Backup and Recovery

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2k6Vlwr

When I sat for (and passed!) my Certified Information Systems Auditor® (CISA®) examination back in 2005, one of the key task statements was "Evaluate the adequacy of backup and recovery provisions to ensure the resumption of normal information processing in the event of a short-term disruption and/or the need to rerun or restart a process."[1] By the time I came to update the *CISA® Review Manual* for the 2016 job practices, an equivalent task read "Evaluate IT continuity and resilience (backups/restores, disaster recovery plan [DRP]) to determine whether they are controlled effectively and continue to support the organization's objectives."[2] Although the wording has changed, the message from ISACA® is clear—backup and recovery are still key controls.

I find this interesting since, due to technological improvements—most notably virtualization and the cloud—IT auditors often receive pushback when seeking assurance on IT continuity and resilience. So, how should an IT auditor respond when presented with these newer technological solutions? In this column, Tommie Singleton previously advocated principles for backup and recovery.[3] I believe it is worth reviewing these principles, considering the changes in technology.

Ian Cooke, CISA, CGEIT, CRISC, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees and is a current member of ISACA's CGEIT® Exam Item Development Working Group. He is the community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke supported the update of the *CISA Review Manual* for the 2016 job practices and was a subject matter expert for ISACA's CISA and CRISC Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed are his own and do not necessarily represent the views of An Post.

Backup Principle 1—Perform Regular Backups

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, this 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").[4]

I think we can all agree that with virtual machine (VM) replication, the first sentence in this section should now end with "at least daily." Indeed, with VM replication you can create an exact copy of the VM on a spare host and keep this copy in sync with the original VM. So, the principle of (at least) daily backups still stands.

However, replication alone can, in certain circumstances, increase the risk. If the VM or the data is somehow corrupted, this corruption will automatically be replicated to the other machine(s). Therefore, it makes perfect sense to maintain separate VM backups. Since we cannot be sure when a data corruption might be discovered, it also makes sense to maintain grandfather-father-son backups.

A word of caution: The administrator of the VM backups should not have Internet access since this would expose the backups to ransomware. All such users should have a second, unprivileged account that does not have access to the VMs, but does have access to the Internet for troubleshooting purposes.

Backup Principle 2—Test Backup Process Reliability

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.[5]

It is a widespread practice to back up entire VMs, but it is possible to exclude data to reduce the size of the VM backup or replica and decrease the load on the network. This principle, therefore, still stands, as an IT auditor should still validate what is being backed up. Furthermore, as there is a risk of corruption during the backup process, an IT auditor should ensure that a health check is periodically performed. This typically means scheduling a cyclic redundancy check (CRC) for metadata and a hash check for VM data blocks in the backup file to verify their integrity. The health check provides assurance that the restore point is consistent and that it will be possible to restore the data.

Backup Principle 3—Use Secure Storage

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 use a location that is at a safe distance from the entity's location. The cloud automatically provides this element.[6]

This principle, obviously, still stands and, yes, the cloud automatically provides this element. However, there is also an element of risk when backing up to the cloud—sensitive enterprise data may be accessible by the cloud provider and/or other third parties who share the cloud. It is, therefore, vital to ensure that VMs backed up to the cloud are encrypted. The type of encryption, key management procedures, etc., should all, of course, be verified.[7]

Backup Principle 4—Perform Test Restores

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.[8]

Ah, the test restore! For some reason, many IT departments just do not see the value. Anyone who is an IT auditor has heard one, if not several, variations of "Test restores are not needed because we use clustering/have a failover solution/use VM replication/use storage area network (SAN) replication/use log shipping and, therefore, we just would not restore that way."

"IT MAKES SENSE TO PERFORM TEST RESTORES TO ENSURE THAT THE CORRECT DATA ARE BEING BACKED UP, THAT THE DATA ARE, IN FACT, RESTORABLE AND THAT THE ENTERPRISE KNOWS HOW TO RESTORE IT."

However, it has already been noted that replication can increase the risk of data loss if data are corrupted and/or sabotaged. Depending on the configuration, the same can be said for each of the above solutions. Regardless, restoring from backup simply provides an additional option in a real disaster scenario. Therefore, it makes sense to perform test restores to ensure that the correct data are being backed up, that the data are, in fact, restorable and that the enterprise knows how to restore it. This principle still stands.

