

# Review of Information System Controls

**Name of entity:**

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

## Purpose

The purpose of the information systems controls review guide is to:

- i) obtain and document a general understanding of the information systems environment in which the entity's financial applications operate; and
- ii) Identify the nature and extent of risk to financial reporting posed by the entity's use of information technology.

Weaknesses in the entity's overall computer environment may adversely affect the integrity and availability of all the underlying financial applications.

## When and How to Review Information Systems

The review of information system controls should be used in conjunction with the assessment of the control environment (NAO 900, Part C) and review of application controls (NAO 910) to assess whether the entity's internal controls provide a sound basis for maintaining accounting records and internal financial controls.

It is recommended that an in-depth review of information systems controls is performed once every (three) years, subject to there being no significant changes in the computer environment.

# Review of Information System Controls

Where the overall assessment of information systems environment is sound, the annual review of the assessment should focus on the high level monitoring procedures performed by management and recorded on the review of monitoring controls.

The review of information system controls form is in three parts.

Part 1 Change and Configuration Management

Part 2 Operations and Management

Part 3 System Security and Business Continuity.

## **Responsibility**

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

## **Information Systems Development and Procurement**

Where a new financial information system is to be developed or procured, the Assignment Director should ensure that NAO 906 (Part 1) of the review of information systems development questionnaire is also completed.

The questionnaire should be completed at an early stage in the project planning and reviewed throughout project implementation as necessary. Its purpose 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.

## **Strategic Planning and Project Management**

An additional questionnaire relating to strategic planning and information systems development (NAO 906, Part 2) is also available. This checklist is optional, and should only be completed where the Assignment Director believes that its completion will assist client service by adding value to the audit.

## Review of Information System Controls

**Part 1: Change and configuration management: 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	What are management's procedures to ensure that controls operate effectively?	Ref.
1.1 Changes to IT systems should be controlled on the basis of documented change management procedures		
1.2 Requests for Change should be documented, authorised and recorded		
1.3 Requests for change should be reviewed to identify consequential risks to the correct operation of the system		
1.4 System changes should be appropriately authorised		
1.5 Change management procedures should pay due regard to an effective separation of roles		
1.6 Authorised changes should be managed to completion		
1.7 Emergency changes should comply with normal change management requirements as soon as possible		
1.8 Configuration management records should accurately describe the live configuration and it's status history		

## Review of Information System Controls

**Part 2: Information system operations and maintenance: Computers and networks shall be operated in a secure manner, and provide a sufficient level of service to satisfy business needs**

Control objective	What are management's procedures to ensure controls operate effectively?	Ref.
2.1 Computer operations should be performed competently		
2.2 Incompatible roles should be separated to the extent practicable		
2.3 All system operations should be authorised and serve legitimate business needs		
2.4 Data input for processing should be valid, complete and accurate		
2.5 Financial stationery should be stored securely and its use accounted for		
2.6 Outputs should be complete and accurate, and distributed promptly to the correct recipient(s)		
2.7 System backups should be readable and their use accounted for		
2.8 The level of service provided should be consistent with business needs		
2.9 There should be a focal point for reporting, recording and resolving incidents and operational failures		

## Review of Information System Controls

<b>Control objective</b>	<b>What are management's procedures to ensure controls operate effectively?</b>	<b>Ref.</b>
2.10 Data stored in multi-user databases should be reliable and available for use when required		

## Review of Information System Controls

**Part 3: Information Security Management: Systems and services should operate to provide users with reliable information and to protect information system assets from accidental and deliberate damage**

Control action	What are management's procedures to ensure controls operate effectively?	Ref.
3.1 Top management should set a clear direction, and demonstrate its support and commitment to information security by defining a corporate information security policy		
3.2 A management framework should be set up to implement information security within the organisation		
3.3 The operation of the system of controls should be auditable		
3.4 The system of controls should be appropriate to the type and level of risks to be managed		
3.5 Security should be addressed in recruitment and leaving procedures, and in contracts and job descriptions. It should also be monitored during employment		
3.6 ICT facilities should be located in secure areas		
3.7 ICT facilities should be protected from environmental risks		

## Review of Information System Controls

<b>Control action</b>	<b>What are management's procedures to ensure controls operate effectively?</b>	<b>Ref.</b>
3.8 Access to computers/systems and data should be controlled on the business of business needs.		
3.9 There should be controls to prevent and detect the introduction of unauthorised software		
3.10 Business continuity plans should be available to protect key business processes from the effects of major disruptions, failures and disasters		
3.11 Information security should be reviewed regularly for compliance and effectiveness		

## Review of Information System Controls

<b>Implication for Audit Strategy</b>	
<b>Interim risk assessment</b>	
<b>Control risk assessment</b>	
<b>Design of audit procedures</b>	
<b>Issues to be reported to management</b>	