefits. Building confidence and trust are vital to user adoption. Integrity concerns, which have limited cloud adoption to date, remain. Like traditional DR solutions, cloud computing has the potential to increase the attack surface, leaving a larger footprint to address. If cloud computing is not appropriately managed, implementation may open doors to increased cyber risk.

The Technical Resilience approach

Combining our strengths, Deloitte Advisory and AWS can help organizations adopt a proactive approach that moves business operations toward always-on capabilities and reduces cyber risk exposure. The AWS computing framework (see sidebar on page 4) integrates security as one of its four pillars: security, reliability, performance efficiency, and cost optimization.

In contrast to traditional contingency planning that serves as a bolt-on to established development and deployment processes, Deloitte Advisory's Technical Resilience helps clients transform to a proactive approach by guiding a fundamental shift in development, operations, and change management processes.

Getting started

Moving to a cloud-based Technical Resilience approach is not an all-or-nothing proposition. Indeed, few organizations can afford to simply walk away from their existing infrastructure investments. And not all systems or platforms are necessarily good candidates to be migrated to the cloud. Cloud services are inherently modular and flexible, making implementation

Features that support a Technical Resilience approach

- Auto-scaling, health sensing computing environment that has multiple failover capabilities
- Software-defines environment allows constant testing of failure scenarios
- Transparent computer expenditure that is easily linked to business owners by which to drive efficiencies
- Architecture templates that rapidly provision and configure entire networks, application services, and databases over multiple Amazon Availability Zones and Regions
- Inventory and configuration services that track configuration changes over time
- Virtual Private Cloud services to peer with third parties through Virtual Private Networks and Direct Connect
- Software-defined Internet Gateways, Domain Name Services (DNS), and Elastic Load Balancing Services to maintain availability and Network Address Translation (NAT) services
- Software-defined networking components that eliminate common network protocol attack vectors
- Integrated detective controls that span network, compute, and storage components
- Threshold and metric monitoring that trigger automation of response procedures as well as notification, both to people and other applications
- Extensive logging and asset tracking to satisfy the most stringent compliance requirements.

Four domains of a Technical Resilience solution

Strategy 	Building an always-on enterprise through agile, scalable, and adaptive solutions.
Governance 	Implementing new design standards that reduce the need for post-deployment contingency planning. Supporting standards enforcement through automated reporting. Employing an ecosystem approach that includes third parties in resilience activities.
Architecture 	Deploying secure, modular, monitored, cloud-enabled infrastructure with automatic failover capabilities.
Operations 	Driving risk ownership across the enterprise with automated testing to actively probe for weaknesses. Identifying preemptive event thresholds and building surge support to scale when needed.

readily adaptable to any organization's strategic IT plan. There are incremental steps that can be taken and expanded over time.

Re-allocate budgets for traditional DR infrastructure to a Disaster Recovery as a Service (DRaaS) solution in the cloud. This can introduce the financial, security, and operational benefits of the cloud while freeing up resources to be reinvested in production services.

Migrate to Technical Resilience for a your most critical digital services. Incorporating always-on principles into the requirements, design, implementation, and operational processes for your crown jewels can immediately improve risk posture and seed the resilience approach for the enterprise. Deloitte and AWS can provide proof-of-concepts that demonstrate the power of Technical Resilience.

Consider AWS for ancillary recovery needs. Traditional DR solutions are too expensive for organizations to provide full data center recovery capabilities. Scalable, cloud-based services can provide baseline protection for mission sensitive applications, data, and processing.

Building technical resilience toward the objective of being always-on does not mean disruptive events will not occur. However a pre-emptive approach leveraging risk-sensing and threat intelligence capabilities can support an organization's ability to take action earlier in the lifespan of the event to reduce overall impact.

