What Every IT Auditor Should Know About Backup and Recovery

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA, is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications.

All entities that use IT and data in their operations have a need for a backup and recovery plan. The plan should enable the entity to recover lost data and to recover computer operations from a loss of data. At the low end of need, the entity may experience a data loss (e.g., corrupted data) and simply need to restore a backup of data. At the high end of need, the entity may experience loss of computer operations and more, from a pandemic event (e.g., fire, flood, tornado or hurricane).

Entities that have a high risk regarding backup and recovery include, at least, those that rely heavily on IT and data to conduct business, operate solely online (e-commerce) and operate 24/7. More than likely, all Fortune 1,000 enterprises are at a high risk; however, a small entity that uses cutting-edge IT and whose business processes are heavily reliant on IT is also at a high risk.

This column attempts to explain the principles of an effective backup and recovery plan and to provide some guidance for conducting an IT audit for backup and recovery.

DATA

Management should provide for a means to back up relevant data on a regular basis. The principle for regular data backups is to back up data daily. That backup could be to media (e.g., tape or external hard drive), or it could be to a remote location via the cloud (i.e., the Internet). If an enterprise is backing up to media, the aforementioned principle recommends that backups be conducted to a different media for end-of-week and end-of-month backups (this daily, weekly and monthly set of backups is known as "grandfather-father-son").

The next concern is whether the backup process is reliable. Therefore, upon using a new backup methodology or technology, management should provide a means to test the data afterward to ensure that the process is actually recording all of the data onto the target backup device.

Another concern is where the backup is stored. If it is stored onsite and if the entity suffers a pandemic event such as a fire, the event would destroy the operational data and the backup data. Thus, the backup principle for storage is to provide a location that is at a safe distance from the entity's location. The cloud automatically provides this element.

Additionally, management should provide a test for restoring the backup at least once a year. That test should be documented, even if it is just a screenshot showing the data restored.

COMPUTER OPERATIONS

The purpose of the computer operations piece of a backup and recovery plan is to recover from a broad, adverse effect on the computer systems of the entity (**figure 1**). This part of the plan is commonly called a business continuity plan (BCP) or disaster recovery plan (DRP).[1] The adverse event could be systems-related, such as the failure of a mainframe computer to operate, or it could be the result of a natural disaster, such as a fire that destroys some or all of the computer systems and data.

Figure 1—Recovery Principles

- Identify and rank critical applications.
- Create a recovery team with roles and responsibilities.
- Provide a backup for all essential components of computer operations.
- Provide for regular and effective testing of the plan.

Obviously, this plan is much more involved than simply making a backup of data and being able to restore it effectively when necessary. In this case, it may be necessary to restore everything about the infrastructure: computers, operating systems (OSs), applications and data. Even systems documentation and computer supplies could be involved.

The principles of developing a BCP/DRP include a step to identify the critical applications and rank them in importance of operations. This list becomes strategically valuable if ever needed in providing the recovery team with a blueprint of how to restore application software.

Another principle, and obvious need, is to create a recovery team. The team should include all of the functions and roles necessary to quickly and completely restore computer operations. There should be a document that identifies all of the members of the teams, their respective roles and the steps each would take in restoring operations.

The heart of a BCP/DRP is to provide a backup means of providing the essential components of computer operations (**figure 2**).

Figure 2—Computer Operations Essential Components to Back Up

- Site/facility
- Computers and infrastructure (hardware)
- OS
- Applications (software)
- Data
- Supplies
- Documentation
- Personnel

The site should include a building, electricity, furniture and other basic needs for housing the computer operations. Typically, the site follows the same principle as storage of backup data in that it is located a safe distance from the entity's facility, but not too far to reach in a timely manner if it is necessary to recover operations.

The hardware aspect does not necessarily require the restoration of a full complement of computers and infrastructure, but it does require the minimum degree of computers and infrastructure to temporarily restore computer operations. For instance, most entities have one or more servers, and at least one of those servers will be needed to restore operations, but maybe not all of them. Likewise, some semblance of the network will need to be restored. Enough computers will need to be restored to conduct the essential business processes as determined by the plan.

The OSs on the computers and servers will need a backup. That includes the network OS and server (e.g., mainframe).

