IBM

Beyond disaster recovery: becoming a resilient business.

An object-oriented framework and methodology

by Richard Cocchiara
Chief technology officer for business continuity
and resilience services

Contents

Executive summary

As you probably understand all too well, today's business environment is characterized by rapid, unpredictable change. Some changes bring opportunities for your business, while others bring challenges and sometimes even threats. But no matter what, your business has to be responsive and resilient—seamlessly taking advantage of opportunities while mitigating risks. Your IT infrastructure must be designed to help ensure the continuity of your business operations in the event of an unexpected disruption, and to secure data integrity. It also must help you comply with government regulations and integrate risk strategies to reduce costs, and it must be able to scale rapidly and automatically as the marketplace changes.

To help organizations understand and manage the process of becoming resilient, IBM has developed an object-oriented framework and transformation lifecycle. Borrowing from the concept of an object-oriented database, IBM has created a business resilience framework that is designed to help you identify the object layers that make up your company—ranging from the strategic overlay, all the way down to the nuts-and-bolts technologies and facilities. Within each layer, the objects are assigned specific attributes that help manage the risks associated with each object. Once you understand these objects, their attributes and the relationships among them, you can begin to identify areas for improvement. IBM can take you through the business resilience transformation lifecycle to help you:

- *Determine which risks may affect your organization*
- *Calculate the potential impact that these risks could have on your organization*
- *Plan for how the objects in your current infrastructure could respond to these risks*

- *Design or update your infrastructure to mitigate these risks and to leverage any opportunities that might arise from marketplace changes*
- *Execute your strategy for improving your business resilience*
- *Implement the changes to each object layer*
- *Test your overall resilience*
- *Manage your resilience program to incorporate improvements and changes in technology.*

This white paper explores the business and technical advantages of an object-oriented framework and transformation lifecycle for business resilience.

Coping with continuous change

As you know, fluctuating business conditions are a double-edged sword. Almost any risk—whether it comes in the form of an opportunity or a threat—requires a response from your business. If you respond inappropriately or too slowly, you could lose ground to your competitors. For example, while too much success may not sound like a threat to your business, it can become one if you're not prepared to handle a surge in customer demand. For example, when Victoria's Secret televised a fashion show during the 1997 American football Super Bowl, the company was unable to scale to meet the ensuing demand for access to its Web site, resulting in significant performance degradation and customer dissatisfaction.

Any risk, whether opportunity or threat, requires a response from your business.

On the other hand, a disruption in business operations and services, whether from a natural disaster, a terrorist strike, a cyber attack or a simple malfunction, can seriously reduce your revenues and even do long-term damage to

Combining several risk management strategies into a single, integrated strategy ist he best response to the threat of disaster.

A business resilience framework should address six key areas.

your brand. Industry estimates indicate that upwards of 40 percent of organizations without business continuity and recovery plans will go out of business within a few years of a major disaster.

The best response to the threat of disaster is to combine several disparate risk-management strategies into a single, integrated resilience strategy that will allow your organization to adapt and respond rapidly to opportunities, regulations and risks—in order to maintain security-rich business operations, be a more trusted partner and enable growth. Because such an approach addresses both the positive and negative ramifications of risk, IBM uses the term "business resilience" to distinguish between this comprehensive strategy and narrower approaches, such as disaster recovery, high availability, security and business continuity.

What business resilience means—some basic requirements
CEOs typically share a common list of concerns that a business resilience framework should address:

- *Continuity of business operations—become more anticipatory, adaptive and robust, from IT through all business processes*
- *Regulatory compliance—comply with new and changing government rules and regulations more quickly and cost-effectively*
- *Integrated risk management to reduce costs—stay competitive by managing risk more efficiently and cost-effectively*
- *Security, privacy and data protection—protect against internal and external threats, and help develop a critical information management policy*

- *Access to expertise and skills (via outsourcing or training)—develop the infrastructure to support the easy acquisition and management of expert assistance in maintaining continuous business operations*
- *Marketplace readiness—anticipate and respond to changing marketplace conditions and accelerating research and development as necessary to get the right products to the right buyers at the right time.*

A holistic approach to a business resilience strategy can help minimize risks, maximize opportunities and address compliance needs simultaneously.

