Overview

Today, organizations face a litany of disruptive threats in the modern business world. Managing Business Resiliency (BR) requires more than business continuity planning, but rather a mixture of building resilient business processes, IT systems and controls, and employing skilled, informed people to ensure the business can not only continue but thrive. The RSA Archer Maturity Model for Business Resiliency outlines RSA Archer’s role in the critical stages in a company’s journey from reactive, compliance-driven business recovery to risk-centric, resilient planning and execution.

Contents

Why Business Resiliency? .......................................................................................................................................................... 3
Key Capabilities........................................................................................................................................................................ 4
The Maturity Journey.............................................................................................................................................................. 5
Maturity Model Crossover ......................................................................................................................................................... 10
Conclusion............................................................................................................................................................................... 10
About the RSA Archer Maturity Model Series....................................................................................................................... 10
Why business resiliency?

Companies have traditionally battled the challenge of business recovery by trying to get business process owners to document and test their business continuity plans to ensure disrupted processes can be recovered after a disruption. An added challenge is the business’ reliance on IT systems, which, if disrupted, must be recovered for the business to continue to operate. However, the business and IT often have different priorities and recovery time objectives, making coordinated recovery ineffective, if not impossible.

Business continuity (BC) planning and IT disaster recovery (IT DR) planning are absolutely necessary because without them, the company would be vulnerable to the smallest disruption. Providing the fundamental defense before, during and after disruptions, this planning, testing and execution is critical in reacting to many events, from natural disasters to man-made (e.g., labor strikes, pandemic) disruptions and others. However, statistics show many organizations that face a major disruption struggle to recover their business afterwards, and often do not resume pre-disruption levels of operations for months or years, if ever. Why is this the case?

- BC planning cannot keep pace with changes (people, processes, places and partners) in the business or IT. Organizations are getting more and more complex from a business process and technological perspective, making recovery much more complex as well. BC plans are not updated or tested very often, and coupling this with lots of changes makes successful recovery a long shot.

- BC planning is complex and expensive. From efforts to evaluate process criticalities, to replicating business functions in other formats and locations, to documenting and testing plans to putting in place recovery strategies, the organization must choose to invest in these activities and perform them well.

- Business processes and IT systems often change organically over time due to such factors as increasing volumes, integrations, or increasing regulatory requirements. As this change occurs, processes and technologies typically are not updated to efficiently handle the impacts. They become more complex and fragile because they are not designed to be resilient.

- BC planning has not historically been a high priority for executives unless the business model (e.g., airlines, utilities), location (e.g. earthquake zone) or regulators require it, or a disruptive event has occurred that brings the need front and center.

- Organizations fail to track and analyze operational events that happen every day, with little or no visibility into the symptomatic issues, or frequency or magnitude of the risk exposure.

- Organizations worsen events simply by not being prepared to manage the crisis. Mishandling of a crisis can lead to additional impacts, and, in some cases, such as slow response or confusion about recovery roles, can make a crisis worse, harm employees, drive up costs and further harm the company’s reputation.
Organizations must shift from just performing BC planning to become resilient. While BC planning is inherently reactive - developing plans to deal with or recover from a disruption, or recovering disrupted IT systems, Business Resiliency (BR) is proactive - developing resilient business processes, operations, IT systems and other aspects so the organization “bends but does not break,” so to speak. BR includes developing resilient practices, partnerships, people and assets.

Key capabilities

Most companies still regard BR in the reactive recovery mode. However, companies that can identify opportunities to build resiliency into their processes and complement effective recovery efforts can use this as a competitive advantage simply by improving business processes and systems, and reducing recovery efforts and costs. With more hardened and efficient processes and technologies in place, the business has additional investment and a safety net to pursue and exploit new opportunities, such as adopting new technologies, expanding into other markets, working with new partners or launching new products and services.

When an executive steering committee considers establishing a BR program, the committee requires many operational groups to collaborate and coordinate efforts.

- Legal, human resources, security, facilities, finance, BCM, crisis teams, business operations, IT, compliance and others must be represented.
- Compliance can be adversely impacted by a disruption, so efforts must ensure the proper controls are designed and operating effectively. This includes knowing what BC planning-related compliance obligations exist, what the current compliance posture is, and how compliance is going to be affected during and after a disruptive event.
- BR-related policies must also be aligned to other regulatory and business requirements.
- Business process improvement initiatives should focus on building resilient strategies, steps and controls into business and IT processes. Strategies must be built to look beyond the immediate and tactical and bring innovative and cost-effective resilient solutions to bear.
- Operational incidents from security, physical security, ethics and other processes should be cataloged and examined to identify systemic issues, risk exposures or common potential areas that could lead to disruptions or crises.
- IT must ensure DR strategies achieve recovery time objectives agreed upon with the business.

