



NAO Form 905

Review of Information System Controls

Notes and supplementary questions

Version 2.3, February 2004

TABLE OF CONTENTS

INTRODUCTION	1
WHY DO IT? THE RELATIONSHIP BETWEEN INFORMATION SYSTEM AUDITING AND FINANCIAL AUDITING.	1
PLANNING A CONTROL REVIEW	2
PART 1: CHANGE AND CONFIGURATION MANAGEMENT.....	6
CHANGE MANAGEMENT	6
CONFIGURATION MANAGEMENT	6
EMERGENCY CHANGES	7
AUDIT IMPLICATIONS	7
SUMMARY OF RISKS	8
SECTION 1: SUPPLEMENTARY QUESTIONS	9
<i>Control objective 1.1: changes to IT systems should be controlled on the basis of documented change management procedures</i>	<i>9</i>
<i>Control objective 1.2: Requests for Change should be documented, authorised and recorded</i>	<i>9</i>
<i>Control objective 1.3: Requests for Change should be reviewed to identify consequential risks to the correct operation of the system.....</i>	<i>9</i>
<i>Control objective 1.4: system changes should be appropriately authorised</i>	<i>10</i>
<i>Control objective 1.5: change management procedures should pay due regard to an effective separation of roles.....</i>	<i>10</i>
<i>Control objective 1.6: authorised changes should be managed to completion</i>	<i>10</i>
<i>Control objective 1.7: emergency changes should comply with normal change management requirements as soon as possible</i>	<i>11</i>
<i>Control objective 1.8: changed components should be fit for business use.....</i>	<i>11</i>
<i>Control objective 1.9: configuration management records should accurately describe the live configuration and its status history</i>	<i>11</i>
SECTION 2: INFORMATION SYSTEM OPERATIONS AND MAINTENANCE	12
COMPUTER OPERATIONS	12
RECRUITMENT, TRAINING AND OPERATING PROCEDURES.....	12
SEPARATION OF ROLES	12
AUTHORISATION OF WORK RUN ON THE INSTALLATION	13
DATA INPUT	14
MANAGING FINANCIAL STATIONERY	16
COMPUTER OUTPUT.....	16
MANAGING SYSTEM BACKUPS.....	17
REPORTING AND MANAGING INCIDENTS	18
DATABASE ADMINISTRATION	19
SUMMARY OF RISKS	21
SECTION 2: SUPPLEMENTARY QUESTIONS	23
<i>Control objective 2.1: Computer operations should be performed competently</i>	<i>23</i>
<i>Control objective 2.2: Incompatible roles should be separated to the extent practicable.....</i>	<i>23</i>
<i>Control objective 2.3: all system operations should be authorised and serve legitimate business needs.....</i>	<i>24</i>
<i>Control objective 2.4: data input for processing should be valid, complete and accurate.....</i>	<i>24</i>
<i>Control Objective 2.5: Financial stationery should be stored securely and its use accounted for</i>	<i>24</i>
<i>Control objective 2.6: outputs should be complete and accurate, and distributed promptly to the correct recipient</i>	<i>25</i>
<i>Control objective 2.7: system backups should be readable and their use accounted for</i>	<i>25</i>
<i>Control objective 2.8: the level of service provided should be consistent with business needs.....</i>	<i>25</i>
<i>Control objective 2.9: there should be a focal point for reporting, recording and resolving incidents and operational failures.....</i>	<i>25</i>
<i>Control objective 2.10: Data stored within multi-user databases should be reliable and available for use when required.....</i>	<i>26</i>

SECTION 3: INFORMATION SECURITY MANAGEMENT.....	27
INTRODUCTION.....	27
INFORMATION SECURITY POLICY AND ORGANISATION.....	27
AUDITABILITY.....	28
RISK ASSESSMENT.....	29
PERSONNEL SECURITY.....	29
PHYSICAL AND ENVIRONMENTAL SECURITY.....	29
LOGICAL ACCESS.....	30
SOFTWARE CONTROL.....	30
BUSINESS CONTINUITY.....	31
SECTION 3: SUPPLEMENTARY QUESTIONS.....	32
<i>Control objective 3.1: Top management should set a clear direction and demonstrate their support and commitment for information security by defining a corporate information security policy.....</i>	<i>32</i>
<i>Control objective 3.2: A management framework should be set up to implement information security within the organisation.....</i>	<i>32</i>
<i>Control objective 3.3: the operation of the system of controls should be auditable.....</i>	<i>32</i>
<i>Control objective 3.4: the system of controls should be appropriate to the type and level of risks to be managed.....</i>	<i>33</i>
<i>Control objective 3.5: security should be addressed in recruitment and leaving procedures, and in contracts and job descriptions. It should also be monitored during employment.....</i>	<i>33</i>
<i>Control objective 3.6: ICT facilities should be located in secure areas.....</i>	<i>33</i>
<i>Control objective 3.7: ICT facilities should be protected from environmental risks.....</i>	<i>34</i>
<i>Control objective 3.8: access to computer systems and data should be controlled on the basis of business needs.....</i>	<i>34</i>
<i>Control objective 3.9: there should be controls to prevent and detect the introduction of unauthorised software.....</i>	<i>34</i>
<i>Control objective 3.10: business continuity plans should be available to protect key business processes from the effects of major disruptions, failures and disasters.....</i>	<i>35</i>
<i>Control objective 3.11: information security should be reviewed regularly for compliance and effectiveness.....</i>	<i>35</i>
APPENDIX: THREATS TO GOVERNMENT IT SYSTEMS (SOURCE: CRAMM).....	36

Workbook: Review of Information System Controls

Introduction

*This workbook follows the NAO Form 905. It is intended to provide a commentary on the various aspects of control that are dealt with in the Form and to provide examples of more detailed questions that the auditor (or client) may need to consider in establishing whether particular control objectives have been met. **The NAO 905 and workbook provide a framework within which to work rather than a prescriptive checklist.***

Queries should be addressed to Ian Petticrew.

Why do it? The relationship between information system auditing and financial auditing.

1. The relationship between financial and information systems auditing is not clear-cut and has been the subject of much debate since computerised financial systems were first used in government.
2. The relationship between the outputs from a review of information system controls and those from other aspects of financial auditing is indirect; they have different, albeit related objectives. Financial auditing aims to assess the extent to which an organisation's financial statements are properly presented and reliable. Information systems auditing aims to assess the extent to which the data processed in a financial system, and from which the financial statements are drawn, are likely to be reliable. In the former the audit criteria are contained in Statements of Auditing Standards; in the latter they are a set of, as yet informal, system control objectives (the NAO Form 905 is based on those aspects of the British Standard for Information Security Management - BS 7799 - that apply to financial auditing).
3. Failure of a system to meet one or more control objectives does not mean the failure of one or more financial audit assertions, or that the client's financial statements are unreliable. It is merely an indicator that the system in question is more vulnerable than might be the case, to threats that could adversely affect the reliability of its data. Whether the data is unreliable as a result can only be established by testing it, which can be an expensive process. In a paperless system testing the reliability of the data (i.e. the audit evidence) could prove difficult (if not impossible) due to the absence of any paper source documents against which to test. ***In a paperless system effective auditable controls over data integrity (completeness, validity & accuracy) are therefore essential.***
4. To better understand the relationship between information systems and financial auditing, one must consider the nature of "risk" as it affects a computerised information system. Within this context, risk is widely regarded to be a composite measure of three factors:
 - **Threats:** are undesirable events such as fire, software error, hacking (or "system infiltration") and computer virus. Over 30 classes of threats are generally recognised to affect information systems (see Appendix);
 - **Vulnerabilities:** are weaknesses that can be exploited by threats to cause damage;
 - **Impacts:** are measures of the severity, expressed in business terms, of the consequence(s) of a threat exploiting a vulnerability and resulting in damage.
5. Each of these factors can be assessed separately and a rough measure produced on a sliding scale; for example *high, medium* or *low* or perhaps a more extensive scale of, say, 1 to 5 might be employed. It follows that where there is no perceived threat there can be no corresponding risk. Similarly, if there is a high probability of a particular threat

Workbook: Review of Information System Controls

exploiting a vulnerability, but the business consequences of the resulting impact are negligible, then the overall risk must also be low.

6. It may be possible to reduce or remove a threat (e.g. the threat of external hacking is removed by not connecting to external networks) or an impact (e.g. removing sensitive data from systems connected to external networks reduces the potential impact of external hacking). However, control reviews do not include the complexities of systematic threat and impact analysis; instead, the emphasis is placed on reviewing the extent to which vulnerabilities to common threats are managed using a range of *better practice* controls.
7. Financial systems that exhibit a low vulnerability to the range of threats that can damage the integrity of financial data are less likely to contain unreliable data than systems that are highly vulnerable. To the extent that unacceptably high vulnerabilities exist, the auditor may recommend to the client various ways in which these might be reduced. Should either the levels of vulnerability remain unacceptable, or the correct and consistent operation of controls for reducing them be impossible to verify, the established practice is to place no reliance on controls and instead adopt an audit approach based on testing paper-based transactions. This may be satisfactory in situations where acceptable audit evidence is available in paper form, but where source transactions only exist in electronic form, an unsatisfactory control review may have a direct impact on the audit opinion. *If the auditor is unable to establish confidence in the reliability of a client's electronic evidence, then its use as audit evidence should be qualified to that effect.*
8. These are important factors that the auditor should bear in mind when conducting a control review, and particularly when making recommendations to a client. Controls can be expensive to install and operate, and the overhead they impose can reduce operational efficiency. They should therefore be appropriate to the nature and level of risk involved.
9. The objectives of a control review are to:
 - understand and record the client's system for processing financial transactions and producing financial statements for audit;
 - review the client's approach to:
 - assessing and managing risks to their financial information systems
 - obtaining evidence of effective control operation;
 - make recommendations to the client for managing poorly controlled risks;
 - based on the adequacy and auditability of controls, determine whether a controls reliant audit approach is feasible and if so, draw up a compliance testing programme.

