



Business Continuity Management

A commissioned point-of-view on behalf of Deloitte & Touche LLP and RSA
Conducted May 2011



The Business Continuity Challenge

The complexity of business continuity management (BCM) and disaster recovery programs (DRP) grows with the adoption of new technologies, rapid business change, and expansion of strategic partnerships and vendor management. Recovery time (RTO) and recovery point objectives (RPO)¹ continue to shrink with the adoption of virtualization technologies. Simultaneously, BCM and DRP are resource constrained, irrespective of the growing awareness of the threats posed by well-publicized calamities. Maintaining business continuity and resiliency is more challenging than ever and calls for a new strategic view.

BCM / DRP's value proposition is rarely voiced outside of a well-publicized natural disaster, e.g., the Japanese earthquake / tsunami. Only then does enterprise attention turn to updating and testing BCM/DRP plans while compliance mandates expand to include new conditions. However, after a time these efforts lose energy, resourcing, and priority. As a result BCM / DRP preparedness tends to deteriorate between highly visible disasters.

Business continuity is enterprise-wide in nature, but implemented along organizational lines. Planning, testing, and implementing follow enterprise guidelines, but in practice, deployment and results may diverge significantly by organizational unit. In an emergency, crisis management at an enterprise level is often hindered by the lack of consistency from standalone organizational initiatives.

Synchronizing BCM efforts and results across the enterprise and in an effective manner calls for a rethinking of the strategy. Many enterprises can strategically reframe their BCM practice and strengthen their risk framework by leveraging the convergence model. Essential elements to address this challenge are:

- Enhance delivery quality,
- Focus on visible, measurable results,
- Deliver proactive management tools,
- Achieve repeatability and responsiveness at lower cost, and
- Combine BCM / DRP, strategically, with high-visibility initiatives in the enterprise.

Many enterprises face the question of “Can we leverage what we have?” Outlined in this point-of-view is an example of an approach that addresses this challenge and leverages the convergence model.

The Convergence Model

An organization-oriented (i.e., silo-oriented) BCM / DRP approach tends to ingrain inconsistencies of practice across the enterprise. For example, one organization tests data

recovery while another tests fail-over. Neither organization conducts these exercises at the same level; the results are inconsistent. While an organization's test results may address a compliance mandate, they may not mitigate the risk outlined by the mandate.

As adoption of virtualization accelerates, inconsistencies can be glaring in a recovery scenario. If unaddressed, these inconsistencies can perpetuate and lead to out-of-date BCM / DRP recovery practices. In many cases, outdated BCM / DRP plans make crisis management difficult, lengthen recovery time, and raise questions about compliance with enterprise policy and regulatory mandates.

The convergence model has demonstrated its value in shaping dissimilar systems to bring order to seemingly unrelated issues. Under Deloitte's² direction, the convergence model uses enterprise governance, risk and compliance (eGRC) technology and methodologies to re-shape the risk management framework by integrating:

- RSA Archer eGRC technology,
- Deloitte's risk assessment and deployment practice methodologies, and
- Client-oriented consultative process (including technology, methodology and collaboration).

As a tool, eGRC's perspective provides information that enhances decision-making, anticipates issues arising, and encourages collaboration.

Deloitte tailors state-of-the-art technologies, assessment methodologies, and its time-tested collaborative processes to address an enterprise's unique requirements in the following manner:

Technology

Applications bring the business to the technology. RSA Archer Business Continuity Management (RABCM) is the platform that allows clients to

- Adapt solutions to your requirements,
- Build supporting applications, and
- Integrate with other systems without touching a single line of code.

Aligning with standards, e.g., National Institute of Standards and Technology (NIST) Contingency Planning Guide for Information Technology Systems³, offers a view of an enterprise's compliance posture. RABCM can provide a rapid return-on-investment (ROI) from a solution that can be implemented out-of-the-box or tailored through code-free configuration.

¹ Recovery Time Objective (RTO): maximum acceptable time for restoring a network or application & regaining data access after an unplanned disruption.

Recovery point objective (RPO): maximum acceptable data loss (elapsed time since the most recent reliable backup) after an unplanned disruption.

² As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

³ NIST Special Publication 800-34, Rev.1. May 2010.

Adding other RSA Archer solutions, e.g., Compliance, Risk or Policy Management, extends the governance and compliance structure beyond BCM and gives greater value-add. More complete and concise reporting across the enterprise hierarchy is the strength of Archer's robust issue tracking and reporting capability. Easy to develop on-demand reporting and dashboards give the capability to drill-down into specific areas (i.e., to view underlying data) and provide visibility across the enterprise.

Methodology

Because Archer technology deploys quickly, Deloitte's methodology gives actionable results and addresses changing business objectives early in project deployment. Deloitte's time-tested Risk Assessment Methodology provides a consistent approach for:

1. Conducting an assessment,
2. Identifying and prioritizing risk components,
3. Tailoring the technology against the assessment,
4. Deploying the technology,
5. Evaluating outcomes, and
6. Refining against results.

Using the RSA Archer eGRC core suite of tools to highlight risk-relevant relationships, Deloitte's convergent vision of eGRC overlays client requirements and improves the governance process.