To achieve these goals, the RSA Archer BR solution focuses on the following key capabilities:

RSA Archer GRC
Maturity Models focus on key capabilities enabled by the RSA Archer solution. As a technology enabler, RSA Archer provides the critical infrastructure to leverage processes, share data and establish common taxonomies and methodologies.
Establish business context for resiliency — Enabling the BR function to understand the business and IT assets, relationships and criticality, establish ownership and accountability and lay the foundation for planning.

Prepare for and recover from system outages — Supporting processes to strengthen the IT infrastructure, as well as document and test IT DR plans and strategies in advance of a technology disruption.

Identify and prepare BR strategies — Supporting processes to document and test business continuity plans and strategies in advance of a business disruption.

Catalog and resolve incidents — Supporting an end-to-end solution to deal with day-to-day incidents, including security events, physical incidents and data breaches that could lead to disruptions.

Manage crisis events and communications — Supporting a solution to manage crisis events and communications and coordinate the activation of BC and IT DR plans.

The maturity journey

RSA Archer Maturity Models are segmented into five major stages: Siloed, Transition, Managed, Transform and Advantaged.

The maturity models are designed to be pragmatic and readily implemented. Elimination of the “Level 0” that typical Maturity Models include avoids the unnecessary definition of a stage of maturity that will not meet today’s BR challenges.

- **The Siloed stage** focuses on baseline activities that all organizations need to manage recovery.
- **The Managed stage** is for organizations that have reached a coordinated, sustainable BC program that is integrated between IT and the business.
- **The Transition stage** and **Transform stage** help the organization “turn the corner” with initiatives that begin to develop resilient capabilities and set the stage for advanced capabilities.
- **The Advantaged stage** is designed to be achievable for most organizations. It is an advanced stage of maturity that optimizes BR across the organization while still leveraging BC and IT DR.

The RSA Archer Maturity Model for BR focuses on building the capabilities outlined over time and implementing the broad strategy with tactical, intelligently designed processes.
Foundations

Foundations are critical elements necessary for the overall success of the BR Maturity Journey. Without these foundations in place, the organization will face difficulties throughout the journey either through the lack of focus, commitment, resources or strategy.

- **Management commitment** – The degree and level of leadership commitment to BR culture, strategy and priorities
- **Performance and acceptable risk** – Defined levels of performance and acceptable risk for BR
- **Expectations and measurement** – Clear expectations and success criteria defined for the BR program
- **Stakeholder involvement** – Importance of improvement and maturity of BR processes to your stakeholders and business constituents
- **Budget and resources** – Sufficient resources for the BR program to achieve success

The siloed stage: Laying the foundation

Companies in the Siloed stage of the Maturity Model for BR have a basic understanding of the business and IT infrastructure, but because they are not well-connected, recovery plans are basic and BC is very separate from IT DR. For example, there is a basic understanding of business processes and technology assets that need to be recovered in the event of disruption, but any tracking records are separate and disconnected. Records for IT infrastructure are kept for IT DR planning and records of business processes and assets are kept for BC planning. There may be a common record of employees and other business contacts, such as an HR system, which allows these resources to be aligned to recovery plans and tasks.

BC planning and IT DR planning are separate and based on unrelated business impact analyses (BIA) and recovery objectives. The organization orients BC planning around major business processes based on high level BIA data, which typically is not updated often enough. IT DR plans are basic and immature and usually limited to high-level recovery strategies, tasks and basic requirements for the most critical systems and infrastructure. BC plans are documented for highly visible processes or those that management intuitively knows are most important. Call trees are documented and associated with separate DR and BC plans.

Usually, a simple process for declaring a crisis event has been implemented, although operational events and incidents are reported and recorded through separate processes. Details and analysis of incidents are documented at a basic or high level, and investigations are tracked and managed in an ad hoc fashion.
The transition stage: Building context for the future

In order to move to the Transition stage, organizations must record their business and IT assets and perform BIAs and risk assessments. They must also start to test their plans at a high level and track findings. Finally, incident management must be established to manage operational events.

