

IT Systems Risk Assessment

This self-assessment is designed to be filled out by the CFO or non-IT role accountable for IT within an organisation.

There are no right or wrong answers to these questions. The purpose is to assist the business assess whether the level of IT risk is acceptable.

The answer boxes will expand to accept multi-line answers.

Organisation (owner of IT systems)

Site

Date

Organisation responsible for IT (if outsourced)

Person(s) filling assessment

1. In regard to on-line data storage such as drives on servers available to users to store files:

a. At what rate are they filling up and when will it become a problem?

Down-time caused by storage filling up is common. Ideally, there should be some record of the rate at which this resource is being consumed so that clean-ups or upgrades can be planned before un-scheduled down-time occurs.

b. In the event that a disk volume fills up, when and how would it become apparent?

Ideally, storage systems are monitored automatically and an alert sent to the person responsible for operations when the available capacity falls below a certain threshold.

2. With regard to the physical disk drives in the servers:

a. If any single physical disk drive failed, would the servers keep working?

Single physical disks failing is common and the normal practice these days it to have all data stored on RAID arrays which can tolerate at least one physical disk drive failing without losing any data or causing un-scheduled down-time.

b. If/when a physical disk drive fails, when and how would it become apparent?

Although these array are tolerant to the failure of a single disk drive, a second disk drive failing will cause data-loss and down-time. Too frequently, the storage systems are not monitored; the first drive fails without anyone noticing, then another drive fails causing a major incident.

Ideally, the 'health' of the arrays and drives is monitored automatically with an alert going to an operations role which is staffed every business day at least and process ensuring that appropriate action is taken.

3. If the server hardware failed but the data remained intact on the physical disks:

- a. What would be the method of recovery?
You cannot take the disks out of one server, and put them into a different model, and expect them to work. You could be lucky, but this cannot be relied on. Ideally, there would at least be a hardware maintenance contract on the server which would ensure that the server hardware would be fixed/replaced in a reasonable amount of time; or a hardware identical device kept as a spare – all the way up to a fully operational disaster recovery site.

- b. How long before full services re-established?
If there is no standby hardware, down-time is likely to be about a week while new hardware is purchased, software installed and data recovered from tape. If anyone estimates less than this, consider insisting that their recovery plan be tested.

4. If the server hardware failed and all data on the physical disks destroyed:

- a. How much data would be irretrievably lost?
The answer here would have to relate to the frequency of backups. If they are daily and all is working, then the maximum likely data loss is one day.

- b. What would be the method of recovery?
Are their maintenance contract of the servers? Are there spare servers? Realistically, how long would it take to fix the servers, reload all software and recover data from tape. Once new hardware has been sourced, 60 hours for 2 to 3 servers is realistic.

- c. How long before full services re-established?
One week without IT is realistic in this scenario for a reasonable size SME without a disaster recovery site.

5. What would be the services impact and expected down-time if any one of the following device types were to fail:

- a. Ethernet switches

- b. Routers

- c. Modems

- d. Firewall appliances

- e. Wireless access devices

- f. Other devices

6. Are Firewall rules checked for applicability and integrity? If so how often?

7. If all equipment and media were destroyed in the server room:

- a. How much data would be lost irretrievably?

- b. What would be the method of recovery?

c. How long would it be before basic services were re-established (and what would those services be)?

d. How long before full services were re-established?

8. In regard to the backup system:

a. When was the last time a backup audit was done (checking that the appropriate data on the servers is being backed up)?

b. When was a test restore last done (checking that data can be brought back from tape or other backup system)?

c. What is the success rate of the backup task (how often does the backup task fail)?

9. If a user noticed that a file stored on the file server had become corrupted, could the file be restored to the original version if it became corrupt:

a. Yesterday?

b. One week ago?

c. One month ago?

d. Three months ago?

e. One year ago?

f. Two years ago?

10. In regard to email:

a. For how long does the organisation keep email messages?

b. In what form are the messages kept? (for example, in the users' mailboxes, files written to DVD)

c. If messages are archived, what systems are in place to perform/manage this?

11. In regard to the UPS (Uninterruptible power supply) system supporting the servers :

a. When was the UPS system's self test run?

b. When was the last time the UPS system was tested with an actual power cut to see that the batteries could last the time taken to cleanly shut down the servers?

c. When were the batteries last replaced?

12. If power was cut to the site for an extended period (hours or days), what actions would be taken?

13. If communications (land-line telephone and Internet) were lost to the site for an extended period, what actions would be taken?

14. Are there any disk drives in PCs (including laptops) which, if they failed destroying all data on them:

a. Would result in irretrievable data loss?

b. Would cause significant down-time (for example PCs which have a complex software configuration)?

15. In regard to keeping operating systems (eg Windows) up to date and secure:

a. Is there a Patch Management system in place for servers and PC's?

b. When was the last check done to ensure that the system is working and that all computers are current?

16. Regarding the anti-virus system:

a. Is there anti virus software on all PCs and servers?

b. Is the software and its updates current?

c. If a virus was discovered on a PC or server, who is notified and by what means ?

17. How is the anti-virus system checked to ensure that:

a. All PCs have the software installed and running?

b. All PCs have current version of the software and latest virus signature file?

18. If a user committed an offence with a web browser on one of the organisation's PCs and the authorities traced the offender back to the organisation, would we be able to identify the user?

19. Regarding user accounts on the systems:

a. Do all users have their own username/passwords, or are there cases where two or more users share the same account; either in the Windows domain or in other systems such as the accounting system?

b. Is there an authorisation process for granting users access to the systems?

c. Is there a process for removing user access once they leave?

- d. When was the last user account audit performed (checking that the enabled user accounts on the systems match the list of current authorised users)?

20. Regarding Internet domain names:

- a. How many names are in use by the organisation and what are they?

- b. When is the registration fee for the names due for renewal?

- c. Who will be notified when it falls due?

- d. Where are the Internet domain names hosted (not to be confused with web hosting)?

21. Regarding the key passwords for the systems?

- a. What are the key passwords? (for example one would be the Windows domain Administrator password)

- b. Where are the keys passwords stored?

- c. Who has access to them?

- d. What is the policy for disclosing them?

- e. When were these passwords last changed?

22. Regarding software licenses:

- a. Is there a central record of licenses owned?

- b. Where is this record kept?

- c. When was the last audit of software used (actually loaded onto PCs and servers) performed?

- d. When were the results of a software-used audit last matched with the record of licenses owned?

- e. If an audit of licenses in use had to be performed immediately, could it be done and how would it be done?

- f. If software needs to be renewed, are the dates known and who will ensure the renewals take place?

23. When was the last security audit performed?

24. In regard to Business Continuity Planning:

a. In there a Business Continuity Plan in place

b. Does it include an IT Disaster Recovery Plan

c. If so, when was the last recovery test performed?

Note: This document only suggests some questions to be considered. These questions assume a typical business with typical IT systems. This document does not exhaustively list the environments or systems which should be considered (or the questions which should be asked) in assessing the level of risk the systems pose to the organisation.