

# **Risk Mitigation Considerations for Backup and Restoration Processes**

Author:  
George Spafford

Updated  
May 25, 2006

v1.0d

# 1 Copyright

This document is the copyright of George Spafford © 2006. Commercial sale of this paper is prohibited. It is provided as a service by Spafford Global Consulting, Inc. who retains all rights to the document and its content.

To provide feedback or to contact the author, please use:

George Spafford  
Spafford Global Consulting, Inc.  
3353 Celina Avenue  
Saint Joseph, MI 49085  
USA  
<http://www.spaffordconsulting.com>  
Phone: 269-556-9597  
FAX: 208-978-6295  
Email: [george@spaffordconsulting.com](mailto:george@spaffordconsulting.com)

## 2 Table of Contents

1	Copyright .....	2
2	Table of Contents .....	3
3	Purpose.....	4
4	Background.....	4
5	Recommendations.....	5
5.1	Understanding Requirements.....	5
5.2	What is the Backup Window?.....	5
5.3	Recovery Window .....	6
5.4	Retention Periods .....	6
5.5	Media Strategy .....	6
5.5.1	Full Backups .....	6
5.5.2	Grandfather, Father, Son.....	6
5.5.3	Eight + Full .....	7
5.6	Media Identification.....	7
5.7	Encryption Requirements.....	7
5.8	Review of Backup Logs.....	8
5.9	Physical Security of media.....	8
5.10	Access Restrictions to Backup Applications .....	8
5.11	Security of Backup Logs.....	8
5.12	Onsite Storage Needs.....	8
5.13	Offsite Storage Needs .....	9
5.14	Redundancy of the Backup System .....	9
5.15	Preventive Maintenance.....	9
5.16	Documented Work Instructions .....	9
5.17	Bare Metal Builds .....	10
5.18	Management of Dependencies.....	10
5.19	Formal Restoration Testing.....	10
5.20	Long-term Archival Strategy .....	11
5.21	Staff Training.....	11
5.22	Audit .....	11
5.23	Change Management .....	11
6	Summary .....	12
7	About the Author .....	13
8	Additional Resources .....	14

### **3 Purpose**

Many organizations, both large and small, rely on their information technology systems to the extent that their loss can be devastating. To alleviate risks, many have invested in data backup systems in the hope that by simply performing backups their data is safe. Unfortunately, as many groups have painfully learned, the truth can be that they have little to no protection at all due to an inability to recover as planned. The purpose of this executive briefing is to set forth strategies for mitigating the risks surround the backup and restoration of data.

### **4 Background**

Most groups recognize that they need to make backups of their systems and data just in case something bad happens. The events can range from catastrophic events, such as natural disasters, to groups who need to restore a single file due to the original being lost or corrupt.

In response to the need, groups have purchased and implemented hardware and software to back up the data. What they have neglected are the processes with adequate controls to ensure that:

- What truly needs to be backed up is
- The frequency of backups meet business needs
- There are sufficient backups historically
- The backup jobs/tasks are performing as expected
- There is proper security
- There is sufficient retention
- Capacity is properly monitored
- Regulatory and legal compliance requirements are being met
- They can truly restore the systems and data to the expected state!

In fact, the list can go on and on. The point is that organizations need to step back and ensure that their systems and data are truly safeguarded to the extent they need.

## 5 Recommendations

The following recommendations are aimed at helping organizations recognize what their backup and restoration requirements are and then suggestions on how to ensure that the objectives of the backup systems are met. Many of these items would be, or could be, covered in Disaster Recovery, Business Continuity Plans, IT Service Continuity Plans and so on. Our objective with these recommendations is to foster review by organizations to ensure that risks are managed and that backups can be depended upon.

### 5.1 *Understanding Requirements*

The first step is to understand what the scope of the backups needs to be. Consider using a Business Impact Analysis (BIA) and a data classification exercise to help set scope and identify requirements.

First, perform a business impact analysis (BIA), you can identify the critical business processes, the various potential risks that could happen, the estimated impact to the organization should they happen, and what countermeasures are required. If there is a business continuity planning team already in place, leverage their work.

Next, by performing a data classification exercise, you can identify the types of data in your organization, the stakeholders, security requirements, retention requirements, backup frequency and so on. This can then be used for consistency across application to ensure that data is protected.