Recovery Principle 1—Identify and Rank Critical Applications

The principles of developing a business continuity plan/disaster recovery plan (BCP/DRP)[9] 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.[10]

In a previous column, I advocated categorizing applications in terms of confidentiality, integrity and availability.[11] The suggested availability categorization provides the list of ranked critical applications and is required regardless of the technology used to restore the applications. Therefore, this principle still stands.

> "THE HEART OF A BCP/DRP IS TO PROVIDE A BACKUP MEANS OF PROVIDING THE ESSENTIAL COMPONENTS OF COMPUTER OPERATIONS."

However, the application list should be adjusted to consider application interfaces and data flows. For example, application A may be more business critical than applications B and C, but may require data from application C, which should, therefore, be restored first. Also, multiple applications may share a single VM. If applications do share a VM, an enterprise may be restoring a lower-priority application alongside a high-priority application.

Recovery Principle 2—Create a Recovery Team With Roles and Responsibilities

Another principle, and obvious need, is to create a recovery team. The team should include all the functions and roles necessary to quickly and completely restore computer operations. There should be a document that identifies the team members, their respective roles and the steps each would take in restoring operations.[12]

A team is still required to perform the actual recovery, so this principle still stands. My concern with virtual and/or cloud technologies is that the recovery is left to the IT operations team responsible for the VMs. I believe it is still vital to confirm the recovery point, that all expected transactions are present and that all interfaces are running correctly—all of which still require the input of application experts and business users.

Recovery Principle 3—Provide a Backup for All Essential Components of Computer Operations

The heart of a BCP/DRP is to provide a backup means of providing the essential components of computer operations. 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.[13]

Regardless of the technology, this principle still stands. The cloud may negate the need for an enterprise to have its own physical secondary data center, but there must still be a location for staff to access the restored services. For example, this article is stored on a Microsoft OneDrive and I am accessing it from my office at home. If my home and laptop were destroyed (perish the thought!), I would need a new location from which to access the article.

Recovery Principle 4—Provide for Regular and Effective Testing of the Plan

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.[14]

There is no doubt that VMs and the cloud can largely automate application recovery while enhancing both recovery times and recovery points. However, in a disaster situation there is still very much a need for human actions and operations. This is the very definition of a process[15] and, where processes exist, there is a need to confirm that they produce the desired results. The only way to do this is to regularly test and document the results of the BCP/DRP. Therefore, this principle very much still stands. Further, regardless of the technology in use, the BCP/DRP can always be enhanced. Testing allows for this while also allowing the IT auditor to provide assurance.

Conclusion

This column could well have been titled "What Every IT Auditor Should *Still* Know About Backup and Recovery." Innovative technologies such as VMs and the cloud help the efficiency and effectiveness of backup and recovery plans, but they do not replace the need to plan, document, or test and test again. The technologies still rely heavily on human intervention and, while that is the case, assurance can be provided only by applying good principles to backup and recovery.

Endnotes

1 ISACA, *CISA Review Manual 2005*, USA, 2004
2 ISACA, *CISA Review Manual 26th Edition*, USA, 2016
3 Singleton, T.; "What Every IT Auditor Should Know About Backup and Recovery," *ISACA® Journal*, vol. 6, 2011, *www.isaca.org/Journal/archives/Pages/default.aspx*
4 *Ibid*.
5 *Ibid*.
6 *Ibid*.
7 ISACA, *Assessing Cryptographic Systems*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/Documents/Assessing-Cryptographic-Systems_res_eng_0817.pdf*
8 *Op cit,* Singleton
9 Business continuity plans and disaster recovery plans are different and separate processes, but in this article, they will be referred to as one unit.
10 *Op cit,* Singleton
11 Cooke, I.; "Doing More With Less," *ISACA Journal*, vol. 5, 2017, *www.isaca.org/Journal/archives/Pages/default.aspx*
12 *Op cit,* Singleton
13 *Ibid*.
14 *Ibid*.
15 Merriam Webster defines "process" as "(a) series of actions or operations conducing to an end." *www.merriam-webster.com/dictionary/process*

Enjoying this article?

- Learn more about, discuss and collaborate on privacy and data protection in the Knowledge Center. *www.isaca.org/privacy-data-protection*