A Strategic Framework for IT Disaster Recovery Assessments

Today’s data centers are extremely complex systems, consisting of thousands or tens of thousands of servers, racks, switches and other equipment, all of which have intricate interdependencies. Moreover, due to the rising frequency and severity of disasters and the high value of data and processes hosted, data centers are required to provide disaster recovery capabilities. To ensure and improve the quality of these capabilities, it is common to conduct disaster recovery (DR) assessments.

In practice, assessing the DR programs of modern data centers is a challenging task. Given the complexity of the data centers and the interdependencies among systems, it is easy to get mired in the details. When the concepts of cloud computing, globalization and virtualization are added, it can become almost unmanageable.

This article presents a practice-tested framework that structures and prioritizes the assessment of DR programs, testing the most business-critical aspects first. This article specifically shows where DR failures and shortcomings are most common or severe. Depending on the scope and budget of a specific assessment, the framework offers an incremental path for adding as much depth and detail as needed. As data center operations are increasingly outsourced, dealing with the client-provider relationship during assessments is also covered.

This article offers guidance to IT executives that enables them to better focus and guide DR assessments. Auditors in charge of conducting assessments will benefit from the proposed framework to structure and prioritize their work.

**ASSESSMENT FRAMEWORK**

DR is a management as well as a technical discipline. Further, management is overseen and controlled by a governance function. The success of a DR program, therefore, depends on all three areas—governance, management and technical operations—working effectively by themselves and in combination. Accordingly, any assessment of a DR program also has to assess all three layers. In doing so, it is important to start with governance (see figure 1) and work down toward assessing the technical and operational aspects. The reason for this prioritization scheme is that a DR program with strong governance tends to be resilient—in the sense that it continuously
finds and eliminates weaknesses in the lower layers. Conversely, even when management or technical operations are designed effectively at the time of the assessment, they tend to degrade over time and become dysfunctional when governance is weak. It is for these reasons that any assessment should start with governance first and proceed from the top down.

The assessment objective is different for each layer of the DR program:

- **DR governance and executive oversight**—In assessing the governance function, the focus is on evaluating the extent to which executive management defines clear and sound goals, policies, procedures, organizational structures with communication and escalation paths, and metrics that enable management to do the right things and do them efficiently.

- **Management**—When assessing management, the extent to which it follows the governance framework defined by executive management and how well it performs its work are evaluated. Typical management work includes choosing DR technologies, tiering applications (i.e., the ranking of applications based on their business criticality and recovery priority), DR planning and DR exercising. As governance bodies do not specify the operational details of these tasks, it is important to assess them relative to good practice norms.

- **Technical operations**—In assessing operations, whether the IT infrastructure is built, configured and managed in accordance with management’s directive is evaluated.

The three tiers in figure 1 are sometimes referred to as “governance, process and technology” or “policy, people and process, and technology,” with some variations in semantics. The terminology as defined here is, however, more descriptive for the purpose of this article and will, therefore, be used throughout this text.

**Assessing Disaster Recovery Governance**

Governance sets the strategy of what DR activities to undertake and, to a lesser degree, how to carry them out. To address the what-related questions, governance bodies use business impact analysis (BIA), which is generally prepared by the business, to determine the criticality of DR for business success and future growth. The DR vision, objectives and budget are accordingly derived based on how important the availability and recovery of IT systems are to the business. The vision and objectives drive the DR methods to which the organization adheres (i.e., the how of governance).

When defining the how, governance bodies do not spell out operational details of disaster recovery, but rather define guiding principles and rules that management must follow, including roles, responsibilities, decision rights and processes, and standards or professional practices such as those from the Business Continuity Institute4 (BCI) or the Disaster Recovery Institute International5 (DRII). Governance bodies must further specify the metrics and reports used to measure management’s performance in executing the DR vision and objectives.

When assessing DR governance, the following areas, which are particularly frequent problem areas, are a good start:

- An element of governance that often gets overlooked is budget. A sufficient capital and operating budget must be in place to help the organization implement and maintain an appropriate level of recoverability.
- Governance bodies must have strong executive representation from across the organization so they can shape how management works. They further need processes to formally approve decisions and to oversee their implementation.
- It is important to check for governance gaps in which entire areas of management are left without guidance or control. For example, when governance does not take a position on DR testing, DR training, DR plan activation or continuous improvement, or when there are misunderstandings and disagreements on roles and responsibilities, these gaps need to be addressed. Conversely, governance bodies overstep their mandate and infringe on management when they troubleshoot
individual incidents. Rather, governance bodies must look for the root causes of such incidents and decide if roles, decision rights or other management structures need adjustment.

Assessing Management
While governance defines the general rules and principles of DR, management is responsible for implementing and operating an effective DR program. This is arguably the most challenging aspect of DR. The core processes that management has to execute are:

• Enabling DR recovery for applications in order to guarantee the achievement of the recovery time and recovery point objectives defined by the business
• Maintaining compliance with applicable laws and regulations
• Defining a DR strategy that specifies the technologies and mechanisms used to recover data, applications, network connectivity, telecommunications, equipment and DR sites in the event of a disaster
• Refining the DR strategy into a step-by-step DR plan
• Implementing and maintaining the DR plan
• Periodically exercising the DR strategy and plan to test their effectiveness
• Educating people throughout the IT organization to ensure that they understand their roles and have the training to fulfill their responsibilities in the event of a disaster

When assessing DR management, these processes must be completed according to the mandate given by governance and in compliance with industry good practice. More detailed guidance on assessing any management processes can be found elsewhere. To focus DR assessments, one should start with the following processes when shortcomings are particularly common or severe:

1. Omissions in the DR plan are a common problem. Templates and checklists can help identify such gaps with respect to, for example, the recovery team organization, emergency contacts, activation procedures, tiering of applications, source-to-backup mapping, application dependencies, recovery of critical suppliers and return-home guidelines for reestablishing normal operation after the disaster.