In the past, businesses typically have addressed these concerns separately. However, many companies now recognize that it's more cost-effective to combine them into a single, integrated strategy. A holistic approach can help minimize risks, maximize opportunities and address compliance needs—all at the same time. But how do you perform a holistic risk assessment of your entire enterprise without missing any critical element? IBM has found that an object-oriented framework can help you model your total business infrastructure and identify issues that must be addressed to make your business more resilient.

The business resilience framework—an object-oriented approach

IBM has identified components that can help companies understand issues and speed improvements and upgrades for enhanced resilience.

IBM has spent years analyzing what is necessary to ensure business resilience. In the process, IBM has identified a collection of components—called objects—that together can be used to model your entire business infrastructure. Inspired by the concept of database objects, these components have attributes that help define them in terms of their ability to address the six basic requirements of business resilience. Objects can share similar attributes, and these shared attributes, in turn, help define the relationships among objects. And objects with shared attributes can be grouped into object classes. Companies can then use these classes to understand common issues and to speed the deployment of improvements and upgrades designed to promote resilience.

Resilience layer	Object class	Object	Attribute	Value	Maturity value	Attribute relationships
Process	IT process	Problem management	Owner	John Smith	3	Common primary owner with change management, with no secondary or tertiary owner defined
		Change management	Owner	John Smith	3	Common primary owner with problem management, with no secondary or tertiary owner defined

Maturity levels
1 = No owner 2 = Multiple owners 3 = Primary owner defined, no backup 4 = Primary and secondary owner defined
5 = Primary and secondary owner with defined authorities

Table 1. Sample objects and attributes

As Table 1 demonstrates, two or more separate objects can exist within a class and share multiple attributes as well−in this case, the attributes of owner and documentation. As values are assigned to each attribute, you can see whether each of these objects has, for example, the same owner. If, indeed, they do share an owner, for example, John Smith, you can begin to understand the consequences for your organization of losing John Smith. In the table, the attribute "John Smith" affects both change and problem management, so the ability of your business to continue operations in the face of such a loss could be restricted.

Identifying single points of failure can help develop failover techniques and redundancies for certain types of object attributes.

An object-oriented framework for business resilience is a useful tool for understanding the strengths and weaknesses of a company's infrastructure.

The same type of analysis may also be applied throughout the organization, so you can assess whether you have undue risk associated with any individual, technology or business process. Once you identify these single points of failure, you can then develop failover techniques and redundancies for certain types of object attributes. At the same time, you may also learn that some objects have attributes that can be consolidated for more efficient risk management. For example, under change management, you could find that you have multiple values for owner and control attributes. While this may be sound from a redundancy standpoint, it can introduce unnecessary confusion into your resilience program. Instead, it may be more efficient to assign primary and secondary owner attributes, so it's clear who will take over if the primary owner is unavailable. In any case, an object-oriented framework for business resilience is a useful tool for understanding the strengths and vulnerabilities of your existing infrastructure.

Clearly, an organization will identify many objects in the process of creating a comprehensive model of its business resilience capacities. To simplify what would otherwise be an unwieldy list of objects, IBM created a super-set of object classes, which IBM refers to as layers within the business resilience framework. Not surprisingly, they echo the layers of most business organizations. These layers are:

- *Strategy—objects related to the strategies used by the business to complete day-to-day activities while enabling continuous operations. Examples include financial, manufacturing and disaster recovery strategies.*
- *Organization—objects related to the structure, skills, communications and responsibilities of your employees. Examples include human resources, training, and internal and external communications.*

Highlights

Super-sets of object classes—
including strategy, organization and
processes—echo the layers found
in most business organizations.

