How To Audit Business Continuity Programs

Planning & Management

Written by Dan Bivens

Being able to continue critical business functions while responding to a major disaster, and then return normal operations efficiently and cohesively afterward, is a critical success factor for all organizations. Effective Business Continuity programs (BCPs) and disaster recovery (DR) programs are vital and have become a necessary cost of doing business.

Internal audits of the BCP and DR programs are highly recommended. The board and management need assurance regarding the effectiveness of those efforts. They want to know that the DR plan will work when needed, the investments in BCP and DR are obtaining good value, and a disaster will not bring the business to its knees. An independent assessment of the BCP and DR programs by internal audit can provide objective feedback that helps ensure the programs are adequate to prevent a business failure. Think about it. While everyone has focused on the requirements of Sarbanes-Oxley for almost five years, have your DR and BCP efforts kept pace with today’s new challenges and expanding requirements? Have an answer, because your board is increasingly likely to ask.

An audit of the BCP and DR program can take many forms. At its simplest, auditors can conduct a quick “BCP/DR health check,” reviewing the plans and interviewing key stakeholders. At its most complex, the audit team can analyze almost every aspect of the program, evaluate the risk-based planning, observe BCP/DR tests, assess the completeness of the business-impact analysis, and so forth. The type and extent of auditing performed depend on the risks involved, management’s assurance requirements, and the availability of audit resources. External specialist resources may be useful on occasion. The auditors might participate as formal observers in mock drills or review the program’s documentation and assess its comprehensiveness and completeness. Your options are numerous. Internal auditors normally will review what has been planned and achieved against management’s expectations and then compare to generally accepted best practices in the field. This is where audit objectivity comes to the fore. The auditors have a legitimate purpose to assess whether management’s expectations are reasonable and sufficient, given the level of risk to the organization and in relation to other similar organizations.

Audit Scoping Phase

As with any audit, defining the goals and objectives for a review of the BCP and DR programs is the auditor’s first task. Scoping is best conducted on the basis of a rational assessment of the associated risks. The following aspects are generally worth considering when scoping a BCP and DR audit:

Overall program governance. How are the programs managed? Are they given appropriate strategic direction and investment? (That is, does the organization place sufficient emphasis on BCP and DR?) Are suitable sponsors and stakeholders involved, representing all critical parts of the organization? Do they take sufficient interest in the programs, demonstrating their support through involvement and action? Most importantly, who is accountable for their success or failure?