

DCMS Business Continuity Planning for Sponsored Bodies – Workshop 2 – Example Exercise Answers

Example Answers for Exercise 2 – Possible Risk Reduction Controls

To mitigate the risks to IT, including communications, systems ensure that:

- as far as possible only authorised users have access and then only to that to which they are authorised, minimising the chances of a successful attack causing failure. Consider:
 - identification and authentication (I&A) controls such as good quality and length user identifiers and passwords - regular enforced password change on a monthly basis, tokens for remote connection (+ ensure passwords stored in encrypted form),
 - good quality logical access control mechanisms controlling users to their authorised areas and in terms of the privileges they can use (e.g. read only, read and write),
- unauthorised events can be quickly detected and dealt with. Check facilities currently in place to see that there:
 - is ongoing use of audit logs (trails) set up to track events to a person, what they did, when and to what etc., with the setting of alarms/alerts if certain events occur,
 - are good audit log analysis tools available and that they are regularly used,
 - is protection afforded to the audit logs and related analysis files,
 - are procedures etc. set in place to review alerts/alarms, logs and their analysis, and speedily deal with identified incidents,
- data thought to have been deleted (not achieved by just hitting the delete button) is indeed dealt with by security deletion facilities and associated procedures,
- the anti-malicious software in place is regularly and automatically updated to ensure that viruses, etc., can be prevented, or detected and removed, and that associated procedures are in operation,
- proper I&A and logical access controls are used to control remote working, and that those people with equipment for remote use are instructed on the security required of that equipment when away from the normal workplace,
- adequate network management facilities and procedures are in place. This includes facilities to constantly monitor the status of the network and early detection of unauthorised use or failure, and the network design including mechanisms for minimising the effects of any disruption to services and applications,
- the firewall facilities are of the approved type and that there is proper documentation of the rule bases, etc., which is subject to good change control facilities and procedures – including for back up,

DCMS Business Continuity Planning for Sponsored Bodies – Workshop 2 – Example Exercise Answers

- content scanning facilities are in place, e.g. to detect unauthorised e-mail messages and content, and check web sites visited and web content,
- controls are in place to detect and control Spam messages,
- mobile code protection is maintained, with facilities to protect end systems against hostile code that may be present on web sites visited, controls over what files users can download from external sources, and controls to prevent external people from tracking which sites users have visited previously,
- the network is protected against denial of service attacks, and that facilities and procedures are in place that will make network personnel aware of such attempts,
- adequate controls, facilities and procedures, are in place for IT including network operations – including for fault logging, monitoring of activities and fully documented procedures (including to prevent errors!), for system administration, and, if relevant, application development and programming,
- adequate controls, facilities and procedures, are in place for software and hardware maintenance, and indeed for users (including to prevent errors!),
- adequate controls, facilities and procedures, are in place for application input and output, and for financial accounting,
- adequate controls, facilities and procedures, are in place for documentation and media, including for storage and proper destruction,
- effective back-up procedures and related facilities, technology, etc. are in place,
- good protection is afforded for the private branch exchanges.

To mitigate the risks not just to IT, including communications, systems, but also other facilities, services, collections, etc., ensure that:

- there is control of physical access to, and thereby making physical ‘attacks’ more difficult on, the two locations, including with:
 - solid external doors with ‘approved’ locks and fitments,
 - good construction external windows and fitments – with ‘approved’ locks on low level floors,
 - good security lighting,
- there is control of physical access to, and thereby making physical ‘attacks’ more difficult on, rooms and areas within the locations to which the public are not permitted entry, with:

DCMS Business Continuity Planning for Sponsored Bodies – Workshop 2 – Example Exercise Answers

- for such as the IT rooms, good room/area design - strength and structure of the walls, floor and ceiling,
 - appropriate 'solidity' of doors, fitments and locks,
 - 'electronic' physical access control systems,
 - controls over keys and their storage and distribution,
- protection is in place to prevent and detect theft,
 - collection items and equipment are sited to protect them from possible environmental threats,
 - secure storage is available for such as laptops,
 - terrorist/extremist warnings and attacks can be effectively dealt with,
 - the fire prevention, detection and suppression facilities are checked regularly, and written assurance is gained from the local fire brigades on the required response times, and that good documented procedures are in place, including for evacuation,
 - the water/liquid/flood protection facilities are checked regularly, and good documented procedures are in place,
 - the environmental protection in place is checked regularly,
 - adequate protection against natural disasters (other than fire and flood) is afforded commensurate with that to be protected, including protection against lightning strike,
 - adequate power protection is afforded commensurate with that to be protected, with effective installation procedures documented, power resilience, power conditioning facilities and emergency procedures,
 - good personnel procedures are in place to reduce the risk of having a 'rogue' member of staff, with such as focused recruitment screening, terms and conditions of employment, security and business continuity aspects in job descriptions, (without 'going overboard') management 'monitoring' of staff, recognised disciplinary process, and regular security, including business continuity, awareness material/briefings for all personnel and training for appropriate people,
 - adequate security documentation is in place and regularly updated, e.g. high level and detailed security policies (the detailed policy including a summary of the risks, and a detailed list of all security controls required commensurate with the assessed risks),
 - an adequate security/business continuity organisation infrastructure is in place with documented terms of reference and responsibilities,

DCMS Business Continuity Planning for Sponsored Bodies – Workshop 2 – Example Exercise Answers

- as relevant, security/business continuity requirements are documented in third party contracts,
- an effective incident reporting and handling scheme is in place, with documented procedures, responsibilities, forms, etc., including coverage of learning from incidents and how they were handled.