2. DR testing is another area of common shortcomings. Specifically, it is important for testing to follow a structured project plan that comprehensively covers all DR functions. Testing must also manage the business risk that tests may fail (leaving applications unavailable) or that application and infrastructure dependencies may trigger unexpected ripple-through effects that impact other parts of the business.

3. Some DR organizations have grown organically. In such organizations, it is common that DR-related roles are not defined and assigned formally, but rather employees fill in for DR-related tasks as needed. Communication paths and decision rights also tend to be implicit, unnecessarily lengthy and sometimes convoluted. Clearly, such organic structures have a negative impact on the effectiveness and efficiency of all management processes, and addressing them should be a priority.

A more technical and in-depth assessment of DR management would include a review of the available backup capacity, technology choices (e.g., use of virtualization), and completeness and correctness of dependency maps.

Assessing Technical Operations
While management may be the most challenging aspect of the framework, the operations of technology and infrastructure may be the most straightforward, provided that one has addressed the other two aspects of the framework. Determining whether the backup, restoration and recovery strategies are implemented, managed and maintained in accordance with management’s directive is relatively black and white. The most common shortcomings encountered here are misconfigurations and omissions of all kinds, including:

• Insufficient equipment or capacity at backup sites
• Failure to recover foundational services such as Domain Name System (DNS) or directory services
• Inaccurate configuration files, asset inventories, contact data, chain-of-command information or recovery sequences
• Understaffing or lack of DR training

Assessing Outsourcing Relationships
It has become common to outsource IT operations. As figure 2 shows, this also affects the DR program.

Roles and Responsibilities
As illustrated, the bottom tier (i.e., the technical operation of the DR infrastructure) becomes the sole responsibility of the outsourcing provider. Management is largely the provider’s
responsibility, but the client retains certain management rights in, for example, the planning and execution of DR tests or the execution of audits. These management rights depend, however, on DR governance, which is split into client-side, provider-side and shared governance. The shared governance is partially defined by the outsourcing contract and service level agreements (SLAs) and partially left open based on implicit agreements.

An assessment of the technical operations, the client-side governance or the provider-side governance can be done according to the framework outlined previously.

**Assessing Shared Governance and Management Processes**

Assessments of shared governance and management are more complex, as they involve two parties: the client and the provider. The Achilles heel of such assessments is always the outsourcing contract, which can leave too many issues unspecified and subject to implicit agreements. In extreme cases, the outsourcing contract may not even authorize the client to audit or assess the provider’s DR program. The most visible symptoms of outsourcing relationships that rely too much on implicit agreements rather than contracts and SLAs are dissatisfied clients, poor DR performance and burdened client/provider relationships.

When such situations are encountered, it is of limited value to the outsourcing client to point out all the ways in which the provider’s DR program falls short of the client’s expectations. Unless such shortcomings are in clear violation of the outsourcing contract, it will be difficult, or even impossible, for the client to request rectification or restitution. Therefore, it is recommended to review the outsourcing contract and SLAs and to identify changes that need to be made to the contract when it is renegotiated. Additionally, it is frequently beneficial to review and revise the client’s approach to managing vendor risk, including its criteria for selecting outsourcing providers.¹⁰

When the outsourcing contract follows good practices, these issues do not arise and the assessment can proceed very much along the lines of the previously outlined framework. In such cases, it is best to focus specifically on the interface between the client-side and provider-side management teams. This interface is frequently the source of errors and communication breakdowns, which negatively impact the management processes (see Assessing Management section).

**CONCLUSION**

In most organizations, the DR function is under constant cost pressure, and efficiency is of the essence. To support this
imperative, this article presents a framework that can help auditors as well as executives focus and prioritize their DR assessments. The framework distinguishes the governance, management and operations tiers and shows what issues are most commonly encountered during assessments of each tier. Many of these issues are mistakes or omissions that can result from the inherent complexities and cost pressures of disaster recovery. The framework also makes an important contribution to the field of DR assessment because it adds minimally to these costs and complexities. The framework applies to outsourced IT operations, in which many issues have their origin in overly vague outsourcing contracts. In these cases, it has been shown that the contract must be made more rigorous before any DR-specific issues can be resolved.

ACKNOWLEDGMENTS
The authors thank Elias Schibli and Florian Widmer for their valuable comments on earlier versions of this article.

ENDNOTES
3 Based on the experiences of the authors
6 Doughty, Ken; “IT Governance: Pass or Fail?,” ISACA Journal, vol. 2, 2005
7 Op cit, Hiles
8 Ibid.
10 Davis, Chris; Mike Schiller; Kevin Wheeler; IT Auditing: Using Controls to Protect Information Assets, 2nd Edition, McGraw-Hill, 2011, ch. 11 and 14