Planning a control review

10. In common with any other type of audit, information systems auditing requires planning if its objectives are to be met efficiently and with minimum disruption to the client's business activities.
11. Planning an information system controls review involves contacting those responsible for the various aspects of system management to arrange interviews and obtain system documentation for examination. Initial discussions with the client together with a review of the system documentation will help the auditor to:
 - explain to the client the purpose of the review and its scope, and obtain co-operation;
 - understand:
 - *how the target system operates and is managed;*

Workbook: Review of Information System Controls

- *the information security risks that are likely to exist (which may differ from those addressed on the NAO Form 905);*
 - identify any technical problems that will require assistance from an IT Audit Group member or from an external consultant via the IT Services Catalogue (“S-CAT”).
12. One does not have to go back far to the time when computers were operated by a central team, and both data capture and output distribution were important aspects of their work. Planning a control review was comparatively straightforward because control was centralised. Later developments streamlined data processing. System users were provided with terminals and printers to perform input/output for themselves. The advent of the personal computer and client/server technology diminished the role of central operations still further by enabling system users to control many aspects of computer operation and with the aid of query languages, spreadsheets and databases, develop some of their own applications. Nowadays it is not unusual to find many operational activities performed by an external contractor under the terms of an outsourcing or PFI contract.
13. These developments make it sometimes difficult to attribute traditional computer operations functions and to identify in advance the most appropriate people to interview. Large mainframe systems that support specialised applications (e.g. taxation) are still likely to have a central group who perform many of the traditional system development and operations roles. However, in mid-range and small systems, bespoke applications have generally given way to off-the-shelf software packages, thus reducing the application development role to one of change management, whilst many operational tasks are likely to be performed by an IT literate end-user, often described as the “Systems Administrator”.
14. Thus when planning a control review of an unfamiliar system it is important to obtain guidance from or via your liaison point (generally the Head of Finance) in regard to the allocation of IT roles and responsibilities and where those involved in discharging them are located (which might not be in the same geographical location as the system’s users).
15. The broad areas of activity that is covered in an NAO Form 905 review, and in which interview are likely to be required, are: -
- **computer operations** : traditionally this covers the following activities :-
 - *starting up, shutting down and operating computers (other than PCs) and networks;*
 - *software, hardware and network problem investigation and resolution;*
 - *producing and distributing centrally produced computer outputs;*
 - *operating “batch” (or “background”) jobs;*
 - *backing up the system and management of off-line files (tape cartridges, laser discs, etc);*
 - *installing new and amended software;*
 - *providing a help desk service for recording and allocating problems (hardware, software, communications) for resolution, and expediting outstanding problems;*
 - **operating system administration**: sometimes referred to as “system programming”, it mainly involves installing, configuring and maintaining the operating system, and controlling its use (e.g. maintaining user accounts and controlling their access permissions);
 - **network administration**: the administration of internal (LAN) and external (WAN) networks, interfaces with public networks, firewalls and intrusion prevention and detection systems where these are used (in small departments this function might be performed by the same team that handle operating system administration);
 - **database administration** : installing and maintaining multi-user databases;

Workbook: Review of Information System Controls

- **data capture** : capturing source data for input to computer application systems (e.g. bills, benefit claims, time sheets)
 - **output distribution** : the production and distribution of computer outputs (e.g. cheques, pro-forma letters and forms, printouts, magnetic tapes);
 - **application system development and maintenance** : developing new applications systems; maintaining existing application systems including the development and maintenance of internal and external web site applications;
 - **change and configuration management** : controlling and recording changes to application systems, and to the computer environment generally; auditing installed system components (i.e. hardware, software, communications equipment) against configuration management records;
 - **information security management** : maintaining information security policy; monitoring and investigating information security incidents; maintaining and testing the business continuity plan.
16. A detailed examination of the implementation of technical controls within the operating and network systems requires technical expertise, but is generally unnecessary for (and beyond the budget of) general financial risk assessment. If, for whatever reason, the auditor wishes to review the implementation of technical controls, the IT Audit Group should be consulted. In the absence of this, a system controls review is based on documentary examination. At the planning stage, the aim is to gain an understanding of how a system operates and is controlled. To the extent that the documentation complies with good practice, it might subsequently provide the criteria for compliance testing (e.g. to verify compliance with the client's change management procedures).
17. The documents that the auditor should seek to obtain at an early stage of a control review are:
- **the client's information security policy**: states management intentions regarding information security (which is what a system review is really about), and provides guidance on the allocation of security roles and responsibilities, and key security requirements to be met (e.g. unique passwords, virus controls, business continuity plans);
 - **high level system descriptions**: help gain an understanding of system operation (e.g. high level descriptions of system objectives and how these are achieved, schematic diagrams showing the flow of transactions, an overview of the network and its main components);
 - **catalogue of the main software components**: e.g. the operating system, database management system, off-the-shelf financial packages, security system (e.g. RACF, ACF2);
 - **operations procedures**: procedures for operating computers and networks, and individual applications systems;
 - **change management procedures**: procedures for managing systems changes;
 - **application user manuals**: the client's procedures for operating and controlling the application systems covered by the review (not to be confused with vendors' manuals, which cover operation of the software rather than the business use of the package);
 - **business continuity plans**: procedures for restoring key business systems in the event of prolonged failure or disaster;

Workbook: Review of Information System Controls

- **risk assessment and risk management reviews:** management reports on any IT risk assessments that have been undertaken within the systems under reviews, and the controls that have been recommended for managing the risks identified;
- **system development and project management handbook:** procedures, standards, methodologies to be followed for specifying, developing (or procuring) new systems, and for managing IT development projects;
- **relevant internal audit reports:** in addition, if the area under review is certified compliant with the ISO 9001 (Quality Management Systems) or BS 7799 (Information Security Management), the certification auditor's most recent report.

Workbook: Review of Information System Controls

Part 1: Change and Configuration Management

Change management

18. Every information system undergoes change at some stage in its life and in many, changes of one type or another are frequent events. For example:
- a new version of an application is introduced to fix problems in an earlier version and/or introduce new features;
 - further terminals are connected to a network that requires it to be extended and its capacity increased;
 - a database is extensively corrupted by a software bug and requires direct data editing to resolve the problem;
 - the computer room's air conditioning system is replaced with more modern equipment (problems here could bring the system to a standstill).
19. System changes are often made by maintenance personnel who were not members of the original system development team, and thus not as familiar with its design. Furthermore, the complexity of modern interconnected systems is such that a change to one component can easily result in unanticipated consequences elsewhere.

“Experience shows that a high proportion of the IT service quality problems currently being experienced can be traced back to a change that has been made to some part of the IT system”.

CCTA IT Infrastructure Library, “Change Management”

20. The lesson is that if problems are to be avoided, system changes need to be managed very carefully, and objective that can be achieved by adopting systematic “change management” procedures.

Configuration management

21. Configuration management is a discipline closely linked to change management, and often the Change Manager also undertakes the role of Configuration Manager. It aims to control all the components (known as “*configuration items*”) that make up an information system. These include computer hardware, data communication equipment and circuits, computer software, and information system documentation (specifications, designs, manuals, etc).
22. Configuration management encompasses four functions:
- **identification**: identifying and specifying all configuration items;
 - **status accounting**: reporting the current status of each configuration item (e.g. under development, under test, archived, in live use) and maintaining a history of all previous states (i.e. an audit trail);
 - **control**: the ability to freeze the status of each configuration item, and then make changes only on the agreement of the appropriate authority;
 - **verification**: also known as “*configuration audit*”, involves undertaking periodic reviews with the aim of ensuring conformity between the Configuration Manager's records of what should be in use with what is actually in use. This may take the form

Workbook: Review of Information System Controls

of, for example, a comparison of all software in live use against configuration management records (and software licenses!) of each software module, its version and release number, and its file size, with the aim of detecting unauthorised software or software that has been subject to unauthorised change. Similar tests should be performed periodically on other categories of configuration items (e.g. to detect unauthorised modems that might be used to bypass the network firewall).

23. A further benefit of configuration management that is of interest to the auditor falls under the heading of “business continuity planning” (see section 3). If an information system is to be rebuilt elsewhere following a disaster it is necessary to know exactly what components it comprises and how they are related. A comprehensive configuration management database can provide this information. An up-to-date copy should therefore be held in the client’s off-site store together with the various data and software backups, address lists, etc.

Emergency changes

24. System changes are not always planned events. Breakdowns and other unforeseen problems often arise which, for operational reasons, require urgent remedial action. Sometimes the urgency is such that invoking normal change management procedures or, in the case of problems that arise outside normal hours, contacting key staff (e.g. the Change Manager), would add significantly to the impact caused by the problem. Under these circumstances normal procedures are generally “relaxed”, but in the interests of maintaining control they should not be discarded completely.
25. Emergency change management procedures ought, as a bare minimum, to include a secure audit trail of all the events that take place during the emergency change. As soon as circumstances permit, a retrospective *Request for Change* should be submitted to address the problem using the normal change management process. *This is not merely a bureaucratic requirement*; it helps to ensure that any consequential risks to the system are identified and managed, the change is designed and built according to the organisation’s development standards (in particular, system documentation is updated), and that adequate testing takes place, even if this is retrospective.