Be sure to involve the right stakeholders. The requirements of the organization must be understood and not just reflect what IT believes adequate. Consider working with each department including senior management, finance, human resources, legal, internal audit and so on to create a holistic understanding of needs.

Lastly, generate a report documenting how the backup and restoration requirements will be met for each form of data and system.

#### **Formalize Plans**

Involve the parties needed to understand your organization's needs and require them to formally approve that what IT will deliver meets their needs.

### 5.2 *What is the Backup Window?*

In defining backup solutions, IT must negotiate with the business to secure a window of time when backups can occur. The systems put in must be architected to meet these needs.

#### **Open File Backup Technology**

For prospective solutions that offer open file backup technology, do research on the Internet, talk to other users and perform your own testing before blindly accepting the vendor's claims.

### **5.3 Recovery Window**

The Information Technology Infrastructure Library (ITIL) discusses how IT provides services to the business which is then comprised of various components such as IT personnel, hardware, software, external services and so on. Each of these is considered a configuration item (CI). From the customer's and user's perspectives, they just want the service restored to the level they expect – they don't care about the technical requirements behind the scenes, or at least they shouldn't. It is IT's responsibility to take the business requirements and architect solutions for the backup and recovery of CIs to meet business needs.

### **5.4 Retention Periods**

IT must understand how long the data must be retained. This will affect the backup architecture, local physical media storage, offsite media storage, and overall costs. For example, it may be that period end financial data must be stored for seven years and that due to some contractual requirement, some weekly tapes must be archived for five. There is no single answer – the period(s) must meet business requirements.

### **5.5 Media Strategy**

Not only must there be backups, but the frequency of backups and strategy of media use must be carefully considered and deployed to support the business.

#### **5.5.1 Full Backups**

Using this method, every backup is a full backup of all data and/or systems. While this sounds enticing, the sheer volume of data to backup may take too long and consume too many tapes in the long term to make this worthwhile.

#### **Operating System (OS), Application and Data Split**

It is possible to split the backups of the OS, applications and data apart into two or even three distinct backups. If this is done, it is very important that Change Management alert operations as to changes to the OS or applications so appropriate backups can be made. This can shorten the backup cycle dramatically and still provide adequate coverage as long as the process is managed to ensure that the current environment can be reproduced. Never forget that the ability to restore the last known good state is every bit as important as performing the backup procedures.

#### **5.5.2 Grandfather, Father, Son**

This method was originally developed by 3M. The idea is to do incremental backups of only the data that has changed each night Monday through Thursday using two sets of media. Thus, you'd have Monday week 1, Monday week 2, Tuesday week 1, Tuesday week 2 and so on. This is the so called "Son" set of media and the tapes get reused every other week (set 1 this week, set 2 the next week, set 1 the following and so on).

The "Father" set of media are the Friday full backups that are performed each week. There are five sets media in order for months with five weeks to be accommodated and are reused each month.

Lastly, the “Grandfather” media contains full backups performed on the last day of each month. There are three sets of these tapes and are reused each quarter.

Some groups will choose variations on this model to archive the Father or Grandfather tapes according to their retention policy.

### **5.5.3 Eight + Full**

A direct variant of the Grandfather, Father, Son model is Eight plus full. In this model, there are two sets of Monday through Thursday media with incremental backups. The Friday sets are then stored according to the retention policy.

## **5.6 Media Identification**

Storing media can be a challenge as it is very easy to quickly accumulate a large number of tapes. To facilitate tracking, the tapes must be labeled so parties can understand what the tape contains. The labeling should be visible from the direction stored so using a tape as an example, it may be that the top of the tape is labeled along with the back edge, or spine.

For organizations using backup software with a media management database (sometimes referred to as “catalogs”), identify the tapes with the unique identifier assigned by the software.

For groups without media tracking, be sure to log the date and tape name/identifier in order to track what was backed up, when and to what tape. Some groups will create log sheets identifying each server and then the tapes used for example.

### **Disaster Recovery Preparation**

Do not forget to backup the media catalogs and store them offsite as well! Otherwise, if the main backup system is lost, you may not know what media contains what data.

## **5.7 Encryption Requirements**

In this day and age of privacy, competition, hackers and so on it is a good idea to encrypt all data unless the encryption drastically impacts performance. In that case, be sure to at least encrypt all sensitive information that is identified with inputs from security, the legal department and your compliance teams (if they are separate from legal).

