

Review of Information Systems Development

Name of entity:

Year of account			
Completed/updated by (Initials and date)			
Reviewed by Assignment Manager (Initials and date)			
Reviewed by Assignment Director (Initials and date)			

Purpose

This review is in two parts and follows on from the Review of Information System Controls (NAO 905, Parts 1 -3). The first part deals with information systems development and procurement while the second part is concerned with strategic planning and project management.

Information Systems Development and Procurement (Part 1)

The purpose of the information systems development and procurement review is to assist the entity's management in taking all necessary steps to ensure that new financial information systems are secure, auditable and in all other respects fit for their intended use.

When and How to Review Information Systems Development and Procurement

The Assignment Director should ensure that Part 1 of this package is completed where a new financial information system is to be developed or procured.

The questionnaire should be completed at an early stage during the project planning phase and updated as necessary during project implementation.

Responsibility

The Assignment Director and Manager are responsible for the review of information systems development and for ensuring that the results of the review are reported to the entity's management.

A member of the Information Technology Audit Group (ITAG) may advise the audit team on the conduct of specific aspects of the in-depth review of the entity's installation controls. However, the involvement of ITAG members does not affect the overall responsibility of the Assignment Director and Manager for the conduct, conclusions and reporting of the results of the review.

Strategic Planning and Project Management (Part 2)

Purpose

To ensure that the entity's information systems satisfy, and are justified in terms of, business needs.

When and How to Review Strategic Planning and Project Management

Review of Information Systems Development

This checklist is optional, and should only be completed where the Assignment Director believes its completion will assist client service and add-value.

Responsibility

As for Information Systems Development and Procurement above.

Review of Information Systems Development

Part 1: Information Systems Development and Procurement

Information systems should be secure, auditable and in other respects fit for their intended use

Control action	What are management's procedures to ensure controls operates effectively?	Ref.
1.1 Information systems should be of sufficient quality for the business needs of the organisation		
1.2 Adequate controls and audit facilities should be built into the system		
1.3 Appropriate and workable continuity plans should exist to cover prolonged system failure and disaster		
1.4 Staff who are to be involved with the new system should receive training appropriate to their particular role		
1.5 Any data to be transferred to the new system from an existing system should be transferred completely and accurately		
1.6 Auditing requirements should be taken into account in the formulation of outsourcing contracts		
1.7 Systems and software developed by end-users for business use should comply with appropriate corporate development standards		

Review of Information Systems Development

Part 2: Information Systems Development: Strategic Planning and Project Management

Information systems should satisfy, and be justified in terms of, business requirements

Control action	What are management's procedures to ensure controls operate effectively?	Ref.
2.1 Investment in information and communications technology should be clearly linked to defined business needs		
2.2 Top management should approve investment in information and communications technology, monitor progress and evaluate the outcome		
2.3 The development and use of information and communications technology should follow a consistent direction		
2.4 Projects should be adequately resourced		
2.5 Project aims should be clearly stated and understood, and there should be an effective management framework for delivering them		
2.6 Project risks should be assessed and appropriate management action taken		
2.7 Project expenditure should be monitored and controlled		
2.8 Project outputs should meet defined quality criteria.		

Review of Information Systems Development

Implication of findings for audit strategy	
Assessment of control risk	
Design of audit procedures	
Issues to be reported to management	

Review of Information Systems Development

Review of Information Systems Development and Procurement: Points of focus

1. Information systems should be of sufficient quality for the business needs of the organisation

Consider, for example, the following topics:

- *What action the organisation is taking to ensure that the system will be of adequate quality in terms of its:*
 - *Functionality;*
 - *Data processing performance;*
 - *Responsiveness to on-line users;*
 - *Ease of use;*
 - *Ease of operation;*
 - *Ease of maintenance;*
 - *Ability to interface with other systems.*
- *How the project plan requires end-users to be fully involved in:*
 - *Specifying the system;*
 - *Evaluating design proposals;*
 - *Acceptance testing;*
 - *Significant project management decisions.*

2. Adequate controls and audit facilities should be built into the system

Consider, for example, the following key topics:

- *The adequacy of the Project Plan to ensure that:*
 - *Risks to information security are identified and assessed for likelihood and potential impact;*
 - *Appropriate controls are implemented to reduce such risks to acceptable levels;*
 - *Controls are documented and tested before live use.*
- *How Internal and External Audit satisfy themselves that basic internal control objectives will be met (e.g. system access controls, data processing controls, financial audit trail, backup and recovery).*
- *The procedures for the review and approval of the system's overall security characteristics by the IT Security Officer.*
- *How management appoints the System Owner and System Administrator to oversee day-to-day security management in the operational system.*

