Media Rating Council ©

420 Lexington Ave, Suite 343
New York, NY 10170

(212) 972-0300
staff@mediaratingcouncil.org

PREPAREDNESS: THE VALUE OF STANDARD A.7.D

In December 2011 MRC introduced a new requirement to MRC's Minimum Standards for Media Rating Research (Standards), the set of criteria that serve as the foundation for all MRC audits. MRC established Standard A.7.d requiring Services to develop, maintain, and periodically test business continuity plan and disaster recovery procedures to ensure business-critical processes continue to execute during an extraordinary event such as a natural disaster or other significant business interruption. Standard A.7.d also requires Services establish data issuance and disclosure policies in the event business interruptions should occur. Our Industry's increasing reliance on timely measurement data spawned the genesis for Standard A.7.d, particularly in light of those segments who have grown to depend on daily, intraday, and in-some instances near real-time data to transact business.

Standard A.7.d is just one element of the set of criteria applied by MRC's CPAs to assess the operating effectiveness of IT control environments among the Services we audit, and what follows is a high-level summary of areas considered by the CPAs when assessing compliance to this highly critical component. Four key aspects are evaluated to assess the resiliency of a Service's information technology environment, and its plans to address an extraordinary event.

1. Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) – Verify the existence of DRP and BCP plans and the extent to which these are sufficient to support continuous operations in case of an emergency or contingency. The DRP should be designed to ensure technical operations can be restored following an unanticipated interruption. The BCP should be structured to allow service operations to continue during an emergency. Both plans should be integrated and tested at least annually.
2. Backup and Recovery Procedures – Review the Service's backup policy to determine whether the policy is current, supports the relevant technology infrastructure including applications and databases, and that backups and subsequent restorations are performed on a periodic basis, and stored within appropriate offsite locations. There should be periodic testing, plus security procedures should exist to ensure only appropriate personnel have access to the backup data and the backup execution schedules.
3. Incident Management – Assess the Service's policies and procedures for incident management to determine whether these address the appropriate risks and that tools and techniques exist to identify, record, escalate, and ultimately resolve incidents that could impact the business and technical operations of the service. Incidents could arise from cyber security events, system capacity issues, program functionality failures, interface failures etc.
4. Job Scheduling and Interfaces – Assess whether the Service has appropriate processes and controls to monitor that data integrity is maintained as it is processed by various applications or components of the system, and that effective incident tracking and resolution processes exist. Also, that interfaces are subject to change management controls and the appropriate personnel have access to modify jobs and their execution schedule.

Services are also held responsible for ensuring appropriate controls exist at third party data centers or any cloud services utilized, and this is typically managed through a review of the provider's System and Organization Control (SOC) reporting.

STANDARD A.7.D EXECUTIVE SUMMARY

Timing of the adoption of the adoption of Standard A.7.d turned out to be fortuitous in that it helped services engaged in the MRC accreditation process become prepared for the current COVID-19 worldwide pandemic. Disaster recovery and business continuity efforts are now underway across all the services MRC audits, and in some instances this crisis is testing the limits of what anyone ever envisioned. A national shutdown of non-essential businesses, with Government orders to avoid social interaction forced a large number of employees to have to work from home, with little advance notice. Telephone Call Centers, which in the past served as backup for one another were all forced to close. Equipment was purchased at massive scale to allow for secure remote access, with monitoring capabilities to ensure continuance of operations with quality oversight. In-person interviewing, meter installations and maintenance procedures, and other in-field activity had to be halted, at least temporarily, and so teams were assembled to develop acceptable alternative solutions. Yet throughout all this, with firm resolve, pre-planning efforts (thank you A.7.d), and innovative thinking, Services have managed to continue to function and supply critical information to clients.

To the staff's knowledge there have been only three instances when additional guidance has been added to MRC's Minimum Standards for Media Rating Research since first written in 1963, and A.7.d qualifies as one of these. We encourage you to review MRC's Standards and other guidelines published on our website at www.mediaratingcouncil.org.