

Disaster Planning and Identity Theft



3. Determine who will be the Disaster Recovery Planning Team Project Manager.
4. Identify at a high level a list of systems that should be considered in scope for this project.

IN SCOPE SYSTEMS, SOFTWARE & LOCATIONS	OUT OF SCOPE SYSTEMS, SOFTWARE & LOCATIONS

Disaster Planning and Identity Theft



9. What is at risk as a result of our vulnerabilities?

10. What must be done to eliminate the vulnerabilities?

Critical Services

Create a list of the IT services that are critical to the continuity of your business. Describe how these services are maintained and what type of redundancy is in place for them.

Some examples of these services include Internet connectivity, e-mail, file access, power, and phone.

CRITICAL SERVICE	MAINTENANCE	REDUNDANCY

Disaster Planning and Identity Theft



Passwords / User Accounts

1. Does policy require unique accounts (no 'guest' accounts)?
2. Are users required to change their password on a regular basis (30-60 days)?
3. Does the policy prevent users from reusing previous passwords?
4. Are requirements in place that force the password to contain a combination of numbers and letters? *Note: You may also want to avoid using common dictionary-based words in passwords as password crackers tend to look for these first.*
5. Does IT change server or main systems passwords on a regular basis?

Disaster Planning and Identity Theft



Internet Use and E-mail

1. Are their policies in place to outline and restrict user access to the Internet? If so, briefly describe the policy. If not, outline why no policy is in place.
2. Is employee Internet use being monitored and are the monitoring system logs being reviewed on a regular basis?
3. Is content filtering in place and active?
4. What, if any, restrictions are placed on e-mail? E.g. attachment size, file type restrictions, etc.

Anti-virus

1. Is antivirus deployed on all servers, workstations, and laptops?

Disaster Planning and Identity Theft



Documentation

1. What documents are presently in place to support a disaster recovery plan? Some examples include system policies, contact lists, network documentation, recovery plans, etc.
2. When was the last time that these documents were reviewed? How frequently are they reviewed?
3. Who is responsible for all of the documentation and what security measures are in place to prevent unauthorized access and changes?

Network

1. Is there a well documented network configuration and architecture?
2. Do all of the network devices and components conform to policies and architecture?

Disaster Planning and Identity Theft



2. Is penetration testing performed by a qualified third party organization?

3. How are the results of penetration testing handled? Who is responsible for performing risk assessment and prioritization?

Disaster Risk Analysis

1. What constitutes a disaster?

2. What type of disasters may your systems encounter? *Some examples include loss power, viruses, data deletion, hardware failure, fire, physical security, floods, storms, civil unrest, sabotage, labour disputes.*
3. What is the likelihood of such a disaster occurring? For each identified disaster, determine if there is a high, medium or low probability that this type of a disaster will occur.

DISASTER DESCRIPTION	RISK LEVEL	DISASTER MITIGATION
Electronic Security Breach		
Virus Infection		