### **Disaster Recovery Preparation**

Ensure that the encryption is reversible. If your backup system stores a key file on the local backup system’s hard drive and that is lost, you will lose access to your data. Work with the vendor and **test** to ensure that encrypted data can be restored on a different system.

## **5.8 Review of Backup Logs**

One of the most important tasks that must be performed is to review the backup job logs generated by the backup application and look for any errors that occurred and take corrective action.

To evidence this activity, create a check list of backup jobs to review and space to record any discrepancies found and corrective action taken. The operator performing the review must sign and date the record and then it must be filed for future evidence. These logs must be routinely audited to confirm the activity is being performed as expected.

### **Log Review is a Mandatory Key Control**

This is a mandatory control. Countless groups have been devastated to find that key data was not being backed up as expected each night because files were open, etc.

## **5.9 Physical Security of media**

Access to backup media must be restricted both onsite and off. Furthermore, it must be protected from environmental hazards such as heat, sunlight, magnetic fields, fire, water damage and so on. Media that is misplaced, damaged or tampered with can all affect an organization's ability to recover from an incident.

There are many organizations being publicly embarrassed for losing backup media. You do not want to add your organization to the list.

## **5.10 Access Restrictions to Backup Applications**

Backup application access must be limited to authorized parties. Unauthorized changes to backup schedules or parameters can affect the integrity of the backups.

## **5.11 Security of Backup Logs**

Whether the archive system's backup catalogs, backup log files in the OS or paper log sheets, access to those logs must be controlled. Loss or corruption of the data can affect the organization's ability to recover from an incident.

## **5.12 Onsite Storage Needs**

Media should not be left casually laying around, in desks, cabinet, etc. Careful thought should be given to the risks the media faces while onsite and then mitigation strategies implemented.

### **Media Safes**

A fireproof safe is not adequate for media because heat and humidity must be controlled. Media rated safes often look like a vault within a vault. For groups storing media on site, even temporarily, a media rated safe is recommended.

### **5.13 Offsite Storage Needs**

Due to the chance of fires and other site-specific risks, a strategy for storing media offsite must be followed. Be sure that the method used is secure, timely and cost effective. In this day and age, this has moved from being an optional safeguard to a mandatory control that all organizations should follow.

All tape movement between the local and off-site facility should be logged including the date, time, tape identifiers, IT representative's signature and the courier's signature. Any recordkeeping and reporting requirements should be identified and implemented with the assistance of the offsite supplier.

#### **Regional Disasters**

Take into account risks to the offsite facility. In New Orleans, companies dutifully sent their tapes offsite. Then, after the flood, they found both their onsite and offsite facilities had been compromised and the tapes ruined.

### **5.14 Redundancy of the Backup System**

There must be fault tolerance in the hardware, software and processes used in the backup and recovery process. In the event that the main backup and restoration device is lost, what will you do? Be sure that you have access to the requisite hardware, software and backup media in the event of an incident. It may be that a backup drive fails or that a disaster occurs.

The objective is to reasonably ensure continuity in the backup process as well as the ability to restore. The level of redundancy is based on the risks that management is willing to accept.

### **5.15 Preventive Maintenance**

Backup devices can have problems. Whether we are talking about dirty tape heads or accumulated file fragmentation on a removable device there is a need to proactively ensure that the device's availability and reliability are maximized.

#### **Tape Drives**

Follow the tape drive manufacturer's recommendations for cleaning the drive. Develop a schedule and log sheet to verify that cleaning is being performed as expected and periodically inspect the log sheets.

### **5.16 Documented Work Instructions**

All policies related to the backup of data and work instructions detailing how to perform the backup and restorations must be formally documented and maintained. On a regular schedule, operations should be audited against the approved documentation to verify compliance.

#### **Process Compliance**

People must realize that there are only two acceptable outcomes with processes – you either follow a process or you formally change the process. There is no other option.

### **5.17 Bare Metal Builds**

As a recommendation, review software that can allow for devices to be recovered from the bare metal meaning that you have a brand new system with nothing on it.

The author has witnessed dramatic improvements in recovery times through the use of these technologies. For example, one server that took over 8 hours dropped down to two and most of that time was spent waiting for the data to automatically restore from the tape drive to the new server's hard drive.