Audit implications

26. From the auditor’s point of view ineffective change management may adversely affect the *integrity* of the client’s financial data and/or its *availability* for business use, thus posing a threat to the reliability of the client’s financial statements. For example, a defect introduced during a change to a computer program causes transactions to be processed incorrectly, or an incorrect change to an important standing data file causes payments to be made at an incorrect rate, in either case resulting in material error in the client’s financial statements.
27. An unsuccessful change can also result in service failure. In this situation the ability of most organisations to maintain accountability is quickly curtailed, whilst the position is further exacerbated by a build-up of unprocessed transactions. This is a particular risk where an organisation introduces a new system or implements a major system change. Although rigorous testing should reduce the risk of failure, it would be uneconomic to attempt to test every possible path through a system with every possible combination of data. It is therefore prudent to draw up a workable plan for regressing to the old system should the new system failing for any unforeseen reason.

Being able to regress quickly to the previous stable state is a key characteristic of effective change management.

Workbook: Review of Information System Controls

28. A further risk for the auditor to consider is the possibility of someone motivated by fraud or the wish to cause malicious damage making an unauthorised change to the system, or including an unauthorised component within an authorised change (a “Trojan horse” - explained in “intoIT” edition 19.... http://www.intosaiitaudit.org/index_to_intoit.htm). This possibility underlines the need for sound computer security. In particular, access to financial software and the means to amend it should be strictly controlled and there should be a separation of roles - so far as circumstances permit - between the functions of authorising, building, testing, and installing a changed component (but see “emergency changes” below).

Change and configuration management are important management controls over the risks of error, failure and deliberate system misuse.

29. Neither discipline is necessarily a full time job; indeed, they rarely are. Rather they are management “roles” that in practice are combined with other responsibilities. In this respect the auditor needs to be alert to an inappropriate separation of roles. For example, a configuration manager often has access to software and the associated documentation, and also the means of submitting amended software for live use. The role should not therefore be allocated to application development or maintenance staff that also have the necessary skills and tools for making changes.

Summary of risks

30. Badly managed, or unmanaged change *will* increase the following risks:
- **system malfunction:** results from lack of attention to impact analysis, and in specifying, designing and testing system changes. Possible consequences are corrupted financial data;
 - **system failure:** ditto, with the added consequence of failure to maintain adequate accounting records;
 - **increasing unreliability:** which builds up over time. It stems from poor system management and failure to maintain *quality* (e.g. system changes are undocumented and inadequately tested). The system becomes increasingly “fragile” and difficult to maintain, and its financial outputs increasingly error-prone, thus adding to audit risk;
 - **fraud and deliberate system misuse :** inadequate controls increase the risk of unauthorised change, and thus the risks of fraud and other forms of system misuse that can impact on the client’s financial statements (e.g. the alteration or destruction of financial data, or induced system failure). Configuration items should be adequately protected against unauthorised change by both physical and logical access controls, and there should be an adequate separation of roles within the change management process;
 - **business continuity failure:** to be of any value in an emergency, business continuity plans must be realistic and workable. Failure to update continuity plans following changes gradually erodes their value, and can easily render them unworkable.

Workbook: Review of Information System Controls

Section 1: Supplementary Questions

Overall control objective: in order to minimise the risks of disruption to processing and of corrupt information, there should be strict control over the implementation of system changes.

Control objective 1.1: changes to IT systems should be controlled on the basis of documented change management procedures

Consider whether the procedures for changing information systems:

- have been considered and approved by management;
- are known about by those who undertake system changes;
- are consistently applied;
- are up-to-date and workable.

Control objective 1.2: Requests for Change should be documented, authorised and recorded

Consider whether Requests for Change:

- provide a clear explanation of the reason(s) for the requested change;
- identify which component(s) are to be changed, and also the version to be changed where multiple versions are in use (*e.g. different versions of a program for use under different operating systems*);
- are appropriately authorised. In general, by both the Change Manager (representing the IT function) and the appropriate System Owner;
- are filed, together with any associated papers, to form a complete audit trail.

Control objective 1.3: Requests for Change should be reviewed to identify consequential risks to the correct operation of the system

Consider how management:

- identifies and assesses risks associated with Requests for Change. *Potential stakeholders should be invited to identify consequential risks. Depending on the nature of the change, stakeholders might include the Operations Manager, Database Administrator, Network Manager, IT Security Officer, other system design team leaders, capacity planning, business continuity, etc.;*
- acts on risk assessments. For example, is a proposed change too risky? Should it be re-scoped to make it less ambitious?
- establishes whether a change has been successful. Depending on the nature of the change this may not be immediately apparent, for example a revised training course or increasing network capacity to improve response times in busy periods;
- restores system stability following an unsuccessful change. Major changes in particular should be accompanied by a regression plan to cater for any severe problem not uncovered during risk assessment or testing.

Workbook: Review of Information System Controls

Control objective 1.4: system changes should be appropriately authorised

Consider the following:

- the extent of delegated powers to authorise system changes. Some changes may be of a minor nature and involve little risk; others may involve significant expenditure and risk to a successful outcome. In view of this authorising powers ought to be formally delegated to appropriate levels of management;
- whether the appropriate System Owner authorises changes to application systems;
- whether an appropriate manager authorises the use of the IT Department's staff and other resources;
- the procedures for ensuring that end users are consulted on proposed changes to the IT infrastructure on which they depend. Examples will include LANs and WANs, servers and operating systems that the end users generally do not own. Changes to infrastructure should take place at times when the end users are least likely to be affected by any problems or failures (e.g. avoiding end of year accounting processes or the monthly bill paying/salary run).

Control objective 1.5: change management procedures should pay due regard to an effective separation of roles

Consider what action management has taken to ensure that:

- no single person can authorise, build and implement a change (see emergency procedures below). In an ideal situation the functions should be separated:
 - *authorising and recording a change*
 - *custody and control of the asset to be changed*
 - *building a change*
 - *reviewing and testing a change (quality control)*
 - *installing a changed component in the live system*
- where the scale of operation permits, an adequate separation of roles applies to emergency changes.

Control objective 1.6: authorised changes should be managed to completion

Consider how management ensure that:

- there is a complete audit trail of all system changes, including emergency changes;
- all steps within the change management procedure are recorded in the audit trail;
- the audit trail for each change is retained for an appropriate period;
- each change has an "owner" or "sponsor" to take decisions on key questions. *For example regarding design features, cost and deadline;*
- authorised changes are planned and scheduled according to business needs. *No organisation has sufficient resources to implement all desirable changes at once. Important decisions have therefore to be made on prioritising changes according to business needs;*
- all scheduled changes are actually carried out according to priority;
- unsuccessful changes are adequately dealt with;
- system changes do not bypass the approved procedures.

Workbook: Review of Information System Controls

Control objective 1.7: emergency changes should comply with normal change management requirements as soon as possible

Consider what procedures ensure that emergency changes:

- are implemented without delay;
- are recorded in an audit trail;
- do not result in abuse of the change control system by bypassing normal procedures (*e.g. authorisation, risk assessment, testing, documentation*);
- are processed through normal change management procedures as soon as possible.

Control objective 1.8: changed components should be fit for business use

Consider the following:

- how management ensures that system changes:
 - comply with the appropriate development standards;
 - are of acceptable quality to end-users;
 - quality review includes inspection of all appropriate documentary changes.
- whether the impact of changes is reviewed following their introduction to live use (*“post implementation review”*);
- what procedures management adopts to detect unauthorised components incorporated within an authorised change. *“Trojan Horses” apply particularly to software changes, although the concept also applies to hardware in the fitting of unauthorised equipment.*

Control objective 1.9: configuration management records should accurately describe the live configuration and its status history

Consider whether:

- a manager has been appointed to fulfil this role, has received appropriate training and has been provided with appropriate software tools (*e.g. specialised database software, auto-librarian software*);
- configuration management records are comprehensive. *Do they adequately record basic information (e.g. item reference, description, version/model, date installed, location, owner, change history) and show relationships/dependencies, where they exist, between:*
 - hardware
 - software
 - documentation
 - data communications equipment and circuits
- configuration management records are promptly updated to reflect system changes (*e.g. RFC reference, sponsor, description, date implemented, change builder*);
- configuration management records are protected from unauthorised change;
- the live configuration management records reliably describe the live system. *In this respect the configuration management team should audit the live system periodically.*

Section 2: Information System Operations and Maintenance

Computer Operations

31. Within the context of this guide, “computer operations” includes the following activities:
- operating multi-user computers and networks;
 - processing bulk data input;
 - producing and distributing centrally produced system outputs;
 - receiving, allocating and expediting fault reports;
 - managing system backups;
 - managing service levels;
 - providing a help desk service.