- *Applications and data−objects related to the software necessary to enable business operations, as well as the method used to develop that software. Examples include customer relationship management (CRM) applications, enterprise resource planning (ERP) applications, databases and transaction processors.*
- *Processes−objects related to the critical business processes necessary to run the business, as well as the IT processes used to ensure smooth operations. Examples include accounts receivable, accounts payable, change management and problem management.*
- *Technology−objects related to the systems, network and industry-specific technology necessary to enable your applications and data. Examples include host systems, workstations and Internet Protocol (IP) networks.*
- *Facilities−objects related to the buildings, factories and offices necessary to house your organization and your production or service technologies. Examples include data centers, office buildings and physical security operations.*
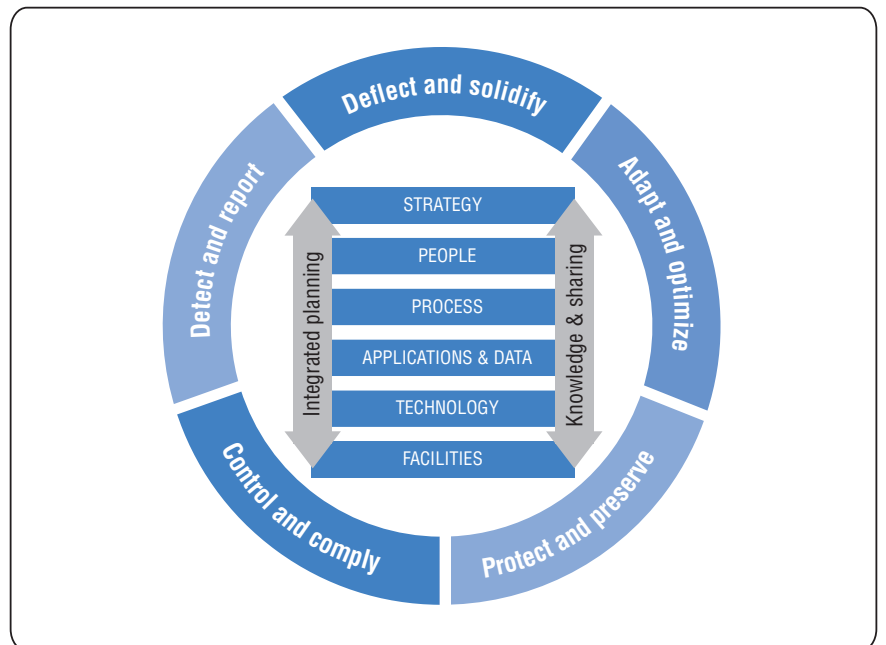

Figure 1.
An object-oriented business resilience framework contains multiple levels of varying granularity.

Five major attribute classes provide a more granular view of business resilience and the traits that enable objects to respond to risks and opportunities.

While these object layers can help you conceptualize and identify the components of your company's business resilience, it's possible to obtain a view that's even more granular. Attributes, too, can be classed according to common traits that may enable an object to respond to risks and opportunities. There are five major attribute classes associated with improved business resilience:

- *Control and comply — the attributes necessary to anticipate, evaluate and control risks associated with complying with industry and government regulations, as well as those risks associated with environmental, social, technical and economic factors*
- *Detect and report — the attributes necessary to detect, estimate, measure and report events to maintain security, privacy and protection of critical data, enabling the business to better respond to any threats that may jeopardize business operations*
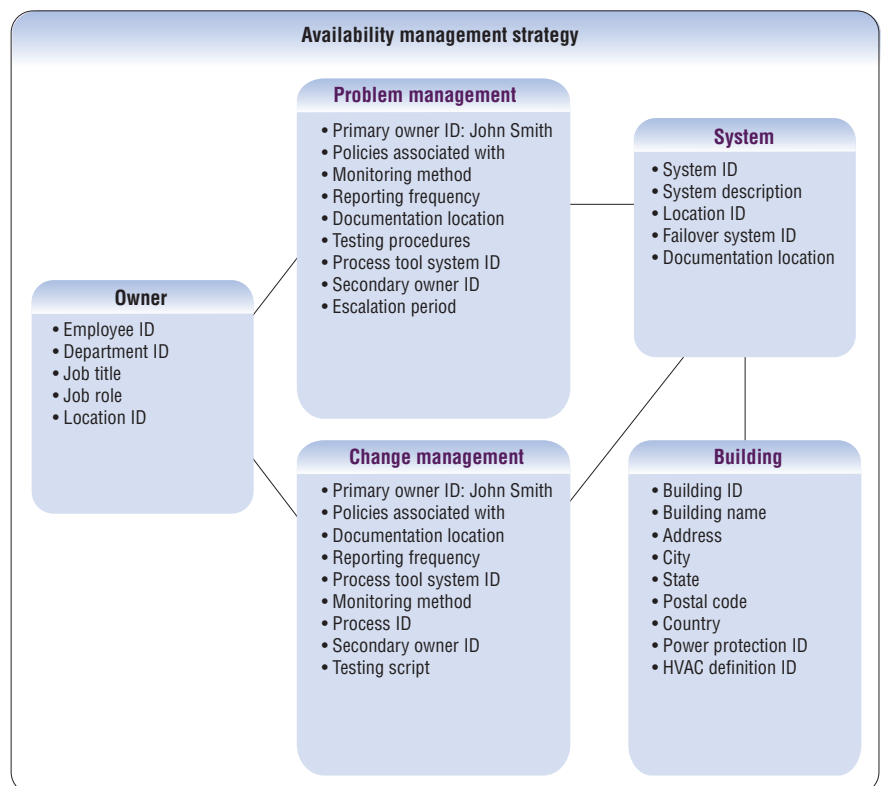
Availability management strategy