When an organization is in the Transition stage, the BC organization performs more detailed BIAs to identify criticality thresholds related to business units and operational risks of the organization. Catalogs for key IT assets, including applications and devices, are established and IT asset dependencies and relationships are mapped.

IT DR plan testing is performed with basic test scenarios, usually through plan walkthroughs. Tests begin to be scheduled on a regular basis and testing results are tracked, but follow-up is not strong. DR plans are usually tested alone or in tandem with related plans on a location-by-location basis.

BC plan testing is implemented using basic test scenarios. Tests are scheduled on an ad hoc to regular basis and testing results are tracked. Major business processes or facilities are targeted for testing.

Incident management matures, with incidents broken out and defined separately based on segments of operations, processes or incident type. With this categorization of incident types, reporting is improved and analysis of systemic issues can be conducted. A process to report ethics violations is established, with steps to ensure confidentiality for whistleblowers.

Testing of crisis management processes is executed during BC or DR testing based on basic crisis event types. Call trees are better defined for emergency notifications.

RSA Archer Maturity Model: Business Resiliency

BC plan testing is implemented using basic test scenarios. Tests are scheduled on an ad hoc to regular basis and testing results are tracked. Major business processes or facilities are targeted for testing.

Incident management matures, with incidents broken out and defined separately based on segments of operations, processes or incident type. With this categorization of incident types, reporting is improved and analysis of systemic issues can be conducted. A process to report ethics violations is established, with steps to ensure confidentiality for whistleblowers.

Testing of crisis management processes is executed during BC or DR testing based on basic crisis event types. Call trees are better defined for emergency notifications.
The managed stage: Operationally sound

In the Managed stage, the organization plans for a wider variety of disruptions based on a more comprehensive understanding of business and IT assets. BC plans then become more extensive and are documented for all process criticalities and combinations. Plan testing is more extensive with the tracking and testing of results and remediation of issues. Operational incident management continues to mature in its workflow, documentation, investigations and resolution. Finally, crisis management becomes a part of the overall strategy with established processes and roles and responsibilities. Communication improves through the use of emergency notification mechanisms or tools.

The organization’s business asset catalog is enhanced with more detailed conceptual topics, like key information assets (e.g., types/locations) and the IT asset catalog includes additional asset categories, like storage devices. Attributes (e.g., owners, managers, business usage, etc.) have been established for these business assets, enabling the organization to take a business information-centric view of BC/DR requirements.

Combinations of assets, such as applications, devices and locations, are documented in related DR plans, as opposed to separate plans for each asset. With the addition of relationships between IT assets and information assets, IT DR plans can be enhanced with more coordinated and detailed recovery requirements.

BC plans are more extensive and documented for each process (all criticalities) or combination of processes, with strategies for supporting infrastructure or linkages to other infrastructure plans.

Plan testing is more extensive, including regularly scheduled tests with varying scenarios that include activating plans and tracking testing results and status. Issues and gaps that arise from not achieving plan objectives during BC and DR tests are documented, and remediation of issues resulting from testing or actual events are recorded and tracked.

Operational incidents are categorized and assigned resources based on the type and criticality of incident. Documentation of incident results and tracking of time spent to resolve the incident are added to the process to monitor the efficiency and effectiveness of response efforts. Broader investigations that may involve multiple incidents or require evidence collection are tracked and managed. Issues and gaps arising from operational processes and events are documented. Remediation efforts for gaps are tracked and reported at regular intervals.

A central crisis team is established, and roles and responsibilities are documented and assigned to appropriate personnel in the event of a crisis. Emergency notification mechanisms are implemented to communicate to involved personnel. This includes definition of emergency communications to be sent to various participants based on crisis events and the ability to deliver communications in the event of a crisis.
The transform stage: Relationships and dependencies

In the Transform stage, companies truly begin to transform to a resilient organization by connecting end customer-facing products and services to internal processes and IT infrastructure. These relationships enable a common BIA process to be established which is being consistently executed for coordinated BC and IT DR planning. Management can then identify upstream and downstream dependencies between BC and related DR plans documenting appropriate connections between plans and supporting exhibits. As these relationships are understood, resiliency risks are regularly identified and evaluated; mitigated through controls and BC/IT DR strategies; and correlated to prior and potential operational incidents and crisis events. Incidents are more proactively managed by defining types (i.e., ethics violations), ownership, standard response procedures and management review.