Recruitment, training and operating procedures

32. *Sound recruitment procedures play an important part in screening and selecting suitable people to undertake an activity, but continuing training and career development policies are equally important. Competence and good staff morale are strong controls over error.*
33. Clear, usable operating procedures help to strengthen competence, particularly where operations staff are unfamiliar with a particular task (e.g. an end of year financial process is performed infrequently), or the process is performed in a number of steps that must be run in strict sequence. There should be operating procedures to support all operational activities, such as starting up and closing down systems and networks, operating batch work, and recovering from system or job failure. Procedures also need to cover “housekeeping” activities, such as backing up and restoring from backup, equipment maintenance, and maintaining a safe computer room environment (e.g. cleaning/waste removal, floor void inspections, and smoke detector tests).
34. Operating procedures should be sufficiently comprehensive for their purpose. They should also be reliable, and to maintain them in this condition they should be subject to change management procedures (if an application is changed, its operating procedures may also need to be changed - see Section 1).

Separation of roles

35. *Separation of roles* means that no one person can initiate and complete an entire activity or transaction. An effective separation can provide a check over error, fraud and malicious damage.
36. In information systems roles can be separated by a combination of organisational controls (e.g. allocation of work and management reporting lines), and controlling both physical access (e.g. restricting access to documents and stationery, and to equipment) and logical access (e.g. restricting access to programs and data, and activity logging coupled with management review).
37. Where a separation of roles exists, the auditor should confirm that the organisational and physical controls that can often be seen in operation are also mirrored in the ‘invisible’ domain within the computer system. *This is not always the case.*
38. Problems affecting the logical separation (i.e. within the computer system) of roles can occur when staff transfer between different jobs and bring their existing access

Workbook: Review of Information System Controls

permissions with them. Alternatively, someone standing in for an absent colleague needs to acquire their access permissions in order to perform their duties, but then retains these permissions when the absent colleague returns. It is also possible that management pays little or no attention to the risks of inadequate separation, or justifies lack of effective separation by citing greater flexibility in the use of their staff (a common claim).

Obtaining the optimum balance between control and the acceptance of risk can involve difficult management decisions.

39. Within the traditional area of computer operations - and to the extent that the scale of operations permits - there should at least be a separation of roles sufficient to prevent computer operators from amending system and application files. This may be accomplished by:
 - prohibiting access to application program code and the means to amend it;
 - controlling access to any system utility programs that can be used to edit application and standing data directly (some tools edit data by addressing the appropriate cylinder and sector on the disc, thus bypassing logical access control).
40. Other activities that, if separated, add to the strength of control, are listed at section 2.2 below.
41. The traditional IT department model provided good organisational and physical separation between operations, development, maintenance and end user activities. The development of client server systems and the resulting transfer of some operations functions to the end users have eroded aspects of this traditional separation. In small installations there may be insufficient staff to enable roles to be separated effectively. The auditor may therefore need to look for other controls - such as increased management supervision and financial reconciliations - to compensate for any weakness. *But beware. Compensating controls are often detective; they operate after an event has taken place. This is less satisfactory than preventing an unwanted event occurring in the first place, as the damage caused may be unrecoverable.*

Authorisation of work run on the installation

42. There are two types of computer processing, both of which can affect financial data and therefore need to be controlled.
43. “Interactive” processing takes place when the user remains connected to a program and controls its operation interactively (a simple example is using a word processor or spreadsheet). A background process is one in which a user initiates a process, and then leaves it to run in the background. The process may be controlled by a set of instructions written in the language of the computer’s operating system, and referred to as a “job control program” (a simple example is backing up or defragmenting a PC).
44. Both these descriptions apply equally to jobs that run on servers and mainframes. Users can either work interactively from the operating system’s command prompt (e.g. on a PC this is equivalent to working under DOS from the ‘C’ prompt) or via a graphical user interface to an application program. They may also submit jobs to run in background mode (e.g. to produce a general ledger report from a database) and then log off leaving the process to complete under its job control program.
45. Sophisticated processes can involve a succession of background jobs linked together by a job control program designed to monitor their progress and to take appropriate action on receipt of specific messages from either the application or the operating system. In turn a succession of job control programs can be initiated and controlled by an automatic job scheduler with little or no manual intervention being necessary.

Workbook: Review of Information System Controls

46. It's good management practice to operate a computer system according to a planned work schedule and to record automatically in audit trails how the system has actually been used. For example, loading on-line applications and backing up the system are events that feature in most installations' work schedules. Other events that take place less frequently, such as end of year financial routines, are nonetheless capable of being planned and scheduled.
47. Management should monitor the use made of computer systems, to verify that the planned workload is being processed correctly and to detect signs of system misuse. Examples of the latter are theft of computer time (using resources for private work) and unauthorised access to data for purposes of fraud, theft of information or system sabotage. Audit trails used in conjunction with work schedules provide a means of verifying that all scheduled work has run successfully and of identifying any exceptional events that require investigation.
48. Where important changes are made to the operating system or its configuration files under the authority of a *Request for Change* (RFC), the appropriate audit trail information should be saved and filed as part of the change record (see Change Management). Management should review changes periodically to confirm that the work actually carried out was that authorised.
49. In practice audit trails (or "logs") often contain a large miscellany of information reported by the system. This data is necessary for diagnostic purposes, but it can obscure the underlying pattern of system use. It may therefore be necessary to interrogate the log with suitable query software to extract the appropriate monitoring information and sort it into user or program-ID order. For example:
 - dates and times of logon and logoff, or of program start and finish;
 - terminal identity or location from which the event was initiated;
 - both successful and rejected access attempts;
 - system use at unusual times;
 - all recorded access to particularly sensitive files or user accounts (e.g. Super or Master user);
 - all recorded use of selected system utilities.
50. Where notional or actual charging for computer use is in force, the system accounting package can provide a very useful source of information on system use, and one that is not obscured by extraneous information.

Data Input

51. Nowadays, data is often captured for processing directly by electronic means. Examples are transactions that are captured via electronic data interchange ("EDI"), file transfer and electronic commerce ("e-commerce") systems. Where transactions remain paper-based, the end-users generally key the data directly into the system from workstations. These forms of data capture are considered within the application system questionnaires.
52. This questionnaire is concerned with bulk data input, where (generally) large volumes of paper documents are converted into electronic form, either by a process of:
 - manual keying; or
 - scanning bar coded or bar marked input forms; or
 - scanning text using an Optical Character Recognition ("OCR") or Magnetic Ink Character Recognition ("MICR") reader; or

Workbook: Review of Information System Controls

- capturing electronic document images using a document scanner.
53. In general, bulk data conversion is carried out by a separate “data conversion” team within the IT operations organisation. The team’s purpose in this respect is to convert paper-based data to electronic form and submit the resulting files for processing by the appropriate application system. Controls are necessary to ensure that the task is performed completely and accurately, and that no unauthorised changes to the input take place. Indeed, experience shows that the most likely point of error and fraud (“input fraud”) in computer systems is during input, where data may be: -
- lost or incomplete;
 - duplicated;
 - unauthorised;
 - manipulated during the input process;
 - inserted without authority (either accidentally or fraudulently).
54. Auditors should review controls in three respects; that the process is documented, there are adequate procedures for handling input forms, and that the data input to the system for processing is first tested for errors and omissions. Further tests should be carried out by the appropriate application system (e.g. duplication, gap analysis, transactions unmatched with accounts) and are addressed in NAO Form 910, Section B.
55. In common with other procedures, those that apply to data conversion should be documented. This is important to ensure that everyone’s understanding of the system is the same, to provide a guide for new staff and a source of reference for existing staff and auditors. Documentation should lay down, step-by-step, the progress of data, the process applied and who is responsible at each stage.
56. Where possible, paper input documents should be gathered into “batches” for control purposes and a “batch control slip” (or “batch header”) prepared. *The earlier in the process that batch control is imposed, the less chance there is of documents being lost or of additional documents being inserted.* A batch control slip will typically record the following:
- a unique, sequential batch number (identifies the basic unit of processing);
 - date, name of system, and type of transaction;
 - number of documents in the batch, and control totals;
 - initials of initiator of the batch, plus additional initials of those who subsequently process it.
57. Input documents are retained within their batches throughout processing and the progress of each batch, and the value of its control totals, is recorded and checked at each stage of the process to provide an audit trail.
58. Following successful processing batches should be cancelled (e.g. by stamping, hole drilling or other physical defacement) to reduce the risk of duplicate input. Batches should then be filed for audit, or destroyed according to the client’s document retention policies and procedures (which might need to observe legal requirements). Where, following data capture, paper documents are to be destroyed, before their destruction appropriate accounting and quality control checks (important where paper document images are captured) should be completed satisfactorily, and the captured data backed up (*successfully*).

Workbook: Review of Information System Controls

59. Where batch controls are not in operation, the auditor should look for compensating controls to ensure the completeness and accuracy of input; for example, comparing a sample of input documents against what has been accepted by the system.
60. Data should be validated automatically during input to detect important items that are missing or are clearly incorrect. Software validation tests typically address the following:
- **check digit:** an extra character attached to a data item and mathematically related to it, which can be used to detect error by re-performance;
 - **range or limit check:** tests on specific items to confirm that they lie within an acceptable range(s);
 - **format check:** tests to confirm that an item is in the required form; e.g. all alphabetic, or all numeric characters;
 - **overflow:** ensures that data cannot be corrupted by a computation generating a figure too large to be accommodated in the receiving field;
 - **completeness:** all expected fields have been completed;
 - **compatibility:** all related fields are reasonable/feasible in relation to each other (e.g. driving licenses are not normally issued to registered blind people!);
 - **duplication:** confirmation that the item has not already been processed (e.g. by reference to invoice number or batch number).
61. The input process should also check that the batch control controls, as keyed in from the batch control slip by the operator, agree with the number of documents processed and the aggregate value(s) of the corresponding control fields. Input documents that are rejected should be referred back to their initiator for correction, and the batch control slip amended and initialled to reflect this change. Corrected items should be re-submitted through the normal batch control process.