Problem management
- Primary owner ID: John Smith
- Policies associated with
- Monitoring method
- Reporting frequency
- Documentation location
- Testing procedures
- Process tool system ID
- Secondary owner ID
- Escalation period

System
- System ID
- System description
- Location ID
- Failover system ID
- Documentation location

Owner
- Employee ID
- Department ID
- Job title
- Job role
- Location ID

Change management
- Primary owner ID: John Smith
- Policies associated with
- Documentation location
- Reporting frequency
- Process tool system ID
- Monitoring method
- Process ID
- Secondary owner ID
- Testing script

Building
- Building ID
- Building name
- Address
- City
- State
- Postal code
- Country
- Power protection ID
- HVAC definition ID

Figure 2.
Using the object-oriented business resilience framework to model your enterprise..

The six object layers expand into more than 140 objects that can be examined for a complete analysis of a company's resilience capabilities.

It's critical to have a roadmap for the process of transforming your business into one that's truly resilient.

- *Deflect and solidify — the attributes necessary to create a solid physical and logical topology to deflect problems and ensure continuity of operations through reliability, redundancy and failover*
- *Adapt and optimize — the attributes necessary to enable adaptable, efficient and flexible integrated risk mitigation strategies, technologies and processes*
- *Protect and preserve — the attributes necessary to help keep the business preserved and protected against accidental and intentional damage, alteration or misuse*

Using these attribute classes as points of reference can help you ensure that each object can address the basic requirements of business resilience. The six object layers expand into more than 140 objects that can be examined through the lens of the five attribute classes for a complete analysis of your resilience capabilities. However, there are two aspects to the process of becoming a resilient business. The first, as discussed, is to gain an understanding of where you are today and where you need to go. The framework was designed to address those questions. The second aspect is more complex. It involves actually transforming your business into one that's truly resilient. This transformation is typically more challenging for companies. Having a concrete roadmap for the process is critical.
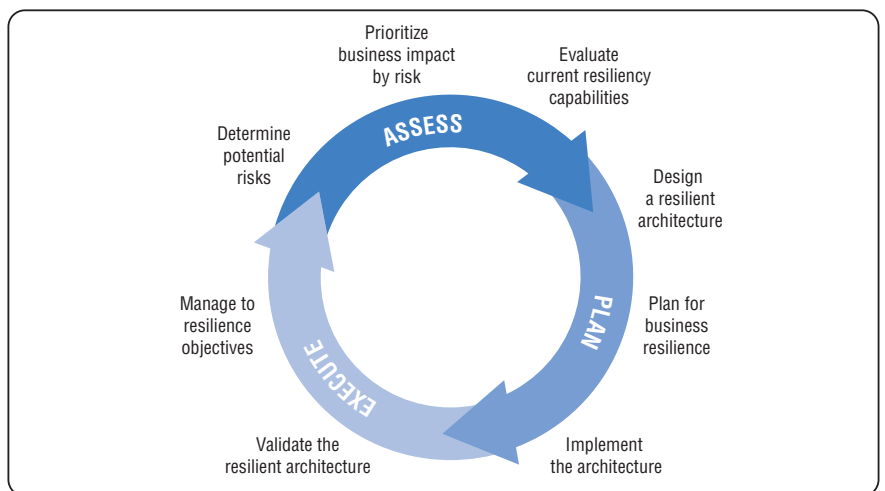

Figure 3.
The business resilience transformation lifecycle moves you through the assess, plan, design, implement and run phases of a typical lifecycle.