The strength of the Deloitte Advisory/AWS relationship

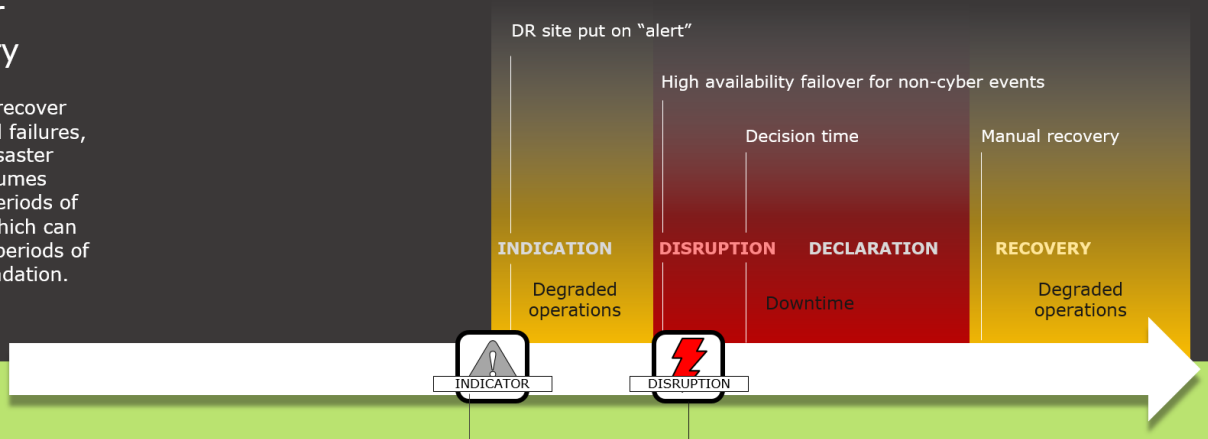
Our alliance brings together Deloitte Advisory's leadership in cyber and enterprise risk management with the leading security-enabled cloud infrastructure of AWS. In 2006, AWS began offering IT infrastructure services to businesses in the form of web services—now commonly known as cloud computing. Today AWS provides a highly reliable, secure, scalable, low-cost infrastructure platform that powers hundreds of thousands of businesses in 190 countries around the world, with over a million active customers spread across many industries and geographies.

In addition to having the right infrastructure, an always on enterprise requires the elimination of risk management silos, and the ability to leverage technology solutions within well-honed operational roles and processes aligned to serve the organization's business risk agenda.

The Deloitte Advisory Technical Resilience offering draws on diverse teams of multi-disciplinary specialists in risk, regulations, strategy, technology, architecture and implementation, offering the broad capabilities needed to help clients develop *Secure.Vigilant.Resilient.*™ cyber risk programs.

Disaster Recovery

Designed to recover from physical failures, traditional disaster recovery assumes acceptable periods of downtime, which can lead to long periods of service degradation.



Deloitte.

Technical Resilience

Developing technical resilience reduces total disruption time through proactive measures, innovative architecture, and operational excellence.

READINESS

IT Infrastructure designed to withstand advanced disruptions and protect data utilizing global resources. Business continuity governance and controls integrated into design.

Proactive risk sensing and fault discovery through application and resource health monitoring and security trip wires. Automated failure detection and notification to trigger incident escalation.

RESPONSE

Maintain business operations as network and compute resources dynamically provision, re-configure, and scale. Scripted incident management to reduce impact and collect data.

RECOVERY

Automatic orchestration of full business failover to counter catastrophic outages. Self-healing solutions designed and tested for failure and validated to properly recover.

Recovery "checks and balances" baked into automation to reduce errors. Robust change management tools focused on moving to and maintaining a new known good state.

powered by amazon web services

Amazon VPC

Amazon CloudWatch

Elastic Load Balancing

AWS CloudFormation

AWS Config

A Technical Resilience approach can—

- **Help you advance toward an always-on enterprise** by aligning organizational elements to a zero downtime expectation.
- **Protect against evolving cyberthreats** and cultivate the ability to be *Secure.Vigilant.Resilient.*™
- **Reduce costs** through a focus on scalable, rapidly-provisioned solutions over redundancy.
- **Improve return on risk management investments** through agile solutions that align risk mitigation spend to actual disruptive events.
- **Improve market agility** through accelerated change management processes.

Take action today! Request a briefing.

Deloitte Advisory contacts

John Gelinne
Managing Director
Advisory Cyber Risk Services
Deloitte & Touche LLP
jgelinne@deloitte.com

Pete Renneker
Senior Manager
Advisory Cyber Risk Services
Deloitte & Touche LLP
prenneker@deloitte.com

Amazon Web Services contacts

Alejandro Flores
Global Partner Solution Architect
Management Consulting and Advisory
Amazon Web Services
alejaflo@amazon.com

Piyum Zonooz
Global Partner Solution Architect
Amazon Web Services
pzonooz@amazon.com

Howard Bandler and Vince Garcia contributed to this article.