Managing financial stationery

62. The auditor will need to consider what types of pre-printed computer stationery the client uses, and whether it is vulnerable to theft or fraud. Obvious examples are cheques, giros and payable orders, but there may be circumstances where licenses or permits might also require protection. In general, use of valuable stationery should be controlled by means of:
- physically secure storage;
 - stock-checks;
 - reconciliations between numbers issued, printed and cancelled;
 - the controlled (and recorded) destruction of spoiled and obsolete stationery.
63. Printers need to be “lined up” when printing forms so positioned that variable data (e.g. the amount for payment on a cheque) can be inserted by the printer at the appropriate position. This process results in a number of forms being spoiled. These and other wastage should be cancelled, retained and accounted for together with receipts, issues and stock balances. Records should be audited periodically by some one other than the person responsible for issuing stationery.

Computer output

64. Computer output arises in a various forms including printed reports, microfiche, optical and magnetic files, screen outputs and transmissions over communications network.

Workbook: Review of Information System Controls

Output is also subject to various risks both deliberate and accidental. It may be inaccurate or incomplete; it may also be dealt with in an unauthorised manner, for example:

- fraudulent payable instruments might be issued, or notifications suppressed (e.g. sales invoices);
- additional unauthorised copies of a sensitive report might be obtained;
- confidential output might be examined by someone who is not meant to see it;
- output documents might be stolen or deliberately destroyed;
- output documents might be amended.

65. The fundamental output control objectives that the auditor should consider are to ensure that data processing and its associated output are:
- accurate;
 - complete;
 - produced by authorised, tested application programs.
66. Computer output should be checked before despatch to confirm that it has been produced by a valid application program, is complete and accurate and, in all other respects, appears to be of appropriate quality (e.g. the print is legible and correctly aligned). In a large installation, a separate Output Control Section might undertake these activities with the aid of the appropriate operating procedures. The operating procedures should also describe how to respond to any error messages that might be produced.
67. All prints and reports should be page numbered (in 'x' of 'n' format) and terminated by an appropriate message to signify that they are complete (e.g. "end of report"). Where a report is to be produced, but no records qualify to appear on it, the application should print a 'nil return' to confirm that the program has not malfunctioned or the report has not been lost. Where receipt of a regular report becomes part of the routine of authorised recipients, they are more likely to notice a report that has been lost or intentionally suppressed.
68. In terms of accuracy and completeness of processing the most common control is an overall reconciliation of output back to authorised input. This reconciliation may be carried out by the end-users, in which case sufficient control totals should be produced with the output to facilitate reconciliation, at least to the extent necessary to prove that all and only authorised input has been completely and accurately processed.
69. Depending on its value and sensitivity, computer outputs may need to be held securely until despatch. Details of who should receive output and any special requirements should be clearly defined and set out in operating instructions. Output distribution is often completely automated in modern systems with reports being emailed to authorised recipients. Where this is the case there should be evidence that the distribution system is tested regularly and that changes in job functions triggers an update of the distribution lists.

Managing system backups

70. Business continuity planning as such is covered in section 3 of this questionnaire. This section deals the management of backup files, an activity that generally falls to the computer operations team.
71. Most business activities now rely to a greater or lesser degree on the availability and correct operation of computer systems. And if key financial systems are unavailable, it is likely that within a comparatively short space of time the adequacy of the organisation's accounting records will suffer. It is therefore important - often vital - that key financial

Workbook: Review of Information System Controls

systems can be restored should the data be corrupted (e.g. by software error, hardware failure, virus attack), the system suffer a prolonged failure (e.g. hardware breakdown, power or communications failure), or a disaster occur (e.g. fire, flooding, bomb blast).

72. Although business continuity depends on identifying potential problems and planning to take account of them, no amount of continuity planning will enable a system to be recovered if there is no usable backup. It is essential that:
- systems are backed up periodically;
 - recovery from backups is regularly tested, particularly when there is any change in the backup hardware or software, operations personnel or the recovery plan;
 - up-to-date backups are stored securely, with additional copies of the software, data, user instructions and any specialised forms held in a secure remote store;
 - management are aware of the location and contents of backup media; and.....
 - backups are usable - they contain the correct components and are readable.
73. Systems should be backed periodically to reflect change, particularly to important business data that often changes rapidly. Although software and system configuration files change less frequently, it is nevertheless important that they are also backed up periodically to reflect changes in the way that operates and has been configured. In the case of internally developed software, which cannot be replaced in the same way as commercially available off-the-shelf products, the source code and development documentation (specifications, designs, test data and test scripts, etc.) needs to be backed up.
74. The frequency with which systems should be backed up will depend on both the rate of change and the maximum period of downtime that the client's business can tolerate. Assuming a high rate of change, the greater the period between backups the greater the obsolescence and the less useful the backup will be for restoring a system to its current state. The auditor should therefore expect to find a backing up strategy that takes all these factors into account, and this in turn should be reflected in the installation's work schedule (i.e. the frequency of backups and of backup/recovery testing).

Reporting and managing incidents

75. For the purposes of this section, and for convenience, the term "incident" will be used to refer to "user queries", "software bugs", "hardware problems", "system failures", etc. - in other words, to anything that requires (or appears to require) some form of IT support and remedial action.
76. The quality of IT service delivery can easily affect a client's ability to maintain adequate accounting records. Hardware and software defects, network failures, problems in using a financial application, and computer viruses are examples of 'incidents' that can affect the integrity and/or availability of financial data to a greater or lesser degree. It follows that the quality of IT services delivery will be improved if there is a fast and efficient means of reporting, investigating and, where appropriate, taking remedial action on IT incidents. In many organisations (the UK NAO being an example) the solution that is adopted is to provide a central help (or "service") desk staffed by trained technicians, although less formal measures can provide an effective solution in a small, centralised organisation.
77. An ideal incident reporting system should provide the following facilities:
- a single point of contact (a "*one stop shop*") for all classes of incident. It should be known about (well publicised) and be readily accessible by its user community;
 - support during times agreed with its users community and a mechanism (e.g. by e-mail or voicemail) for recording incidents at other times;

Workbook: Review of Information System Controls

- a means of recording and classifying incidents (e.g. by system, location, type and severity) to help prioritised response (resources are rarely available to respond to everything at once!) and to provide incident statistics;
 - allocation of incidents to the appropriate technical support group for investigation and resolution;
 - regular review and expedition of outstanding incident reports, coupled with escalation of outstanding incident reports;
 - closure of resolved incident reports, and user follow-up where appropriate;
 - periodic analysis of incident reports and production of management statistics. These are essential for identifying common and recurring types of incidents from which lessons might be learned.
78. Sensible statistics help management to monitor the quality of service delivery (e.g. periods of downtime, incident response times, times to fix, times to restore service) and identify any emerging trends that require further investigation. For example, a consistently high level of user queries on the use of an application system might suggest that the users need to be trained more effectively. Numerous reports of PC failures might suggest inadequate quality in the PCs provided, or in engineering support.

Database Administration

79. This section applies to the administration of multi-user databases. Most financial applications utilise database systems and, in the interests of reliable data, a database should be effectively managed and controlled.
80. A “database” is a *structured* collection of interrelated data items, which often supports a number of different applications. These can be batch, on-line or both, and they may run concurrently. Although there are several types of database, those that the auditor is most likely to encounter are:
- **relational** : in a relational database, data items are organised in two-dimensional “tables” comprising rows (referred to as “tuples”) and columns. A row forms a record, whilst columns may be regarded as data items. Each row may be uniquely identified by the values of one or more columns. A “view” of the database may be constructed by taking elements from one or more tables (“relations”). Relational databases are ideal in situations where the power of enquiry is more important than processing performance;
 - **network** : in a networked database, data items are organised in a hierarchy of parent, child, grandchild, etc. relationships; e.g. a record relating to a *doctor* may have associated with it a number of subsidiary *patient* records, each of which may have associated with it a number of subsidiary *prescription* records. However, in a network the hierarchy is modified to allow each data item to have more than one parent if necessary; e.g. a *doctor* can have more than one *patient*, but unlike a pure hierarchy, a network will also allow a *patient* to have more than one *doctor*. Data is therefore accessed through a mesh of routes and relationships. This type of database is commonly found in high volume production systems due to its superior performance over relational types, although its more rigid structure makes it less flexible.
81. Regardless of the manner in which data is organised within the database, a database system comprises two principal components, the database and the database management system (“DBMS”):

