



Business Continuity Management

Installation Management Review

1. Introduction

Installation Management Reviews are carried out to help clients assess the effectiveness of controls and security within all areas of their IT environment and the service it provides to users. They are intended to highlight any potential risks to the client's business operation which may arise from lack of controls or ineffective operational practices in their IT activities.

Reviews can be carried out in any size of IT operation, and in all business sectors. The length of time taken to carry out and report on a review will depend on the scope required by the client. This will usually be the IT Manager, but a review may be requested by senior management.

2. Scope

All reviews are tailored to suit the size of the client's IT operation and business activities. This includes allowance for the existence of any corporate standards which must be complied with in the client's IT environment. If necessary, the review will comment upon the effectiveness and suitability of any such standards, in relation to the client's IT activities.

There are three levels of review. All cover the same topics, but each progressively goes into greater depth, dependent upon the purpose of the review requested by, and agreed with, the client. Each level generally involves more of the client's IT personnel, and possibly users, to get a more detailed picture of the operation. If any points are highlighted for concern in a level 1 review, the client should decide whether a further review in more depth is necessary.

The time planned for each review allows for a close-out meeting with the client at the end of the visit. This meeting is intended to provide an immediate summary of results and to highlight areas of concern, enabling the client to take any corrective action with a minimum of delay.

Each review is followed by a written report to the client. This includes an executive summary and also outlines the scope of the review and the areas covered. The points highlighted during the review are categorised as :

- Critical and needing immediate attention ("show-stoppers" or "red lights")
- Of concern but not exposing the operation to immediate risk ("amber")
- Minor points which should be addressed in the "normal" course of planning ("green").
- Observations (e.g. potential future exposure(s) which may arise as a result of planned changes discussed during the review)

The scope of any follow-on work should be the subject of a separate agreement.

3. Summary of Review Levels

Level 1

This generally will be a 1 day assessment of the IT environment at one location, involving the IT Manager and other key players. The review topics are covered in top level outline only. This "Health-Check" allows the client to get an overall opinion on how effectively and securely the IT operation is managed, and highlights obvious areas of concern.

Level 2

This will usually be specifically scoped, covering specific topics which the client wishes to have reviewed, possibly arising from a Level 1 review. Timing is dependent upon scope of the review and the size of the installation. Topics are covered in the same detail as for a Level 3 review.

Level 3

This is the most detailed review, in which we will “drill down” to the cause of any problems identified. At some point during the review process, we would also include discussions with IT management, and appropriate staff, to identify methods of reducing highlighted risks and the most suitable corrective action to improve areas of weakness.

The time to be taken to complete a level 3 review will be agreed with the client.

4.Procedure

Although individual reviews are unique, each one follows the same general pattern, unless the client wishes for a “snapshot” review to be carried out within a timescale which precludes detail planning activities beyond agreeing the scope and timing.

- Agree scope and timing of the review with the client (level, areas to be covered, visit dates, etc.)
- Opening meeting at the start of the review visit to clarify the purpose and scope. Where possible, this should be attended by IT departmental or section managers involved in the review, and the client, if this is not the IT Manager.
- Review (with planned appointments if other personnel are involved).
- Close-out meeting to summarise the results of the review. Where possible this should be attended by the same personnel as in 2 above.
- Written report to management (usually within five working days).

If the client requires any follow-up action to assess progress, this can be scheduled.

Decisions on the choice of corrective action(s) to resolve potential exposures highlighted during a review must always be taken by the client, who is best placed in terms of knowledge of the specific business requirements, strategies and budgetary constraints.

5. Review Topics

The following is a summary list of the topics covered by the review. Each topic has its own detailed sections which are reviewed to ensure that we understand the nature of the operation and the activities being carried out (or not).

This is not necessarily the order in which topics are reviewed. This is dependent upon the scope of the review, the size and organisation of the IT operation and, in more detailed reviews, the availability of key personnel.

- IT services and criticality to business operations (IT, management and user perspectives)
- IT policies and standards (eg if part of a corporate group which sets standards which must be complied with)
- IT organisation and responsibilities (to assess management structure, resources)
- Use of, and dependence upon, external resources.
- User support (eg help desk problem reporting and escalation procedures)
- Physical environment and vulnerability (eg work areas, safety, intruder / fire security)
- Disaster planning and recovery
- System security (eg access controls / system security)
- Data security (eg back ups, restore/rerun authorisations)
- Systems development activities and controls (life cycle, authorisations, etc.)
- Computer operations activities (scheduling, event logging, etc.)
- Communications / network (LAN /WAN) controls and security
- PC controls and security (access and data security, virus prevention and/or detection, etc.)
- Documentation (hardware, software and applications systems)
- Installation management and controls (internal / external audit, hardware / software acquisition controls, capacity planning, management reporting, training and personnel development, etc.)
- Information Security Standards Compliance, if appropriate.



contact

Pentire Solutions Ltd
4 Queens Crescent, Burgess Hill, West Sussex, RH15 9EU
Tel. +44 (0)1444 257088
www.pentire.co.uk

To find out how Pentire Solutions can help you address your business continuity management challenges, email us at pentireinfo@pentire.co.uk