*The business resilience transfor-
mation lifecycle is designed to help
you appropriately restructure objects
to help mitigate risk and enhance
your ability to exploit opportunities.*

*Transformation begins with
identifying risks unique to an
organization.*

**The business resilience transformation lifecycle — a roadmap for becoming a
stronger, more responsive business**

Resilience needs are not the same across all industries, or even across compa-
nies within a given industry. As a result, the process of becoming a resilient
business is highly individualized, but the complexity of the task demands a
methodical approach. While the business resilience framework evaluates each
component of your business for its resilience factors, the business resilience
transformation lifecycle actually maps your transformation journey. It's a
step-by-step process designed to help you appropriately restructure all objects
in your enterprise to help mitigate risk and enhance your ability to exploit
opportunities.

Phase one: determine risk exposure

The transformation lifecycle begins when you identify the risks that are unique
to your organization. These may include the risk of natural disasters, and
should also include civil unrest, technical failures, regulatory compliance,
sudden changes in demand, operational requirements and any other risks that
may interrupt normal business activity. As discussed in the previous section of
this paper, it's important to include opportunities in the assessment as well —
such as sudden spikes in transaction volumes, new acquisitions or mergers,
or highly effective marketing campaigns. Companies tend to perform these

types of assessments infrequently, in response to regulatory requirements or other changes to the business model. However, many organizations are now appreciating the value of moving to a more structured, scheduled approach to analyzing their risk profiles in the face of rapid global changes in business conditions. In any risk analysis, the following steps are critical:

- *Rank threats based upon past occurrences, the amount of potential revenue loss, damage to your brand, compliance risks and single points of failure*
- *Prioritize your safeguards*
- *Conduct a cost-benefit analysis if you are performing a quantitative risk assessment*
- *Determine your next steps based upon the severity of the threat, the selected safeguards, and the cost and ease of implementing those safeguards*

The transformation lifecycle next involves ranking risks according to how they will affect business.

Phase two: rank the risks according to potential business impact

The second step is to rank the risks you identified in phase one according to the way in which they will likely affect your business. Identify and prioritize your business services, functions or processes according to how your finances would likely be affected if the risks to these areas were realized. It's important to go beyond a simple business-impact analysis here, which can make every part of the business seem critical, requiring every object to be resilient. Most businesses have just a few truly key functions or processes. You can target your resources more effectively by understanding not only which areas of your business are most important, but also what the exact requirements of those areas

are. In the event of a disruption, how much uptime would you actually need to restore each critical function? The process of analyzing the business impact of the risks your business faces should include the following steps:

- *Identify all critical business functions and processes*
- *Link business processes to the applications and data that support them*
- *Establish appropriate availability and recovery strategies by ranking each process in terms of the length of time it can operate without its supporting infrastructure*
- *Establish appropriate security levels by classifying data by its importance to your business*
- *Identify critical physical recovery resources and vital records, as well as the time frame within which they must be available for recovery efforts*

Enterprises consider business impact with two measures — recovery time objectives and recovery point objectives.

Enterprises typically consider business impact in light of two measurements: recovery time objectives (RTOs) and recovery point objectives (RPOs). An RTO specifies the amount of downtime a business can tolerate. Worldwide, acceptable RTOs are quickly approaching zero. In some industries, such as financial services or credit card processing, downtime can cost millions of U.S. dollars per hour. An RPO specifies the amount of unrecoverable transactions or data that the company can tolerate. It, too, is converging on zero. Many companies have come to see the cost of any downtime as unacceptable; but it is important to analyze that cost if you are to devise a targeted, cost-effective strategy for minimizing or eliminating it.