Review of Information Systems Development

Review of Information Systems Development and Procurement: Points of focus

3. Appropriate and workable continuity plans should exist to cover prolonged system failure and disaster

Consider, for example, the following key issues:

- *How the criticality of the system, in terms of the maximum tolerable times to restore emergency and full processing, has been established and agreed with the System Owner.*
- *The backing up strategy defined and agreed with the System Owner.*
- *How the business continuity plan has been defined in the Project Plan.*
- *What the responsibilities of the Business Continuity Plan owner are, eg maintenance and testing of the Plan.*
- *The suitability of the off-site facility for the storage of backup media and emergency equipment.*

4. Staff who are to be involved with the new system should receive training appropriate to their particular role

Consider for example the following key issues:

- *The extent to which the new and existing systems and working practices differ, and hence the need for training.*
- *How staff training needs are identified in the project plan.*
- *How the quality of training is to be monitored, in terms of its:*
 - *Timing;*
 - *Relevance, duration and content;*
 - *Delivery.*
- *How the training programme is designed to address the particular needs of:*
 - *The System Owner and System Administrator;*
 - *Managers and senior managers;*
 - *Other end-users;*
 - *ICT support staff;*
 - *System security staff;*
 - *Auditors.*

Review of Information Systems Development

Review of Information Systems Development and Procurement: Points of focus

5. Any data to be transferred to the new system from an existing system should be transferred completely and accurately

Consider, for example:

- *The need for the Project Plan to include timing in respect of transferring (or “migrating”) data.*
- *How data transfer is to be controlled in respect of:*
 - *The completeness and accuracy of the data transferred;*
 - *Correct accounting (e.g. differing charts of accounts).*
- *What procedures are in place to ensure that data cannot be subject to unauthorised change during the transfer process.*
- *How the data is to be kept up-to-date during the period following transfer but before live operation.*

6. Auditing requirements should be taken into account in the formulation of outsourcing contracts

Where financial data is processed under contract, consider, for example, the need for the contract to be formulated to specify:

- *Access for auditing purposes to:*
 - *System facilities, data and documentation;*
 - *Process control records;*
 - *Contractor's staff (for interview).*
- *That the contractor provide and maintain:*
 - *An adequate standard of information security;*
 - *Appropriate backup, recovery and standby procedures and facilities;*
 - *Adequate process control records.*
- *The facilities which allow data to be elected and downloaded from the system.*

Review of Information Systems Development

Review of Information Systems Development and Procurement: Points of focus

7. Systems and software developed by end-users for business use should comply with appropriate corporate development standards

Consider, for example:

- *The awareness of management of the extent of its reliance on end-user produced software and systems.*
- *How management ensures that systems and software built by end-users are not vulnerable to the risk of “key staff” (i.e. only the designer knows where they are, or how they work).*
- *In particular, how management ensures that end-user built systems and software are:*
 - *documented;*
 - *of acceptable quality (i.e. are fit for purpose);*
 - *secure (software, data and documentation is protected from unauthorised use or change);*
 - *adequately backed up, including a copy in remote storage;*
 - *accessible by all those who have legitimate need to use it.*
- *The procedures to ensure that end-user produced reports are:*
 - *Clearly distinguishable from those produced by the core system;*
 - *Clearly attributable to the end-user who produced them.*
- *Where reports and files are produced by “report writers”, how a copy of the record selection parameters is included in the output.*

***Note:** if you are relying on the integrity of end-user produced reports in your audit you will need to be satisfied about the third bullet point above.*

Review of Information Systems Development

Review of Information Systems Strategic Planning and Project Management: Points of focus

1. Investment in information and communications technology should be clearly linked to defined business needs.

Consider, for example, the following key issues:

- *How the organisation's overall business aims and objectives are documented in the business plan.*
- *The regularity with which senior management reviews the organisation's information needs within the context of:*
 - *the stated business aims and objectives.*
 - ***Known risks and constraints.***

2. Top management should approve investment in information and communications technology, monitor progress and evaluate the outcome.

