

# IBM Cloud Resiliency Consulting Services

*Take a strategic approach to making your enterprise more resilient and always-on*



---

## Business benefits

- Collaborate with disaster recovery and business continuity specialists to help you avoid downtime in a more demanding and complex environment
  - Apply a structured approach with the IBM Resiliency Services Framework seven-layer model to make your business resilient and always-on
- 

Surviving in today's competitive business environment requires continuous availability of your IT systems, applications and data. Your employees, customers and business partners expect that the information, products and services they need will be always-on—available when, where and how they want them.

To better meet these demands, systems are increasingly integrated and distributed across complex IT environments including private, public and hybrid clouds, which can create potential vulnerabilities. Linking more critical systems together to manage higher expectations complicates business continuity, disaster recovery, resiliency, regulatory compliance and security. When one link in the chain breaks or comes under attack, the impact can ripple throughout the business. Your organization can face revenue loss and eroded customer trust if you fail to maintain business resiliency while rapidly adapting and responding to risks and opportunities.

IBM® Cloud Resiliency Consulting Services offers a holistic approach to evaluate your cloud risk awareness and determine your organization's resilience level. IBM uses an object-oriented framework combined with a robust enterprise-wide approach to determine resiliency readiness and define measures to mitigate identified risks. This approach helps you identify both cloud and traditional IT risks and vulnerabilities to continuous business operations. It also recommends solutions to help manage those risks, along with measures to enhance or establish your resiliency program.



## IBM Resiliency Services Framework

Businesses in today's digital environment cannot afford downtime. The IBM Resiliency Services Framework is a seven-layer model that helps your business and IT leaders examine resiliency operations at both the physical and virtual layers of the organization to identify risks and vulnerabilities.

As part of a detailed resiliency program, operations in each layer of the framework must meet industry and corporate standards for business continuity, disaster recovery, resiliency, regulatory compliance (where required) and security. Because these layers are interdependent, each must be examined in terms of its ability to support the others. This approach helps your organization promote an integrated resiliency that is built in, not bolted on. It also can prepare you for an always-on world.