Phase three: evaluate your resilience capabilities

Once you have created a risk profile for your critical business services, functions or processes, you need to perform a gap analysis of your needs and capabilities. To help you reduce the time and resources you need to complete this assessment and focus on areas that may need a more stringent analysis, it's helpful to break this phase into two steps. The first step entails performing a high-level review of your company's ability to meet the basic requirements of resilience. To revisit them, they include:

- *Maintaining continuous business operations*
- *Achieving regulatory compliance and meeting industry standards more quickly and cost-effectively*
- *Integrating risk strategies to optimize resources*
- *Providing data protection, privacy and security*
- *Obtaining the knowledge and skills necessary to achieve and maintain resilience*
- *Maintaining marketplace readiness.*

***Five maturity levels can be used
to determine how an object
will perform in reference to the
company's risk profile and to
identify potential for improvement.***

Such a review allows you to focus on the areas of most concern. In the second step, IBM can help you use its business resilience framework to delve deeper into these areas. Each of the 140 objects in the framework can be analyzed to determine how it will perform in reference to your company's risk profile and to identify its potential for improvement. Such an analysis can help produce an assessment of each object's maturity level. The following maturity levels can be used to assess an object:

- *Basic — These capabilities range from physical and systems security to awareness programs regarding company policies and emergency procedures, as well as communications, privacy, governance and compliance programs. They may also include comprehensive continuity planning and are the backbone of an ad hoc approach to mitigating risks as they arise.*
- *Managed — These capabilities focus on process and policy compliance and the fundamental automation tools necessary to manage a disruption or opportunity when it occurs. Management plays a strong role here to ensure that employees understand their responsibilities and follow policies.*
- *Proactive Detection — These capabilities are centered on establishing thresholds and advanced warning systems that allow the company to take preemptive actions to help prevent disruption. The ability to monitor current performance and determine out-of-bounds conditions and behaviors for specific components is critical. The company still manually mitigates the risks as they are identified.*

• *Adaptive — These capabilities focus on the organization's ability to sense and respond to unforeseen circumstances by using contingency plans and resources to maintain operations. Responses to situations must be defined in advance, but the system has the ability to adapt automatically to prevent a loss to the business.*

• *Autonomic — These capabilities focus on the business model itself and leverage the innovation, optimization and capacity management characteristics that respond dynamically to changes in the marketplace, which can help you to anticipate and exploit opportunities faster than competitors. The idea is to actively foster business growth through a resilient business and IT infrastructure, rather than merely reacting to threats.*

Phase four: design a resilience strategy

The next step is to incorporate your view of the maturity of your existing objects into a design for a resilient architecture that can help mitigate the identified risks. You can adjust the attributes for any object in order to improve its capabilities and overall maturity level. However, it can be dangerous to undertake this without a comprehensive plan. If you over-engineer your business resilience architecture, you could spend scarce resources increasing the maturity levels of some objects unnecessarily. But under-engineering your architecture could leave your organization at risk — and perhaps worse, leave you with a false sense of security.

The next step incorporates the view of the maturity of existing objects into a design for a resilient architecture that can mitigate the identified risks.

Aligning the objectives of business and IT within the resilience-oriented architecture is necessary for success.

You must determine your desired level of maturity for each object, and then, again, analyze the gaps between your current and desired states. You may find that only a few changes need to be made to your architecture. However, it's important to remember that not all the changes will be IT-related. Some may require business service, function or process adjustments, as well. In fact, a resilience-oriented architecture could easily fail if the needs of business and IT are addressed separately. Aligning the two must be part of the process from the beginning. As a first step, you need to create a conceptual design of the new architecture that aligns business and IT objectives in the following areas:

- *Confirm resilience objectives*
- *Analyze the interdependencies of objects*
- *Develop guidelines and principles*
- *Confirm current configurations on systems, networks, databases, storage and applications*
- *Document and design the solution for the baseline infrastructure*
- *Create a preliminary investment analysis*

After the business and IT sides of your business create and agree to the conceptual design, you then need to create a solution design that can guide them through the following steps:

- *Develop an architecture for business resilience*
- *Define resilience strategies for systems, networks, applications and data*
- *Build the design specifications*
- *Create functional descriptions for the solutions*
- *Define test requirements*
- *Build a roadmap for implementation*
- *Finalize the investment analysis*

Phase five: develop resilience plans and procedures

The architecture provides the structure for improving your business resilience, but you still need plans and procedures for managing and maintaining it. Such a plan should include an initial implementation strategy as well as alternatives that allow for changing business conditions. Each procedure should be defined with respect to:

Managing and maintaining the architecture should include an implementation strategy and alternatives to meet changing business conditions.