There needs to be a backup of all relevant applications. The list of critical applications mentioned previously will provide the list of applications that need a backup and the order in which to restore them.

As discussed previously, data backup can be stored offsite at or near a location close to the backup site, or it can be stored in the cloud for easy and efficient data restoration. The list of applications provides the primary source of data needed.

The plan should include a means of providing supplies such as preprinted forms (e.g., checks, invoices), as well as consumable computer supplies (e.g., printer ink). This can be provided by storing a reasonable quantity of supplies at or near the backup site or by having a contract with a vendor to provide them on short notice.

Certain manuals will be needed as well, including user and technical manuals. These manuals are needed because members of the recovery team may not normally do some of the business processes.

Last, the plan should provide for adequate personnel to maintain necessary computer operations. The recovery team is usually a key part of the personnel element.

There are some common methodologies used to provide for the first few elements. Utilizing a hot site is an approach that usually provides for the site (e.g., building, electricity, furniture), computer and OS (specifically the server and/or mainframe the entity uses, which is up and running) needs. When using a hot site, recovery gets a "jump start," allowing the entity to take its data backups and applications backups and begin the remainder of the process to restore computer operations.

A cold site, however, provides only the site aspect. If the entity chooses a cold site, it would need some way to provide backup for computers and the OS (possibly a backup of the OS on media). A mutual aid pact involves the broadest scope of backup. In this approach, the two entities use the same computer, OS and, often, applications. For example, a large retailer has two branches back up data to another branch and, then, uses the systems at the other location to restore operations. This approach is inexpensive and has less associated risk.

Principles of backup and recovery suggest that the most important step is to provide a full test of the BCP/DRP at some regular interval to ensure that it actually works and to improve the plan to be more efficient and effective. Ideally, it would be tested annually, but for larger or more complex environments, once every three years may be sufficient. Often, internal audit or IT would conduct the test. That test can include as much reality as needed, including something as radical as unplugging the computer in the main computer center.

The scope of what an IT auditor would do to test and collect evidence about backup and recovery depends on the type of audit involved and the risks (**figure 3**). In an internal audit or special IT review, the objectives of management would dictate the scope.

Figure 3—Possible Tests/Procedures for Backup and Recovery

Data	• Review or observe backup procedures. • Review documentation of a successful restore (within the last year). • Verify restoration personally (when risk is high or restoration is an audit objective).
Site/computers/ OS	• Review the provisions of the BCP/DRP. • Review a contract (hot site, cold site, mutual aid, etc.). • Verify the ability to restore these aspects.
Applications	• Review the plan's provisions. • Review the critical applications list, including ranking. • Verify the ability to restore (personally, when risk is high or restoration is an audit objective). • Observe or inquire about the backups of application software and location.
Supplies/ documentation	• Review the plan's provisions. • Observe or inquire about the provisions and location.
Recovery team	• Review the plan's provisions. • Interview one or more members of the team, and ask about roles and responsibilities. • Gain assurance that there is provision for adequate personnel for a successful restoration.

For a financial audit, the scope of testing would be concomitant with the nature and complexity of IT, which is directly correlated to the risk that IT presents to the risk of material misstatement. Thus, an entity with standard commercial equipment and applications, with only one server and a limited number of computers (i.e., simple IT), would need a low-level, simple audit procedure. The IT auditor would probably use a simple test for the backup of data (e.g., a screenshot showing that a test restoration was successfully conducted in the fiscal year). The IT auditor would definitely want to review the data backup procedures and the BCP/DRP. Procedures would also likely involve some questions about backup and recovery of the chief information officer or similar position's data, but the procedures would probably not include testing the recovery of a data backup or testing the full BCP/DRP. However, if IT were highly sophisticated and spread across multiple locations, there would be a need for more powerful and complex test procedures and more evidence.

CONCLUSION

All entities must consider and provide a plan for backup and recovery. The IT auditor would want to test the recovery of data and computer operations, but only to the level necessary. When risks or objectives call for simple tests, the IT auditor needs to develop low-level, simple tests that will provide adequate evidence. For more complex situations, more complex and powerful tests are needed to provide assurance that backup and recovery will be successful—especially in the case of a pandemic event.

ENDNOTE

[1] BCP and DRP are different and separate processes, but for the sake of this article, they will be referred to as one unit.