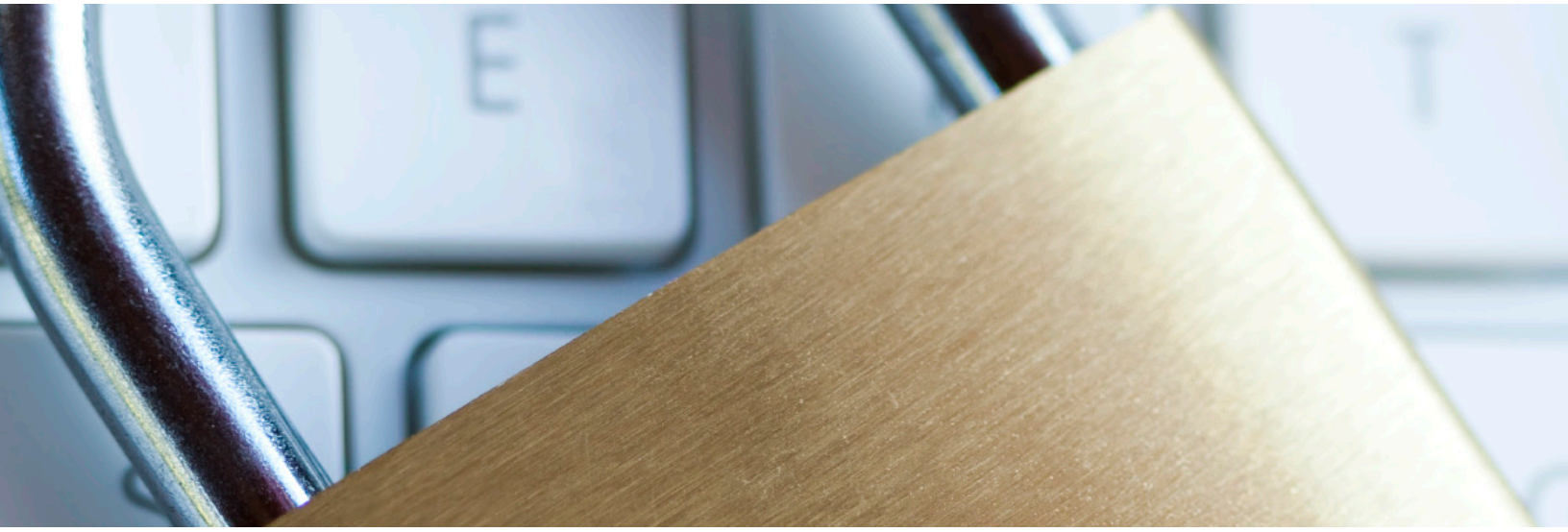
Frank Cowan Company



# Creating a Data Backup and Disaster Recovery Plan

This guide is intended to assist you in creating a Data Backup and Disaster Recovery Plan by providing the necessary background and context. A Data Backup and Disaster Recovery plan should be part of your overall Disaster Recovery and Business Continuity Master Plan. The Master Plan will address all of the systems and resources required to operate your business in the event of a disaster or under other adverse conditions that would prevent normal business operations.

1. **The critical role of data in business operations:**
   a. Every organization needs a comprehensive Disaster Recovery Plan that:
      i. Identifies the critical business functions that could be affected by a disaster.
      ii. Identifies the resources that must be preserved or recovered in order to restore business operations after a disaster.
      iii. Documents action plans for how those resources will be restored.
   b. A comprehensive Disaster Recovery Plan includes planning for areas including human resources, physical resources, information resources, and external systems, such as power and communication channels.
   c. Protecting business data is second in importance only to protecting life. Buildings, fixtures, machinery, computer hardware, and computer software can all be replaced. Data cannot, and thus requires special protections.
   d. This is not a comprehensive Disaster Recovery Plan. The scope of this plan is restricted to those processes required to recover “electronic data” which includes any documents or other records that are stored in an electronic form and are required for effective business operations.
   e. Although this Data Backup and Disaster Recovery Plan pertains to electronic data, some organizations also maintain physical records. These are generally paper documents. Physical documents are beyond the scope of this Plan. If physical records are important to your organization, a process for preserving them should be documented in a separate policy.
      i. By definition, there can be only one “original” document. If it is destroyed, recovery is not possible. However, it may be possible to create physical copies for disaster recovery purposes.
      ii. Electronic copies of physical records are considered electronic data and would be included in the Data Backup and Disaster Recovery Plan.
2. **All digital copies of electronic data are identical:** Electronic data that is digitally encoded can be duplicated and any number of copies may exist. All copies are identical and there is no differentiation for any legal or other purpose between existing copies.