- *Its benefits and limitations*
- *The dependencies among business services, functions or processes*
- *The characteristics of the alternative strategies, such as recovery times, acceptable annual minutes or hours of outage, or security level*

- *The high-level cost model for the selected strategy, with recommendations for implementing technologies, processes, tools and staffing—including critical-path items such as technology delivery times, business process reengineering requirements and organizational considerations*
- *A high-level implementation plan that delineates key tasks and milestones for the selected strategy.*

Phase six: implement the plan

With agreement on the implementation plan, it is time to deploy the architecture and structure the resilience program.

Once the implementation plan has been agreed upon, you're ready to deploy your new architecture and structure your ongoing resilience program. The implementation plan must include the following elements:

- *Workload division*
- *Hardware alignment and provisioning*
- *Storage strategy*
- *Replication strategy*
- *Recovery and availability strategy*
- *Network connectivity and capacity measures*
- *Shared services and infrastructure components for base operational capabilities*

- *Virtualization alternatives*
- *Systems management mechanisms*
- *Command and control mechanisms*
- *Testing capabilities*
- *Physical and logical security features*

Phase seven: validate the plans, procedures and architecture

Validating work completed in the transformation process can help confirm that all aspects of the resilience architecture have been implemented properly.

The next step in becoming a more resilient business is to validate the work you have completed in the transformation process. The validation exercise helps confirm that all aspects of your business resilience architecture have been implemented properly and are working effectively to mitigate the risks you identified earlier in the process. Any validation has three parts:

- *Develop a resilience exercise for the architecture*
  - *Verify the resilience requirements, objectives, scope and timelines*
  - *Identify the resource requirements and planning tasks*
  - *Review the processes and procedures and assess the capability of each to perform the resilience exercise*
- *Review the technical resilience procedures*
  - *Review the resilience procedures and record your feedback*
- *Execute the resilience exercise*
  - *Provide audit and exercise observations with documented results*
  - *Execute the resilience exercise, including the technical recovery procedures*
  - *Provide ongoing semiannual audits of resilience plans with documentation of actions to be taken*

Phase eight: ongoing management of your resilience program

It's important to remember that a resilience exercise is not a static event, but is, instead, part of a concerted management program designed to help maintain continual monitoring, testing and improvement of the infrastructure. A defined business resilience program should be managed so that everyone involved understands and adheres to the resilience principles that underlie the architecture. That architecture ultimately must allow for the following:

- *Overall management of a total enterprise-wide business resilience program*
- *Communication of program results to the management team*
- *A linkage between business executives and IT-related resources*
- *Thought leadership for future availability, continuity and security initiatives*
- *A blueprint for the establishment and execution of a governance process*
- *Coordination and direction of continuity-related staff among entities, such as your IT organization, consultants and outsourcing providers, or partners*
- *Ownership and direction of all aspects of disaster recovery exercises*
- *Management of the financial plan, with assigned responsibility for the costs of the program*
- *Coordination of third-party relationships that satisfy the needs of the continuity program*

Highlights

The ultimate goal is a comprehensive but targeted program that is designed to address your unique needs and goals for resilience.

- *Annual review sessions to ensure alignment between business and IT objectives*
- *Qualification of new projects and engagement of solution design and delivery*
- *Communication of strategies, directions and requirements to all relevant employees*
- *Definition of a single point of contact to manage resolution of resilience issues*
- *A change management process to incorporate business and infrastructure changes into the resilience strategy and plan*

In the end, you'll have a comprehensive, but carefully targeted, resilience program that is designed to address your company's unique needs and goals. With a well-designed architecture based on an object-oriented framework and a roadmap, you'll know where you need to go and why. You'll also better understand how to avoid unnecessary expenditures of time and resources.

Why IBM?

The IBM business resilience framework and the IBM business resilience transformation lifecycle are part of a family of IBM offerings designed to help you make your business stronger and more resilient in the marketplace. Drawing on IBM's long-standing systems integration capabilities and best practices, IBM Business Continuity and Recovery Services offerings run the gamut from business and technology consulting services to technical solutions for implementation, and ongoing management of your business resilience program. Our customized solutions can help you at any stage of the process. IBM can apply its unmatched global resources and broad business and technology expertise to your unique business needs.

For more information

To learn more about IBM's business resilience programs and offerings, contact your IBM sales representative, or visit:

ibm.com/services/its/resilience