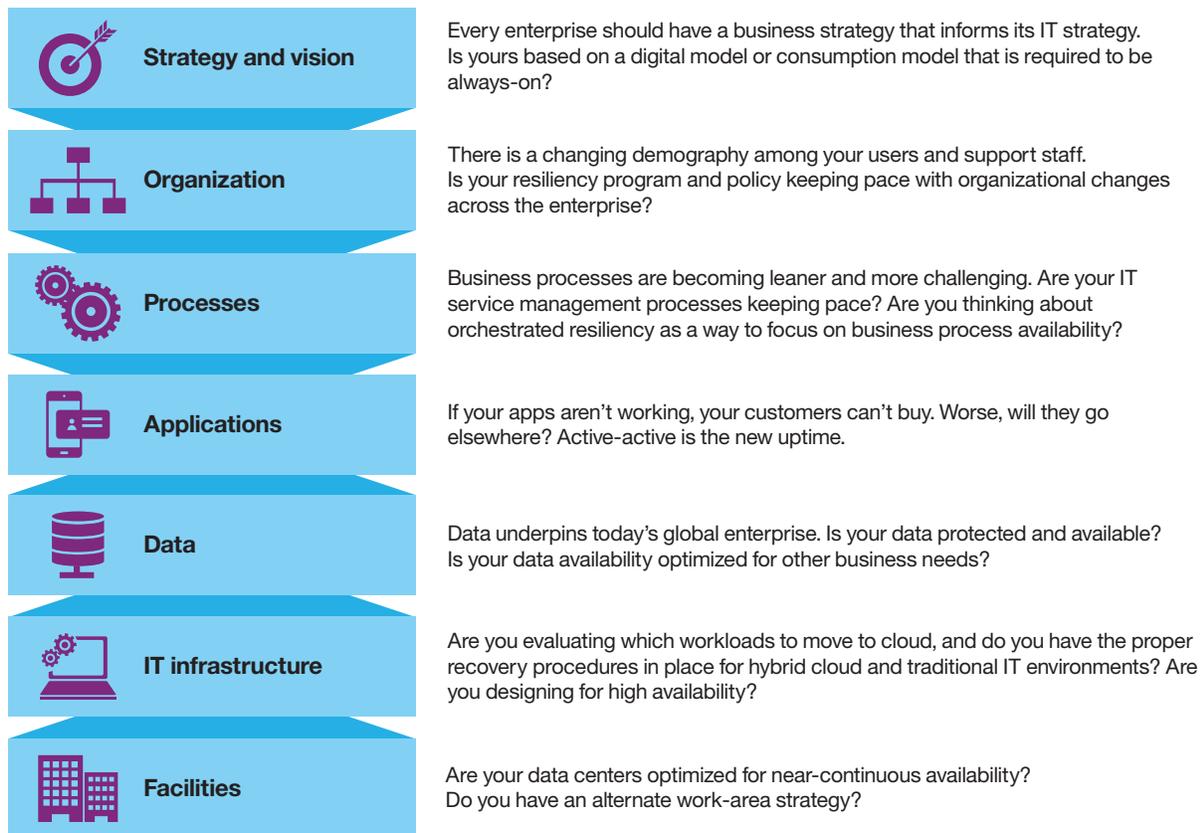


Figure 1: IBM Resiliency Services Framework.

## IBM Cloud Resiliency Consulting Services four-phase approach

Phase 1 — IBM's consulting approach begins with **Assess and Evaluate**, and includes an analysis of potential cloud-related risks to your business, their impact and your ability to mitigate them. IBM can diagnose the risks to your business objectives and prescribe appropriate actions.

Phase 2 — **Plan and Design** looks at your current state and helps you define the right strategy. In this phase, IBM can also develop the corresponding resilient cloud architecture; resiliency program; recovery and restart workflows; and run books for business continuity, IT resiliency and enterprise crisis management.

Phase 3 — The next step is **Implementation and Test**, which validates your resiliency program, plans, procedures and workflows for cloud-based and traditional IT environments to identify any issues and gaps to be addressed before a disruptive event occurs.

Phase 4 — **Manage and Sustain** provides a centralized governance program for managing and maintaining a sustainable business resiliency program. This program can monitor current conditions to respond to risk—managing regulatory compliance and reporting using resiliency dashboards to demonstrate readiness and results of business investment in resilience.

A good way to start this approach is with a consultative discussion with IBM to measure your current resiliency program using the framework. During this face-to-face discussion, IBM representatives help you prioritize exposures that pose the greatest risk to critical operations. This helps you build a business case to implement appropriate mitigation technologies and techniques to more effectively address your risks.

IBM's thorough onsite risk assessment uses industry best practices and comparisons to more quickly document findings and recommendations for mitigating and managing IT and operating risks that present the highest potential to interrupt your business. The resulting action plan shows how you can address these risks with expected business values.

## Why IBM Resiliency Services?

IBM Resiliency Services can design, implement, manage and test your resiliency solutions through every layer of the IBM Resiliency Services Framework. Many solutions are offered as managed services, including cloud services for resiliency orchestration, data and application backup and availability, server recovery, incident and crisis management workflows, and communications. Integrating managed services into your organization is a way to facilitate a viable and sustainable resiliency program while allowing internal resources to focus on the day-to-day operations of the business.

With more than 50 years' experience in business continuity, disaster recovery and resilience, IBM is an acknowledged market leader and innovator in this field. IBM's 4,000 continuity and resiliency professionals serve over 10,000 clients. You can find IBM's 330+ cloud resiliency centers in 68 countries. Few organizations operating in the resiliency arena can match IBM's track record, expertise, portfolio breadth and reach.

## For more information

To learn more about the IBM Cloud Resiliency Consulting Services, please contact your IBM representative or IBM Business Partner, or visit the following website:

[ibm.com/services/continuity](https://ibm.com/services/continuity)



---

© Copyright IBM Corporation 2017

IBM Corporation  
IBM Resiliency Services  
3039 Cornwallis Rd., Bldg. 201  
Research Triangle Park, NC 27709

Produced in the United States of America  
July 2017

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



Please Recycle