3. **Risks to electronic data:** Threats to electronic data can be placed into 3 categories:
   a. Data confidentiality – data confidentiality is violated when information is viewed or accessed by a person or process that is not authorized to do so.
   b. Data integrity – Data integrity is violated when the data is altered by a person or process that is not authorized to do so.
   c. Data Availability – Data availability is violated when persons or processes that are authorized to view or access data cannot do so when required.
4. **The role of disaster recovery in a business risk management plan:**
   a. Your organization should complete a risk assessment and create a Cyber Risk Management Plan to address all threats to the confidentiality, integrity, and availability of electronic data. This Backup and Disaster Recovery Plan is one component of Cyber Risk Management Plan.
   b. This Disaster Recovery Plan is primarily intended to address data availability in the event of a natural disaster or other unanticipated failure. Your organization needs to create other policies, procedures and controls that address data confidentiality and data integrity, as well as other business risks.
   c. Although disaster recovery addresses risks to data availability, the recovery processes must be designed and implemented in such a way that data confidentiality and data integrity are not compromised.
   d. Data is often unusable unless the systems required to process the data are available. If line-of-business applications or systems are required to make the data usable, you must also create an Information Systems Business Continuity Plan.
5. **Data backup – the 3-2-1-A rule:**
   a. Electronic data can be damaged or lost as a result of human error, external events, or device failure. The MINIMUM requirements to protect data from these threats are:
      i. AT LEAST **3** updated copies of the data must be maintained.
      ii. Copies must exist on AT LEAST **2** physical devices in order to protect against device failure
      iii. AT LEAST **1** copy must be maintained "off-site". That is, in a geographically separate location that would not be affected by a fire or weather affecting the location where other copies are maintained.
      iv. Backup processes must be executed **A**utomatically. If the backup process depends upon someone remembering to initiate backups at the proper times, there will inevitably be failures.
         1. Automatic backup processes should, at a minimum, include notification of failures.
         2. There some failures that will include failure of the notification system. Therefore, monitoring for expected backup "success" notifications should be implemented whenever possible.
6. **Defining data sets:**
   a. Determine which folders contain data that must be backed up. This must include any files or documents that are created by users or by applications.
   b. Folders with the same backup and recovery requirements should be combined into data sets. The data sets that are directly accessed by users or applications are the "production data sets". Backup copies of the production data sets are "backup data sets".
   c. Database files:
      i. Unlike most documents, database files are constantly changing. Maintaining the integrity of database files requires special processes. Therefore, database files should be identified separately to ensure that the proper processes are applied. In many cases, proper database file backup can only be achieved by using the vendor's backup process. The resulting files should then be backed up as part of the regular backup routine.
7. **Data backup confidentiality and integrity controls:**
   a. Confidentiality controls:
      i. When confidential data is backed up, the same access controls that apply to the production data sets should be applied to the backup data sets
      ii. Encryption of backup sets: Most backup software provides an option to encrypt the backup data sets. When backing up confidential data, encrypting is generally best practice. However, there must also be a process for securely storing the encryption keys (usually a password) and ensuring that it is available and can be applied during the restore process. A lost encryption key will generally render a backup data set useless.
   b. Integrity
      i. File integrity controls (checksums, hashes, etc.)
      ii. Database integrity controls

8. **Data backup vs. data replication:**
   a. Data replication and data backup have different purposes. Proper protection of your data may or may not require replication, but will always require data backup.
   b. Data replication is essentially creating a "mirror" of the data. Changes made to the production data are replicated to the "mirror" at specified intervals, or in as nearly to real time as possible.
      i. Replication is used to maintain a copy of the data set in the most current version possible.
      ii. Replication is NOT a substitute for data backup. Events that would damage the production data set, such as file corruption and inadvertent deletions, are typically mirrored in the replicated data as well. Replication does not provide an option for restoring data to a previous known state.
   c. Data backup is used to create the ability to restore data to a previous state. A data backup set is a point in time "snapshot" of the data. The backup data set is not affected by any subsequent changes.

9. **Backup types:**
   a. Backups are generally classified as full, differential, or incremental. Backups are also either done at the file level or at the storage device "block level". The type of backup determines the time required to complete the backup and the storage requirements. Some backup types depend on a "backup chain". If any link in the chain is broken (e.g. a file is corrupt), then all subsequent backup points in that chain are unusable. Details regarding the most effective use of these backup types are beyond the scope of this document. The person(s) responsible for planning and implementing the backup plans MUST have a thorough understanding of these backup types and how to implement them.

10. **Backup data set locations:**
   a. As per the 3-2-1-A rule described above, critical business production data sets must ALWAYS be copied to AT LEAST 2 locations, with one of them being "off-site".
   b. As per the "Backup data confidentiality and integrity controls section above, access to ALL data backup locations must be controlled.
   c. When backup sets are being transmitted over local or wide-area network connections, consider:
      i. Security. Use secure, encrypted connections when transmitting confidential information.
      ii. Bandwidth requirements. In order to minimize the amount of bandwidth consumed by the transfer of backup data sets, it may be possible to:
         1. Implement backup methods that use or generate smaller backup data sets, such as incremental and/or block-level backups.
         2. Save backup sets to local disks during business operating hours and then copy those backup data sets to off-site locations over slower wide-area connections during non-business hours.
         3. In either case, the increased risks of data loss should be balanced against the need to conserve bandwidth.

11. **Data backup interval:**
   a. The interval at which backups are conducted is determined by the amount of data loss that is tolerable. It is always reasonable to assume that all data entered, updated, or processed since the most recent backup will be lost. Thus, if the maximum tolerable data loss is 1 hour, backups must be conducted on an hourly basis.

12. **Data retention policies:**
   a. Each data set must have an associated Data Retention Policy. This policy documents the number of restore points that must be maintained. In order to address storage space limitations, these restore points are typically consolidated after a specified period of time. A typical data retention policy would look something like this:
      i. Hourly restore points are retained for XX days, and are then consolidated into a single restore point for each day.
      ii. Daily restore are retained for XX days, and are then consolidated into single weekly restore point.
      iii. Weekly restore points are retained for XX weeks and are then consolidated into monthly restore points.
      iv. Monthly restore points are retained for XX months
   b. The data retention policy should be determined by the business needs for access to data.

13. **Data restore testing:**
   a. File restore testing must be done periodically to ensure that the process can be completed successfully. After all, what your business needs is really a data RESTORE solution, rather than a data backup solution.
   b. Database testing must be done as a separate process. Simply restoring a database file does not ensure its internal integrity. It is necessary to mount the database file in the application that uses it in order to test functionality.