### **5.18 Management of Dependencies**

Understand any dependencies that the backup and recovery processes have. Take into consideration:

- Hardware – the host, backup devices, local area networks, wide area networks, etc.
- Software – the backup software, license keys, physical license devices such as “dongles” and so on.
- People – who must be involved? Who must be alerted, etc.?
- Other issues – environment, physical space, power, etc.

The author once had to restore a system after a hard drive failure only to find out that the operating system CD supplied was an “upgrade” version and then had to scramble to find a previous OS version CD in order to recover the system.

### **5.19 Formal Restoration Testing**

The reason that backups are performed is to allow for recovery. The only way to ensure that recovery is possible is to formally test the processes involved. There have been countless incidents where organizations failed to test their ability to restore data and then, in a crisis, found that they could not. For whatever reason, hardware, software and media can conspire to return “backup successful” messages when in fact the backup is corrupt and recovery impossible.

Bear in mind that the ability to recover an entire service is very different than restoring a file. The author has encountered many groups who believe they are safe because they periodically restore individual files for users. This is a very different scenario than recovering entire servers or complicated systems using multiple tiers of architecture where even small variations can inhibit IT's ability to restore the service to acceptable use to users.

This must be formal testing with the involvement of the business. First, IT must have sufficient funds and resources in order to have necessary hardware, software, people and time to perform these tests. Second, they must be performed as if the original is gone and then business personnel must execute documented test plans to verify the service has

been successfully restored. The test and results must be formally documented and signed off by the participating parties.

### **5.20 Long-term Archival Strategy**

With age, media can and will fail. In situations where media is archived for a long time, there must be a strategy that ensures the data can still be accessed. The strategy may involve moving from one format to another, periodic testing of old media, etc. The objective is to ensure that data can be accessed if the organization needs it. The strategy must address the needs of the organization tempering risks with costs.

### **5.21 Staff Training**

Staff must be trained on the use of the hardware and software needed to backup and restore systems in order to ensure that they have the needed skills. Furthermore, there should be annual refresher training. All training activity should be formally logged.

### **5.22 Audit**

Internal audit teams should be leveraged to assess compliance to documented processes and work instructions. They also need to assess the economy, effectiveness and efficiency of the processes and that the needs of the business are being met.

#### **Internal Audit Assistance**

Internal audit can help IT understand controls in general and what type of evidence should be generated and maintained to adequately verify compliance. Bear in mind that to be objective, Internal Audit can not design the processes, but they may be able to give recommendations. They are definitely a stakeholder to who should be consulted when identifying the requirements of a backup process.

### **5.23 Change Management**

Changes to hardware, software, schedules, documentation, personnel and so on should all be controlled through the formal IT Change Management process. Unauthorized changes can create risks to the organization and must be avoided.

## **6 Summary**

For many reasons organizations must have backups of their systems and data that they can rely on. In the event of an incident, they must know that the systems can be recovered to an agreed state in order to ensure continuity of the business. Failure to formally manage and oversee this process risks IT's ability to perform as expected. In many cases due to regulatory and legal concerns, failure is not an option and both IT and the organization as a whole needs to plan accordingly.

## **7 About the Author**

George Spafford possesses a strong interest in the intersection of human factors, security and complexity in IT and how that impacts organizations. He is an experienced practitioner and has directed all aspects of IT operations in production environments, planning, implementation and improvement of IT processes. His expertise has lead to providing regulatory compliance, IT Governance, and process improvement training to colleagues in the USA, Australia, New Zealand and China. He is a prolific author on a wide range of topics encompassing technology business, security, IT governance and co-author of “The Visible Ops Handbook”. His Daily News e-mail list subscribers include high level executives from Fortune 500 and international companies.

George has a MBA from Notre Dame, a BA in Materials and Logistics Management from Michigan State University and an honorary degree from Konan Daigaku in Japan. He is a Certified Information Systems Auditor (CISA) and holds ITIL Foundations and Practitioner Release and Control (IPRC) certifications plus has completed ITIL Service Manager training. George is a current member of the ISACA, the IIA, and the IT Process Institute.

## **8 Additional Resources**

The following can provide additional insight.

### **Control Objectives for IT and related Technology**

<http://www.isaca.org/downloads>

### **ISO/IEC 17799:2005**

<http://www.iso.ch>

### **NIST SP800-34 Contingency Planning**

<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>