Workbook: Review of Information System Controls

- a **database** is a collection of data, which is generally organised according to one of the systems described above. Each user will not necessarily be aware of all the information stored in the database, only that used by their particular application;
 - a **DBMS** comprises the software that is used to program and operate the database, and to manage where the data is actually stored (“physical storage”).
82. The consequences of implementing a database are to bring together a great deal of corporate data in a central repository, which is accessed by users via query languages, spreadsheets and a range of application programs. Problems can arise concerning the ownership, rights and responsibilities for the data since a given part of the database may be used by many applications. For example, should ownership be vested in the creator of the data, the majority user of the data or those responsible for its maintenance? *Failure to address these difficulties via a policy decision leaves no clear ownership and hence poor control over the reliability of the data.*
83. One approach to the problem is to assign ownership to the originator of the data, and to assign to that person the right to grant or revoke privileges to its access, modification and deletion. Another is to assign “proxy ownership” to a Database Administrator (“DBA”), and leave the DBA to arbitrate between the various parties that use the database.
84. Regardless of what solution is adopted, *there should be a well defined policy and procedures* for: -
- identifying data and agreeing a common definition for each item;
 - assigning ownership to a suitable *post holder* (not to a *named individual!*);
 - identifying problems and arbitrating between interested parties;
 - identifying and agreeing changes to the database structure;
 - enforcing the procedures.
85. Regardless of the client’s policy on data ownership, it is essential to create a co-ordination role. The conventional solution is to appoint a DBA to perform a database administration function. The DBA often needs to operate at all levels within an organisation and should therefore have sufficient status and appropriate reporting lines to be able to perform the role effectively. In a large organisation the role may be full time with a support team.
86. The principal functions that the DBA will perform are to:
- **resolve conflicts** between different users and **setting standards** over data formats; precision; access and user privileges; accountability and data naming;
 - make sure that **user requirements** are (in general) met;
 - make sure that the relevant parts of the organisation’s **information system strategy** is being met; e.g. in respect of database growth, its responsiveness and its ability to service new application systems. This requires **capacity planning**;
 - ensuring **co-ordination** between users and system development teams on data requirements;
 - maintain the overall **integrity** of the database structure and its contents (i.e. *domain, entity and referential integrity* – see below);
 - ensure that all modifications, **changes**, structural alterations to the database and application system implementations proceed smoothly;

Workbook: Review of Information System Controls

- ensure that **the database is backed up** in accordance the business continuity planning requirements, and that the database can be **recovered** from backup, if necessary on a standby machine at another location;
 - **liaising with the vendor** of the database management system on problems, expediting their resolution, testing new releases of the database management system, and **co-ordinating** their live implementation through the client's change control system.
87. An important function that falls to the DBA is to ensure that the overall integrity of the database is maintained and to resolve problems where they occur. The three main aspects of database integrity are:
- **domain integrity**: a “domain” is a set of legal values that a data item may take. They are centrally defined, and once defined they should be enforced by the database management system and inherited by all items based on a particular domain;
 - **entity integrity**: requires that every row in a database table is uniquely identified;
 - **referential integrity**: this is perhaps the most important aspect of database integrity. It means that all internal references are valid; in other words that the database does not contain data items that are linked to incorrect items or to items that no longer exist. For example, all orders for a customer should be deleted automatically when the customer record is deleted – there should not be any unattributed fragments left behind.
88. In respect of database integrity, the auditor needs to know how the client gains assurance that domain, entity and referential integrity are maintained and, where problems arise, how these are detected and corrected.
89. Some vendors provide software utilities to detect database integrity errors, but if such tools are not provided, there should be some mechanism within the database management system that will report errors where they occur. It should also be possible to detect database integrity problems through the accounting system by reconciling computer produced records against externally maintained control accounts; bank reconciliation is an example under this heading. CAATs can also be employed to reconcile trial balance items against direct interrogation of the relevant database tables.
90. Other controls which the auditor should examine are:
- **separation of roles**: the DBA is provided with software tools to restore integrity when data is corrupted. These tools operate outside of the control of the application system and could be used to make unauthorised changes to the data. To reduce the risk of abuse, end-users should not have access to utilities or query languages that can be used to modify data outside of application system controls, whilst the DBA function should not be performed by someone who has detailed knowledge of business applications or physical access to the appropriate stationery;
 - **access control**: a database often hosts many users and many applications. If numerous individuals are able to make uncontrolled decisions regarding the integrity of given data, the risk increases that the data will be corrupted or used improperly. Responsibility must therefore be assigned to an appropriate end user for the ownership of the data, and for authorising individual access to it. It falls to the DBA to implement access on the data owner's authorisation and the client's data ownership policy.

Summary of risks

91. Inadequate control over computer operations increases the risks of business disruption, inaccurate financial data and fraud for the following reasons:

Workbook: Review of Information System Controls

- inadequate staff training and/or system operating instructions increase the risks of business disruption through:
 - *system malfunction (e.g. running jobs in the wrong sequence, or not at all; not responding to error and warning messages);*
 - *system failure (e.g. not responding to warnings of inadequate media space);*
 - *inadequate or unusable backups to guard against malfunction and failure;*
- inadequate separation of roles and authorisation of work increase the risks of:
 - *system misuse (use of the computer for unauthorised purposes);*
 - *system malfunction due to lack of management scrutiny of work carried out;*
- inadequate data preparation and input procedures increase the risks of:
 - *invalid, incomplete and erroneous data being accepted for processing;*
- inadequate procedures for managing financial stationery increase the risk of theft (licenses, permits, etc.) and fraud;
- inadequate control over computer output increases the risks of:
 - *fraud (theft, duplication or modification of financial instruments);*
 - *disruption to business operations (failure to deliver usable outputs, to the correct location and on time);*
 - *incorrect business decisions based on incomplete outputs;*
 - *disclosure of sensitive business and or personal information;*
- inadequate control over computer backups increases the risks of:
 - *prolonged business disruption due to irrecoverable system failure, leading to.....*
 - *failure to maintain adequate accounting records following unrecoverable system failure (see Foreign and Commonwealth Office - qualification of 1989-90 appropriation accounts)*
- inadequate procedures for reporting and managing incidents increase the risks of:
 - *poor system availability and high incidence of unreliable data due to unresolved problems;*
 - *ditto, due to failure to collect, analyse and act on incident statistics;*
- inadequate multi-user database administration procedures increase the risks of:
 - *fraud, through unauthorised modification of financial data;*
 - *system malfunction or failure due to incorrect database design (including design changes);*
 - *system malfunction or failure due to incorrect operation of the database management system.*

Workbook: Review of Information System Controls

Section 2: Supplementary Questions

Overall control objective: computers and networks should be operated in a secure manner and provide a level of service sufficient to satisfy business needs

Control objective 2.1: Computer operations should be performed competently

Consider the following:

- how management ensure that operations staff know what is expected of them. For example, have roles and responsibilities for managing and operating computers and networks have been allocated and included in job descriptions and contracts?
- how management ensures that operators are competent to perform these tasks;
- management's procedure for defining and documenting operating procedures.
- whether there are sufficient documented operating instructions. For example, are there **usable/workable** operating instructions to cover (as appropriate):
 - *starting up and closing down systems?*
 - *backing up and restoring?*
 - *transferring backups to remote store?*
 - *scheduling batch processes, their interdependencies with other systems, earliest job start and latest job completion times?*
 - *instructions for amending work schedules?*
 - *instructions for handling errors or other exceptional conditions which might arise during job execution?*
 - *system restart and recovery procedures for use in the event of system failures?*
 - *support contacts in the event of unexpected operational or technical difficulties?*
 - *special output handling procedures, such as the use of financial stationery, including the secure disposal of output from failed job?;*
 - *migrating new and changed software into live use?*
- how management ensures that operating instructions keep up-to-date and remain effective;
- what controls are in place to ensure that individual applications systems:
 - *can be loaded, operated, backed up, restored (if necessary) and shut down correctly;*
 - *which produce exception or error messages are investigated, and appropriate action taken.*

Control objective 2.2: Incompatible roles should be separated to the extent practicable.

Consider the extent to which management has separated roles to provide a check over error and system misuse. Ideally the following roles should be separated from each other (using an appropriate combination of organisational, physical and logical controls):

- problem reporting and resolution (help desk);

Workbook: Review of Information System Controls

- authorising changes to applications and to infrastructure items (operating system, servers, network, etc);
- application development and maintenance (program changes installed by operators – see section 1);
- multi-user database administration (maintaining the database and the database management system);
- system programming/administration (maintaining the operating system);
- testing system changes;
- operating multi-user computers and networks;
- data preparation (this task is now generally performed by end users);
- output distribution (ditto, except for the management of system backups);
- IT security administration.

Control objective 2.3: all system operations should be authorised and serve legitimate business needs

Consider the following:

- *how computer processes are authorised*. This is often by means of daily work schedules authorised by the Operations Manager, and restrictions on which users can initiate computer processes;
- *how management would detect unauthorised processing (both batch and interactive)*. For example, does the Operations Manager periodically review records of processes that have run on the installation? (e.g. computer-produced job accounting reports). What do they look for?
- *whether all processes have an unique, identifiable owner* (e.g. to whom to refer problems, and to ensure that any unrecognised processes are suspended pending investigation).

Control objective 2.4: data input for processing should be valid, complete and accurate

Where bulk data is converted into machine-readable form, consider what controls ensure that:

- only valid data is accepted for processing (i.e. authorised and excluding items applicable to other populations, items already processed and forgeries);
- missing, incomplete and inconsistent data is identified and corrected;
- data is protected from unauthorised change during conversion;
- all data is converted completely and accurately;
- all converted data is input to the appropriate application systems for processing.

Control Objective 2.5: Financial stationery should be stored securely and its use accounted for

Consider the following:

- whether the installation produce computer printed forms that are inherently valuable and require protection (e.g. cheques, payable orders, giros, licenses, permits);

Workbook: Review of Information System Controls

- how management ensures that valuable output forms are not tampered with or stolen.

Control objective 2.6: outputs should be complete and accurate, and distributed promptly to the correct recipient

Consider the following:

- how operators know what outputs to expect;
- how would recipients identify missing output;
- what ensures that incomplete and inaccurate outputs are detected;
- the procedures for handling incomplete or inaccurate outputs;
- what prevents duplicate outputs being distributed;
- what ensures that outputs are promptly distributed to the correct recipients;
- whether outputs awaiting distribution are stored securely in relation to their value or sensitivity.