Consider, for example, the following key issues:

- *How the strategy for satisfying corporate information needs is defined.*
- *If there is no strategic plan, how management plans to meet its information needs. Consider, for example:*
 - *the comprehensiveness of its approach;*
 - *its procedures for examining alternative solutions;*
 - *its procedures for examining risks and assumptions;*
 - *its knowledge of costs and benefits;*
 - *its knowledge of lead times.*
- *If there is a strategic plan :*
 - *What the process is for senior management approval;*
 - *How management ensures it is kept up-to-date;*
 - *How the business case supports the plan by examining and explaining:*
 - ◇ *important planning assumptions;*
 - ◇ *alternative solutions;*
 - ◇ *business and technical risks;*
 - ◇ *costs and benefits;*
 - ◇ *delivery times.*

Review of Information Systems Development

Review of Information Systems Strategic Planning and Project Management: Points of focus

- *How management ensures that the strategy covers foreseeable information requirements (e.g. over the next 3-5 years).*
- *Senior management's procedures for:*
 - *Monitoring delivery of the strategy;*
 - *Evaluating the return on its investment in ICT.*

3. The development and use of information and communications technology should follow a consistent direction.

Consider, for example, how management ensures that:

- *It provides adequate direction and guidance to project teams on the development of new systems.*
- *New systems will be able to exchange data with existing systems, and with trading partners' systems where necessary.*
- *Suitable methods are used for designing and building new systems.*
- *The range of technical and managerial skills required is kept to a minimum.*
- *New systems can be maintained efficiently in operational use.*
- *New systems will be of acceptable quality.*
- *Adequate attention is paid to information security and business continuity during system development.*
- *Bought-in systems and equipment will interface adequately with those that already exist.*

4. Projects should be adequately resourced.

Consider, for example, the following key issues:

- *The procedures for drawing up and approving a comprehensive estimate of project costs in line with the original business case.*
- *How the following costs have been evaluated in the estimate:*
 - *Training;*
 - *Testing (parallel running ought to be considered);*
 - *Data migration;*
 - *Security/continuity.*

Review of Information Systems Development

Review of Information Systems Strategic Planning and Project Management: Points of focus

- *Whether the project management team considers project funding to be adequate. If not, consider the basis of its reservations.*
- *How management ensures that the project backed by sufficient skill and experience in:*
 - *project management;*
 - *information and communications technology;*
 - *procurement/contracting;*
 - *project accounting;*
 - *end-user requirements and activities.*
 - *the client's willingness and ability to buy additional skills where necessary.*

5. Project aims should be clearly stated and understood, and there should be an effective management framework for delivering them

Consider, for example, how management ensures that:

- *There is a clear and common understanding of:*
 - *what the project is to achieve;*
 - *within what constraints;*
 - *project risks.*
- *All significant stakeholders in the project will participate:*
 - *in key project management decisions;*
 - *in project activities, where appropriate.*
- *There is a single, recognised manager to control day-to-day activities with adequate authority to control resources.*
- *The roles and responsibilities of project team members are clearly defined.*
- *The project will be monitored in terms of:*
 - *Expenditure;*
 - *Quality of outputs;*
 - *Progress against deadline.*
- *The main steps to be taken during the project are documented in a Project Plan, which has been approved at an appropriate management level.*

Review of Information Systems Development

Review of Information Systems Strategic Planning and Project Management: Points of focus

6. Project risks should be assessed and appropriate management action taken

Consider, for example, the following key issues:

- *How project risks have been identified and assessed in terms of their likelihood and impact on project goals.*
- *The procedures for ensuring that the risk assessment is:*
 - *Comprehensive;*
 - *Periodically reviewed and updated.*
- *How the project management team consider risk management recommendations made and the action to be taken.*

7. Project expenditure should be controlled

Consider, for example, the following key issues:

- *How management ensures that reliable information on the costs of project activities and procurement is readily available.*
- *How budgets have been set up for individual project outputs.*
- *The procedures for comparing expenditure with budget on a regular basis.*
- *How regular project outturn reports are communicated to management.*
- *The adequacy of the separation of roles between the project management, procurement, and project accounting functions*

8. Project outputs should meet defined quality criteria

Consider, for example, the following key issues:

- *How quality criteria for project outputs are specified.*
- *The procedures for ensuring that quality criteria are consistent with the organisation's system development standards.*
- *How management ensures that project outputs (which may be services, rather than 'hard' deliverables) meet these criteria.*
- *How management controls changes to:*
 - Defined quality criteria;*
 - sub-standard outputs.*

Review of Information Systems Development

Review of Information Systems Strategic Planning and Project Management: Points of focus

- *The appropriateness of end-users involved in specifying quality criteria and in monitoring the quality of project outputs.*