The business asset catalog has been extended to account for broader and more complex organizational areas like products and services, connecting end customer-facing products to internal processes, and IT infrastructure. The business hierarchy (organizational structure) has been mapped into the business asset and IT asset catalogs. Additionally, a mapping between IT assets and business assets is better managed. Relationships between IT and business assets allow a common BIA process to be established, which is consistently executed for coordinated BC and DR planning.

Management has identified upstream and downstream dependencies between BC and related DR plans, and documented the interdependencies in the plans and supporting exhibits. There is a greater understanding of these relationships, which enhances recovery documentation and effectiveness. Risks to resilience are documented in the BCM risk register and cross-referenced to controls, BC plans and actual or potential crisis events.

Exceptions resulting from issues detected with BC and DR testing are better recorded, reviewed and tracked.

Standard response procedures are better defined by incident type. For example, follow-up by a compliance manager on cases to validate claims of ethics violations and determine the best course of action is enabled. In addition, exceptions resulting from operational events are documented and tracked. A process to connect crisis management to key organizational assets and initiate associated BC or DR plans in the event of a crisis is established.

The advantaged stage: Optimized for risk management

Companies reach the Advantaged stage by altering their approach from simple business recovery to innovative resiliency. Organizations in this stage develop resilient strategies and operational processes to operate fluidly and adapt quickly to threats and disruptions which allows them to continue on their strategic path, beat competitors to market, launch new products and services with calculated efficiencies, and avoid major issues that affect operations, reputation and the bottom line.
With a common BIA process in place, business and IT criticalities and RTOs are coordinated across business processes and associated upstream and downstream dependencies, including key systems and infrastructure. Business context has been infused into all BC and DR processes and technologies. Issues are reported at macro and micro levels with integrated business attributes and impact.

Management conducts full joint BC and DR tests and follows up on issues. Risks are assessed on a periodic basis to evaluate and plan for any changes in risk levels and any necessary plan updates based on those changes. Any policy and process changes needed based on issues uncovered during BC/DR events and tests are documented and assigned ownership.

A common framework for working all operational incidents is established to address a wide range of events such as theft, harassment, fraud, violence, bribery, corruption, equal opportunity violations, conflicts of interest, phishing or denial-of-service attacks. Incident and response procedures are documented in a centralized, reusable repository that allows for visibility across operational events. Incident responders are trained on triage and response procedures. Policy and process changes needed as a result of issues arising from operational events are documented and tracked.

Crisis management is fully integrated with BC and IT DR efforts, including coordination between internal and external parties (outsourcers, service providers, etc.). BC and IT DR plans are initiated in coordination with crisis management processes. BC/DR plan owners and constituents are communicated with regularly regarding crisis management practices.

**Maturity Model crossover**

Business Resiliency is a critical consideration for all companies and a major component of an overall operational risk management program. BR is cited by executives as one of the fastest growing areas of risk today. As the last line of defense when disruption affects a business, BR deserves a significant place in an organization’s strategic portfolio of risk management and should be factored into the operational risk program.

Another reason for BR risk management is the growing reliance on outside providers within business processes. As such, third party governance must be tackled as part of BR management, given that many organizations provide external parties with access to internal systems or rely on third parties for critical business operations.

Finally, BR is a critical component of today’s regulatory and corporate compliance environment. The inability to prove that business processes, IT systems or critical information can be recovered following a disruption can lead to significant regulatory fines, reputational damage and compliance issues.
Conclusion
A BR approach is necessary for an organization to mature from reactive business continuity to a proactive posture that enables them to reduce the effects of disruptions on their business. BR brings together groups with separate, yet with common objectives, such as protecting critical business areas, managing third parties, or risk assessment and mitigation. BR is a discipline that can also streamline organizations, reduce costs and strengthen operations.

About the RSA Archer Maturity Model series
RSA Archer’s vision is to help organizations transform compliance, manage risk and exploit opportunity with Risk Intelligence made possible via an integrated, coordinated GRC program. The RSA Archer Maturity Model series of white papers outlines multiple segments of risk management that organizations must address to transform their GRC programs.

About RSA
RSA, a leader in cybersecurity and risk management solutions, provides organizations with technology to address challenges across security, risk management and fraud prevention in the digital era. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce operational risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.