Control objective 2.7: system backups should be readable and their use accounted for

Consider what procedures ensure that, in the event of a system failure or disaster:

- up-to-date backups (software and data) are available;
- the contents of system backups storage unit (e.g. tapes) are known;
- the whereabouts of individual storage units are known;
- the restored system is usable (staff can be accommodated and have the correct equipment and stationery to use the system);
- software and data backups are viable (*i.e. backing up has saved the correct files, and the resulting data is known to be readable*).

Control objective 2.8: the level of service provided should be consistent with business needs

Consider the following: -

- how the level of service to be provided to end users is formally defined;
- how management monitors the level of service provided;
- how management ensures that the level of service provided meets defined targets and is sufficient to meet business needs;
- how the end-users are consulted in setting service delivery targets;
- what procedures exist for addressing inadequate service delivery.

Control objective 2.9: there should be a focal point for reporting, recording and resolving incidents and operational failures

Consider the following:

- the procedures in place to ensure that incidents that affect the quality of service receive attention;
- how management decides what action to take on an incident;

Workbook: Review of Information System Controls

- whether incidents are dealt with according to their impact on service delivery;
- the controls in place to ensure that incidents requiring remedial action are fixed:
 - *correctly;*
 - *in line with quality standards;*
 - *within an acceptable deadline;*
- the procedures for gathering incident statistics and the use that is made of them for improving service quality.

Control objective 2.10: Data stored within multi-user databases should be reliable and available for use when required

Consider what procedures ensure that:

- in respect of each item stored within the database:
 - *its source, description and meaning are known;*
 - *ownership is known;*
 - *access is controlled for purposes of reading, updating and deleting;*
- the database and its associated application programs remain compatible following changes to either of them;
- any corruption to data or to the logical database structure is detected promptly;
- changes to the structure or contents of the database, or its physical storage, are authorised and controlled;
- data is backed up at a frequency sufficient to meet business needs;
- all authorised users agree to the deletion of a data item before it is removed; and....
- the database can be recovered from backup if necessary.

Workbook: Review of Information System Controls

Section 3: Information Security Management

Introduction

92. Corporate data, and the computer systems and networks that support it, are vital business assets. Their security is essential for enabling departments to discharge their statutory role, for maintaining sound financial control over their operations and for producing reliable financial statements.
93. “Information security” comprises the range of controls that operate to ensure business continuity and minimise business damage by preventing or minimising the impact of security incidents (i.e. “unwanted events”).
94. “Information security management” is the means by which information security is implemented. Its aim is to enable information to be shared whilst ensuring its protection, and that of the associated computing assets, from a range of threats that could damage them in some way, *but only to the extent necessary*. Controls can be expensive to install and maintain, and they can also act to reduce operational efficiency. Furthermore controls that are adequate for protecting one organisation may be either excessive or inadequate for reducing the risks faced by another.
95. Information security management aims to achieve four objectives:
- **confidentiality**: sensitive information is not disclosed to anyone who does not have a legitimate need to see it;
 - **integrity**: information is valid, complete and accurate;
 - **availability**: information is available for use when and where required;
 - **nonrepudiation**: proof of the integrity and origin of data by a means that cannot be forged and that can be verified by a third party at any time.
96. In general, external financial auditors are not directly concerned with the confidentiality objective because it does not contribute directly to the audit opinion. However, if confidentiality is breached (e.g. by an attacker gaining access to a user’s password), there is a risk that data integrity and/or availability could be compromised as a result. In other words failure of one security objective can impact on the others.
97. The remainder of this section explains those aspects of information security management that are covered in the NAO Form 905.

Information Security Policy and Organisation

98. An Information Security Policy (or “IT Security Policy”) is the foundation of effective information security management. The policy should be written and available to all who have information security responsibilities (in general, everyone).
99. The form of information security policy documents varies, but in general one would expect to find a definition of information security, an explanation of its importance to the organisation and a statement on what needs to be achieved. There should also be an explanation of specific security policies, including those on:
- **security management**: the allocation of roles and responsibilities for implementing, managing and reviewing the effectiveness of information security, including the role to be undertaken by internal audit;
 - **risk assessment**: the arrangements for undertaking and maintaining a programme of information security risk assessments across the organisation;

Workbook: Review of Information System Controls

- **incident reporting and investigation:** the process for reporting and investigation actual or impending security incidents;
- **security awareness:** procedures for ensuring that all staff are aware of the organisation's information security policy and understand their role in implementing it;
- **computer virus prevention and detection:** controls over importing new files onto the organisation's machines;
- **legal compliance:** compliance with the law on, for example, data protection, copyright protection, computer misuse, industry sector legislation and regulations, and the common law (defamation);
- **business continuity:** roles and responsibilities for ensuring that appropriate and workable business continuity plans are in place;
- **contravention:** a statement on the action to be taken in the event of deliberate or negligent contravention of the policy.

Auditability

100. In order to undertake a controls reliant audit, there should be adequate controls in place over financial data, *and also satisfactory evidence* ("process control records") *that they have operated correctly and consistently throughout the period covered by the audit.*
101. Observation and interview are important sources of audit evidence, particularly in respect of current activities, but they are unlikely to prove persuasive with regard to the operation of controls at other times. Process control records ought to be available; indeed they are a requirement for organisations wishing to obtain certification against the British Standard for information security management (BS 7799). The following is what the British Standards Institution's guide to certification auditors has to say on the subject:

*Records are a vital component in demonstrating proper security control. Records are different to general documents in that they record events which have taken place and are not updated and so not subject to version control. Auditors must ensure that the records kept and retained are adequate to demonstrate compliance to both the standard (i.e. BS 7799) and the organisation's security requirements. The procedures (i.e. those of the organisation) shall describe how the records are identified, maintained, retained and ultimately disposed of. It is also required that records **shall** be stored and maintained in such a way as to be readily retrievable and protected against damage, deterioration and loss. All these points must be confirmed by the auditor. Again records may be electronic or paper form and it is increasingly likely that both will be need to be catered for within the same organisation.*

102. The following are some examples of the types of documentary evidence that an auditor might require:
- **personnel recruitment and training:** personal files recording individual background and qualification checking; letters of appointment, individual training records;
 - **IT security management:** agenda and minutes of security committee meetings; documented security policies and procedures; individual job descriptions for those with security roles;
 - **risk assessments and security reviews:** risk assessment records, approved by appropriate business area and security management; internal audit reports and related working papers;

Workbook: Review of Information System Controls

- **physical access to sensitive areas:** certificates, signed and dated by an appropriate manager, that the access log has been reviewed, with what objectives and with what results (logs may be electronic or paper-based);
- **computer operations:** certificates, signed and dated by an appropriate manager, that the computer operations log has been reviewed, with what objectives and with what results (computer logs may be reviewed using CAATs – such as IDEA – or any other suitable file interrogation tool or package, or alternatively the system might be configured to send specific messages to a separate security log);
- **logical access control:** certificates signed and dated by an appropriate manager of general password and encryption key changes; individual access permissions reports signed and dated by appropriate business area manager;
- **system changes:** documented Requests for Change authorised by an appropriate business area manager and approved by the Change Manager; records of emergency changes reviewed and signed off by the Change Manager; formal acceptance of completed changes by appropriate business area managers;
- **configuration audits:** documented audits, signed off by Configuration Manager, of comparisons between operational components and those recorded within configuration management records (including checks for unlicensed/unauthorised software on PCs) together with records of what was found and any action taken;
- **business continuity:** documented plans, records of testing and of analysis of test results; logs from computer backup jobs showing notification of successful completion; records of the location of individual backup media (e.g. tapes) and their contents.

Risk Assessment

103. Good practice dictates that there should be some form of *systematic* assessment of the risks faced by an organisation's information systems, and a record of the controls that management have approved for reducing each to acceptable level. It ought to be possible to associate each risk with its related controls or, where management have decided to accept the risk, review their reason(s) for so doing.
104. Documented risk assessment is a requirement for certification against BS 7799.

Personnel security

105. Most security incidents stem directly from the activities of people, and particularly from staff. It follows that it is essential to exercise control over the suitability of people employed (their integrity and professional competence and ability to develop), their training and professional development, their deployment and employment termination (particularly when 'under a cloud').
106. Deployment of staff to key roles within IT (e.g. systems programming; data communications; database administration; development of financial applications) is particularly important because their activities often effect the entire organisation.

Physical and Environmental Security

107. Physical and environmental security addresses the well being of physical ('real-world') information system components. It addresses the risks of physical damage (e.g. from fire, water, lightning/electrical interference and malicious damage), theft, utility failure (power, communications, water, gas) and failure of environmental support systems

Workbook: Review of Information System Controls

where these are required. Although many modern systems do not require a controlled environment (temperature, humidity) this does not apply to large mainframe computers.

108. There will be several 'sensitive areas' in most information systems. These are locations that house components that are key points of failure and as such could be exploited to disrupt a system or gain access to its electronic files. Access to sensitive areas should be restricted to staff who have a legitimate business need, and in high risk situations should be recorded. These include servers and operator consoles; system documentation (which might be employed for attacking the system); media libraries; telecommunications and power distribution equipment; environmental support equipment; printers for producing financial instruments and other sensitive material; and financial stationery stores.
109. Auditors should be aware that staff often move job within an organisation, or act for more senior staff during absence, and in so doing acquire additional access permissions. For this reason it is important that management review individual access permissions periodically and that a change of role automatically triggers a review of access rights. Procedures should also ensure that the access permissions of staff who leave the organisation are removed, and that any keys, physical passes, electronic key cards are recovered and that any passwords known to the leaver are changed.

