

Audit Trails and Disaster Recovery MS

13.6 Audit

1. Data must be recorded to enable auditing of ICT systems.

For each of the following examples, state **two** items of data and describe how they may be used in the audit of the system:

- (a) a company's stock control system; (3 marks)
(b) a company's network security system. (3 marks)

(a) Items of data . (any 2 x 1)

User ID/User Name/.user.

Function reference

Date & Time (Must have both)

Item Code/Stock code/Product code/Item of stock/.Item. (NOT name/description)

Quantity/No of items/Amount/How used (any 1)

to identify the ups and downs of stock usage/able to know when reorder level reached

to reconcile stock levels during a stock take

to identify who accessed the data, when and what for.

(b) Items of data . (any 2 x 1)

Logon ID/User ID/Name/.user.

Terminal ID/I.P.address/.Terminal./.Workstation.

Date & Time (Must have both)

Length of connections/Time spent logged on

Number of login attempts

Applications accessed

Data or Files accessed

CPU usage

Storage usage

How used (any 1)

to identify who was connected, when, where and for how long. For security control purposes/ to monitor for malpractice (allow hacking)

what system resources were accessed and used, for accounting purposes in a company that has internal accounting systems. (3 marks)(3 marks)

Total (6 marks)

13.6 Disaster recovery management

2. A growing organisation has realised that so far they have been lucky in that their information systems have not failed. Before they expand their business operational reliance on ICT, they have been advised by their insurer to carry out a risk analysis and then plan what to do next.

- (a) Explain what is meant by *risk analysis*. (3 marks)
(b) State **three** different potential threats to an information system, and describe a counter-measure for each one. (9 marks)
(c) Describe **three** of the criteria that could be used to select a disaster contingency plan. (6 marks)

(a) Any 3 × 1

(To identify each element of a successful information system (1)

(place a value – to the business – on that element (1)

(identify any potential threats to that element (1)

(the likelihood of the threat occurring (1)

(3 marks)

(b) 1 for threat(T), 1 for counter-measure(C), 1 for description of why/how it would counteract the threat(E). Any 3 × (3,2,1,0)

t. Physical – e.g. theft/terrorists – use locks etc – prevent easy entry

t. Personnel – e.g. accidental overwrite – have procedures – trained staff less likely to make mistakes

m

m. Communications breach – e.g. hacking in – firewalls, encryption, passwords – to lessen ability to see/steal/tamper with data

s. Virus – e.g. Trojan – anti-virus software – to stop files getting Infected

s. Natural disaster causing hardware/software/data loss – e.g.

Fire/flood/earthquake - backup kept off-site – so that a safe copy is held and system can be reloaded

r

as above

a. Data errors, inaccurate data in system – verification and validation – pick up data errors before they get into the system.(9 marks)

(c) 1 for criterion(C), 1 for description(E), Any 3 × (2,1,0)

(Scale of the organisation and its ICT systems

(

system would be operating, and if this is important to the business

s. Costs of recovery options relative to “value” of systems

s. Perceived likelihood of disaster happening, based on risk analysis

NOT:

N Volume of data

N Size of the system

N Any of the contents of the recovery plan (e.g. how to set up, reciprocal site, who does what or anything to do with back-ups)

(6 marks)

3. A medical practice, in an area prone to flooding, has carried out a risk analysis and is now preparing its disaster recovery plan. The main elements of its ICT system are the patient records and prescription systems, and the network used to access and maintain them.

(a) Explain what is meant by *risk analysis*. (3 marks)

(b) State **two** different potential threats to **this** ICT system, and describe a counter-measure for each one. (6 marks)

(c) Name **three** criteria that the medical practice should consider when preparing a suitable disaster recovery plan. (3 marks)

Any 3x1

A to identify each element of a successful information system (1)

place a value to the business on that element (1)

identify any potential threats to that element (1)

the likelihood of the threat occurring (1)

use an algorithm to calculate an overall risk figure (1)

that will indicate a degree of severity (1)

(b) 1 for threat (t), 1 for counter-measure(c), 1 for description of why/how it would counteract the threat(e). Any 2x (3,2,1,0)

Candidate does not need to have the threat to get the other two mark; however, if a valid threat is offered, then no credit to non-matching countermeasure and expansion.

Two countermeasures for one threat can gain both (c) and (e) marks

Threat

Counter measure

(examples)

Example/expansion

(examples)

Natural disaster. e.g. flood, earthquake

backup kept off-site;

hardware kept above flood-line;

so that a safe copy is held and system can be reloaded;

Electrical surge/power loss UPS/ RAID/ off-site duplication/ Mirror as above

Physical . e.g. theft use locks etc prevent easy entry

Personnel . e.g. accidental overwrite

have procedures trained staff less likely to make mistakes

Hardware . e.g. disk crash have duplicate system/

hot site arrangement so that system can be up and running a.s.a.p

Communications breach . e.g.

hacking in

firewalls, encryption,

passwords to lessen ability to see/steal/tamper with data

Virus . e.g. Trojan anti-virus software to stop files getting infected

Data errors, inaccurate data in system verification and validation

pick up data errors before they get into the system

(c) Any 3 x 1

(Scale of the organisation and its ICT systems/Volume of data/Size of the system

(Nature of the operation / The importance of data held

(Timescale until the system is up and running

(Costs of recovery options relative to .value. of systems

(Perceived likelihood of disaster happening, based on risk analysis

NOT: Any of the contents of the recovery plan (eg how to set up, reciprocal site, who does what or anything to do with back-ups)