Process

Deloitte's consultative approach engages the client, technology and methodology iteratively to adapt enterprise processes to a risk-based approach. RSA Archer eGRC offers out-of-the-box templates that help expedite project start by giving early functional alignment, budget optimization, and risk awareness. Frequently, the process reveals deficiencies that demonstrate eGRC's value almost immediately.

The convergence model becomes a vehicle that improves an enterprise's understanding of risk and its BCM / DRP governance capability. The model is easily replicated and allows new business function to be added incrementally. The working approach that follows demonstrates its practical use for a major financial services organization across major functions.

The Working Approach

Interest in BCM / DRP, traditionally triggered by a catastrophic event, is on the radar now with the adoption of virtualization. Improved and responsive BCM / DRP are virtualization's unintended consequence. Virtualization provides a powerful capability for transitioning from recovery-centric to resiliency-centric operations.

Because applications running in a virtual environment can move, seamlessly and transparently, the BCM model is transformed from routine, manual processes to responsive, automated processes.

Virtualized BCM / DRP can be exercised at any time: a 24/7/365 capability. Operational impacts are minimal. Results from the exercise are known immediately and adjustments made as necessary. As part of the operational flow, BCM / DRP is a given rather than an exception driven event.

Under 20% of disaster recovery customers also employ a BCM approach. As awareness of the uninterrupted availability through virtualization and cloud computing grows, so does BCM's value. Several financial services firms relied on Deloitte to develop a recovery assessment based on their DRPs. They asked Deloitte to conduct risk assessment reviews of current recovery scenarios, identify gaps in recovery, and outline "future" scenarios that shortened recovery times. Lastly, they asked for remediation cost estimates to refine the future state.

Benefits from these efforts included:

- Bringing remediation costs to practical levels,
- Rapidly deployment using out-of-the-box configurations,
- Consolidating sources and solutions to produce actionable results, and
- Rationalizing regulatory mandates into a single set of controls across the enterprise.

Given assessment results and realistic remediation costs, Deloitte was asked to leverage clients' existing deployments in support of BCM by adding the RABCM solution. By applying advanced BCM / DRP practices, such as standardizing virtual machine offerings, Deloitte tailored the model to help management address their requirements and helped to bring alignment, capability and enhanced risk management to these client environments.

Alignment

Before the engagements, BCM / DRP were largely viewed as a redundant task that required repetitive, non-essential testing. As a result, the results were largely ignored. Because results were viewed as routine, they were only accorded priority during the audit cycle. Audits were seen as a time of intense activity to meet the control point, and unless there was a negative finding, no further BCM / DRP effort was expended.

After the engagements, BCM / DRP awareness in the business units increased without a corresponding increase in workload. By using virtual machine migration capabilities, BCM / DRP capabilities have been exercised on a consistent basis. By displaying key performance indicators (KPIs) in the BCM / DRP dashboard, management is more aware of compliance status and the health of existing programs.

Capability

RSA Archer eGRC reporting and dashboards (summarized KPI views) were tailored to include control and compliance categories. The initial deployment relied on standard templates of risks and controls in the BCM / DRP solution. Display of control and compliance KPI status was used to correct impending issues.

Perhaps the most important aspect of RSA Archer eGRC is its enablement of enterprise communication through workflow technology. Leveraging workflow, issue tracking, reporting and resolution provided immediate and clear, concise reporting to the Audit Committees and the business management hierarchy and were particularly useful under crisis conditions.

Risk Management

Deloitte's tailored Risk Assessment Methodology accelerated deployment and leveraged RSA Archer eGRC risk and control libraries. Several outstanding recovery conditions were highlighted during the deployment cycle and action was taken to address them.

Removing redundancy and repetitive work allows the BCM / DRP group to adopt a consultative and strategic role. Members of the group are viewed as collaborators that integrate the BCM / DRP into daily processing.

Indicative Costs

Project deployment costs may be offset by savings. For instance, external audit fees associated with BCM / DRP may decline based on results from the RSA Archer eGRC solution. This is because reliance can allow external audit efforts to focus on areas requiring more attention, as compliance with mandates were now easy to track, view, and manage.

Internally, routine BCM / DRP, such as testing, were done transparently and without intervention. The repositories for data gathering encourage the "capture once, use many" approach. Tracking of non-compliance issues, timely remediation, and visibility within the controls hierarchy reduces overall risk by improving response time to issues arising and providing data for effective crisis management.

Demonstrable real-time BCM / DRP compliance may reduce risk of outage as well as reduce the work effort of the external and internal audit groups. Costs may decline and reliability increase. The intangible benefits from improved BCM and DRP are seen through the immediate response and correction of KPI lapses and the move toward a resiliency-centric operation.

The Author

Charles King, CISSP, PMP

Managing Partner
charles.king@kinginfosecurity.com
+1 415 999 4522
www.kinginfosecurity.com

Contacts

To discuss your business challenges and solutions, contact a Deloitte or RSA professional below.

Sean Peasley

Principal
Deloitte & Touche LLP
+1 714 436 7410
speasley@deloitte.com

Kim Altern

Senior Manager
Deloitte Services LP
+1 212 436 3634
kaltern@deloitte.com

Rick Hedeman

Alliance Manager
RSA, The Security Division of EMC²
+1 781 515 5332
rhedeman@rsa.com

Scott Cogan

Strategic Alliances
RSA, The Security Division of EMC²
+1 703 864 1613
scott.cogan@rsa.com