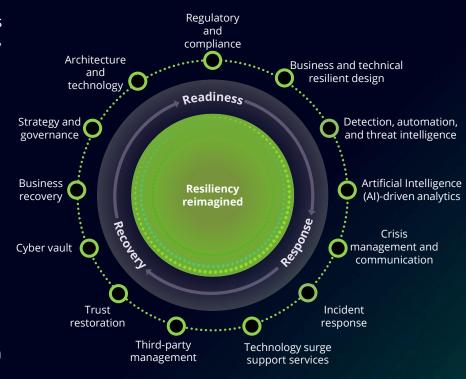
Deloitte.

Resiliency reimagined: Readiness, response, recovery

Recent disruptions to business operations show that conventional risk management, business continuity and disaster recovery approaches are not enough for organizations to effectively respond and recover from severe but plausible disruptions. It requires an approach that integrates different disciplines and design thinking to balance resilience spend with an organizations' risk appetite.

Unforeseen disruptions are often inevitable. By preparing with readiness, response, and recovery, companies can significantly enhance their *resiliency*. Leveraging our vast experience and ecosystem and alliance collaborators, we've developed key guidelines to assist in formulating a resilience strategy that aligns with your risk tolerance so you can remaster resilience.



O Disciplines and solutions of a comprehensive resilience program

Market drivers and trends

The reality of today's environment



Cyberattacks are more frequent and far-reaching

Threats do not exist in isolation—there is a cyber lifecycle challenge affecting many industries.



Increased focus on protecting the business is needed

Lack of a business-centered strategy results in deprioritized investments and resources to mitigate threats.



Legacy resilience is costly and ineffective

Traditional redundancy and replication strategies can inadvertently propagate modern cyber risks rather than mitigate them, highlighting the need for smarter, more secure solutions.



There is a growing pressure to be 'always on'

Customers and business partners expect services to be "always on," necessitating organizations to improve cyber resiliency practices and technologies to meet these demands.



Organizations often struggle to recover critical technologies

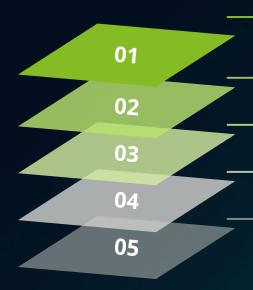
Threat actors target critical infrastructure, including backup technologies that are often ill-equipped.



Resilience efforts are often siloed and lack accountability

As threats grow in frequency and scope, an organization's ability to prepare, respond, and recover hinges on a shared sense of responsibility.

Building blocks of modern resiliency



Unified strategy and accountability

Cultivating a shared vision and sense of responsibility across an organization, including its board members

Third-party risks

Managing and mitigating risks associated with external partners and suppliers

Ransomware preparedness

Protecting data and organizational operations against critical impact cyberthreats

Demonstrable recoverability

Establishing confidence in response and recovery from disruptions

Cost optimization

Reducing costs while improving efficiency and performance by assessing and comparing cloud services and recovery solutions

Solutions for cyber readiness, response, and recovery



Resilience strategy

Business resilience



Technical resilience



Cyber and data resilience



Resilience as a service

Resilience strategy prepares and designs capabilities and processes for an organization to effectively anticipate, respond to, and recover from disruptions.

Build end-to-end resilience into critical operations so you can more effectively protect your organization against significant disruptions.

Through innovative architecture designs and integrated technologies, technical resilience shifts the paradigm away from reactive recovery measures toward a more proactive resilience-centered approach.

Improve your organization's resilience against a wide range of data disruption scenarios, including destructive cyberattacks and data breaches. Employ a broad suite of managed services, including functional testing and continuous monitoring, built upon your existing technology foundation so you can focus on what matters most.



Sharon Chand
Cyber Defense & Resilience
Principal
Deloitte & Touche LLP

shchand@deloitte.com



Mike Kosonog Resilience Partner Deloitte & Touche LLP mkosonog@deloitte.com



Kevin Urbanowicz
Security Operations
Managing Director
Deloitte & Touche LLP
kurbanowicz@deloitte.com



Niloo Bedrood
Crisis & Incident Response
Managing Director
Deloitte & Touche LLP
nbedrood@deloitte.com



Andrew Douglas
Attack Surface Management
Managing Director
Deloitte & Touche LLP
andouglas@deloitte.com

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this presentation, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.