Logical Access

110. This is access to a computer system's electronic files. These may contain data, software or configuration parameters (e.g. containing user passwords, user's file access permissions). They may also be electronic files in transit, such as e-mail. The risks are that data/software will be subject to unauthorised change ("modification"), corrupted or destroyed; or that confidentiality will be breached which, in the case of passwords, could result in attacks on data integrity and system availability.
111. As with physical security, the principle of 'least privilege' should apply in general, with user access to *sensitive* files and facilities being limited to what is consistent with each individual's employment needs. Auditors should be aware that staff often move job within an organisation, or act for more senior staff during absence, and in so doing acquire additional access permissions. For this reason it is important that management review individual access permissions periodically. Procedures should also ensure that the logical access permissions of staff who leave the organisation are deactivated promptly, and any electronic tokens (e.g. swipe cards, smart cards) used during the logging process are also deactivated.

Software Control

112. There are two aspects to this problem. The first concerns the use of unlicensed software, which can, and increasingly does result in civil actions by software trade associations to recover damages. The second, which is of more immediate concern to financial auditing, is the use of software that attacks data integrity.
113. Some types of system utility programmes (software that is used by IT support staff to maintain the system) can bypass file access controls. Their use should be restricted and monitored. Software is also publicly available that can intercept messages passing over local area networks. Unauthorised software is also a common cause of virus infection.
114. Corporate policy on both software and virus control should be spelled out clearly in the Information Security Policy document.

Workbook: Review of Information System Controls

Business Continuity

115. Business continuity includes the strategy and plans for ensuring that key business processes can be recovered following a system failure or disaster, and within a time frame that minimises damage to business activities. This can include loss of financial control of business operations, and failure to maintain adequate accounting records (the leading case in government is the UK NAO's qualification of the F&CO appropriation accounts for 1989-90).
116. An aspect of information system risk assessment (see above) is to identify the information systems on which the organisation depends, their relative priority and the period of time in which each would need to be recovered (even at reduced efficiency) to avoid significant damage to business operations. Recovery period can range from weeks to hours depending on business needs, or in the case of a highly critical system it may be necessary to ensure continuous operation using a mirrored system. In common with other aspects of information security, business needs must be balanced carefully against the cost of providing continuity, which increases as scope increases and recovery period falls.
117. In addition to risk assessment, and within the context of business need, the broad essentials of business continuity are adequate system backup, availability of accommodation and stationery for users, a formal continuity plan, a management framework for operating and maintaining the plan and periodic testing. An untested continuity plan is unlikely to prove effective, and no amount of continuity planning will help if the system has not been backed up or, as in the case of some disasters, the backups are inaccessible.

Workbook: Review of Information System Controls

Section 3: Supplementary Questions

Overall control objective: systems and services should operate to provide users with reliable information, and to protect information system assets from accidental and deliberate damage

Control objective 3.1: Top management should set a clear direction and demonstrate their support and commitment for information security by defining a corporate information security policy

Consider whether the corporate information security policy is appropriate to the business and is available to, and known by, staff:

- is there an information security policy? Is it written down? Has it been authorised by top management as a statement of corporate policy?
- does the scope of the Policy encompass the entire organisation and all information processing activities?
- how is the policy kept up-to-date with changing business and ICT risks?
- is the Policy effectively communicated to all information users?
- how is the effectiveness of the Policy monitored?

Control objective 3.2: A management framework should be set up to implement information security within the organisation

Consider what action management has taken to ensure that:

- a board member has been appointed to be responsible for security management;
- a representative forum (chaired by a suitably senior member) discusses and takes decisions on matters affecting information security;
- security roles and responsibilities have been clearly defined and included in:
 - *employment contracts?*
 - *control procedures?*
 - *job descriptions?*
- a “system ownership” policy has been implemented;
- specialist security advice is readily available;
- the operation of this management framework is reviewed independently;
- there are effective procedures for reporting, investigating and taking action on security incidents (are “security incidents” clearly defined?);
- data on security incidents is collected from all sources, categorised and periodically analysed to establish trends.

Control objective 3.3: the operation of the system of controls should be auditable

Consider how:

Workbook: Review of Information System Controls

- management obtain assurance that controls work correctly and consistently in practice;
- whether management assurance is based on reliable evidence of control operation.

Control objective 3.4: the system of controls should be appropriate to the type and level of risks to be managed

Consider how management ensures that:

- information system risks are:
 - *identified and assessed (“risk analysis”)*;
 - *adequately managed (“risk management”)*.
- controls are documented and linked to the risk(s) which they are designed to manage;
- the decision not to manage an identified risk (“risk acceptance”) is justified;
- system changes do not render existing controls inoperative, or introduce new risks that existing controls do not address.

Control objective 3.5: security should be addressed in recruitment and leaving procedures, and in contracts and job descriptions. It should also be monitored during employment

Consider:

- how management ensures that potential recruits are unlikely to be prone to human error, theft, fraud or misuse of ICT facilities;
- what procedures apply to the engagement of temporary staff and contractors;
- what security procedures apply to personnel who:
 - *Leave of their own accord or retire;*
 - *Are asked to leave or are dismissed.*
- what formal security related assurances potential employees and leavers are required to provide;
- how staff performance is monitored, recorded and acted on.

Control objective 3.6: ICT facilities should be located in secure areas

Consider how management:

- identifies which facilities need physical entry controls;
- determines:
 - *what types of controls apply (are they sufficiently ‘strong’ for the purpose?);*
 - *who is to have access to the restricted area;*
- restricts and monitors access to key areas, such as:
 - *computers;*
 - *operators’ consoles;*
 - *off-line media;*
 - *telecommunications equipment and distribution frames;*
 - *environmental plant;*
 - *valuable stationery;*

Workbook: Review of Information System Controls

- *output distribution area;*
- *system development area.*
- is alerted to unauthorised access (e.g. intruder detection systems and extended alarms);
- is alerted to attempted unauthorised access (e.g. review of entry logs for repeated access rejection reports).

Control objective 3.7: ICT facilities should be protected from environmental risks

Consider how management:

- determines which facilities need environmental protection and what protection to apply;
- ensures that appropriate environmental protection has been provided for ICT facilities and end-user accommodation:
 - heat and smoke detectors
 - moisture and humidity detectors
 - alarms for the above (out of hours operation).

Control objective 3.8: access to computer systems and data should be controlled on the basis of business needs

Consider how management:

- determines which individuals can access the system and what they can use it for;
- ensures that each user's access permissions remain appropriate to their current business needs;
- removes (or deactivates) the accounts of those who no longer use the system;
- controls the access of highly privileged systems users; for example:
 - *system programmers (e.g. SUPER USER profile);*
 - *computer operators;*
 - *maintenance engineers;*
 - *database administration team;*
 - *system administrators for individual application systems.*
- restricts and monitors access from external sources:
 - *private wide area networks;*
 - *dial-up connections;*
 - *the Internet.*

Control objective 3.9: there should be controls to prevent and detect the introduction of unauthorised software

Consider how management prevents the introduction of unauthorised software. Consider the following possibilities:

- *loaded onto PCs;*
- *loaded onto servers as part of a bespoke software amendment or a vendor update;*

Workbook: Review of Information System Controls

- *downloaded over external connections (e.g. the Internet).*

Consider how management ensures that infringement of software copyright does not occur.

Control objective 3.10: business continuity plans should be available to protect key business processes from the effects of major disruptions, failures and disasters

Consider:

- what action management has taken to identify:
 - *its key financial systems;*
 - *the maximum tolerable period the organisation could exist without them;*
 - *plans for recovering key systems within an acceptable timeframe in the event of prolonged failure, denial of access to the premises, or disaster.*
- the procedures to ensure that software and data can be recovered in the event of their being damaged/corrupted or made unavailable for use;
- how management ensures that data and software can be recovered and used in practice;
- the controls in place to ensure that continuity plans remain workable.

Control objective 3.11: information security should be reviewed regularly for compliance and effectiveness

Consider:

- how management gains assurance that information security policies are being implemented effectively across the organisation;
- the mechanisms for addressing deficiencies in information security implementation and compliance, e.g. bringing information security weaknesses to top management's attention.

Appendix: Threats to Government IT Systems (source: CRAMM)

Fire
Water/moisture damage
Natural disaster (e.g. lightening strike, subsidence, severe weather damage)
Staff shortage
Wilful damage by outsiders
Terrorism
Wilful damage by insiders
Theft by outsiders
Theft by insiders
Masquerading of user identity by outsiders
Masquerading of user identity by contract service providers
Communications infiltration by outsiders
Communications infiltration by contract service providers
Introduction of damaging or disruptive software
Masquerading of user identity by insiders
Communications infiltration by insiders
Unauthorised use of an application
Misuse of resources
Technical failure of network host, or....
Technical failure of non-network host
Technical failure of storage facility
Technical failure of print facility
Technical failure of network management or operations host
Technical failure of network distribution component
Technical failure of network gateway
Technical failure of network interface
Accidental mis-routing
Power failure
Air conditioning failure
Operations error
Application software failure
Hardware maintenance error
Software maintenance error
User error
Technical failure of network services