

Part 3

Information Security Management

Systems and services should operate to provide users with reliable information when required, and protect information system assets from accidental and deliberate damage.

Control objective	Controls	Workbook
<p>1. Top management should set a clear direction, and demonstrate their support and commitment for information security by defining a corporate information security policy</p>	<p><i>Is there a written corporate information security policy?</i></p> <p><i>Is it appropriate?</i></p> <p><i>Is it available to all staff?</i></p>	<p>Risks – high risk of security failures due to inadequate -</p> <ul style="list-style-type: none"> - awareness of risks - priority - resources - direction - authority to implement policy <p><i>Lack of commitment at lower levels of management</i></p> <p><i>Discussion on –</i></p> <ul style="list-style-type: none"> - the need for a formal policy - the need for top management commitment - minimum guidance - review and maintenance
<p>2. A management framework should be set up to implement information security within the organisation</p>	<p><i>Has a board member been appointed to be responsible for security management?</i></p> <p><i>Does a representative forum discuss and take decisions on matters affecting information security? Is it chaired by a suitably senior manager?</i></p> <p><i>Have security roles and responsibilities been clearly defined and included in –</i></p> <ul style="list-style-type: none"> - employment contracts? - control procedures? - job descriptions? <p><i>Has a “system ownership” policy been implemented?</i></p> <p><i>Is specialist security advice readily available?</i></p> <p><i>Is the operation of this management framework reviewed independently?</i></p>	<p>Risks – high risk of security failures due to -</p> <ul style="list-style-type: none"> - lack of accountability - ineffective policy - unallocated tasks - lack of professional advice - non-compliance with policy or best practice <p><i>Discussion on typical roles and responsibilities, and management framework</i></p> <p><i>System ownership</i></p>

Part 3

Information Security Management

Control objective	Controls	Workbook
<p>3. The operation of the system of controls should be auditable</p>	<p><i>What ensures that it is possible to verify the correct and consistent operation of controls retrospectively?</i></p> <p><i>Does this requirement cover all aspects of control which require active management?</i></p> <p><i>Do process control records provide adequate evidence of the operation of controls?</i></p>	<p>Risks – security failures due to an inability to detect -</p> <ul style="list-style-type: none"> - non-compliance with policy requirements and procedures - failure to take or follow up policy decisions - incorrect or inconsistent operation of controls <p><i>Record keeping</i></p> <p><i>Documented controls</i></p> <p><i>Process control records</i></p> <p><i>Change management</i></p>
<p>4. The system of controls should be appropriate to the type and level of risks to be managed</p>	<p><i>How does management ensure that information system risks are -</i></p> <ul style="list-style-type: none"> - identified and assessed? - adequately managed? <p><i>Have controls –</i></p> <ul style="list-style-type: none"> - been documented? - linked to the risk(s) which they are designed to manage? <p><i>Are there any risks which management have decided would not be cost effective to control? Is there adequate justification for these decisions?</i></p>	<p>Risks –</p> <ul style="list-style-type: none"> - unmanaged risks - inability to verify the adequacy of control - unrecorded decisions on the rationale underlying risk management <p><i>ICT risk assessment and risk management</i></p> <p><i>Link to system of controls</i></p> <p><i>Cost-effective controls and risk acceptance</i></p>

Part 3

Information Security Management

Control objective	Controls	Workbook
<p>5. Security should be addressed in recruitment and leaving procedures, and in contracts and job descriptions. It should also be monitored during employment</p>	<p><i>How do management ensure that potential recruits are unlikely to be prone to human error, theft, fraud or misuse of ICT facilities?</i></p> <p><i>What procedures apply to the engagement of temporary staff and contractors?</i></p> <p><i>What security procedures apply to personnel who –</i></p> <ul style="list-style-type: none"> - <i>leave of their own accord or retire?</i> - <i>are asked to leave or are dismissed?</i> <p><i>What formal security related assurances are potential employees and leavers required to provide?</i></p> <p><i>How is staff performance monitored, recorded and acted on?</i></p>	<p><i>Risks – incompetence, theft, fraud, blackmail and misuse of facilities. Security is more likely to be compromised by staff who have a record of being psychologically unstable or untrustworthy, or do not have the skills, qualifications and experience that they claim.</i></p> <p><i>Recruitment and leaving procedures. Background checking. Monitoring and reporting. Typical checks.</i></p> <p><i>Job descriptions, contracts of employment and written declarations on starting and leaving</i></p> <p><i>Risks associated with key ICT staff.</i></p>
<p>6. ICT facilities should be located in secure areas</p>	<p><i>How do management identify which facilities need physical entry controls?</i></p> <p><i>How do management determine –</i></p> <ul style="list-style-type: none"> - <i>what protection to apply?</i> - <i>who is to have access?</i> <p><i>How is access restricted to key areas, e.g. –</i></p> <ul style="list-style-type: none"> - <i>computers?</i> - <i>operators' consoles?</i> - <i>off-line media?</i> - <i>telecomms equipment and distribution frames?</i> - <i>environmental plant?</i> - <i>valuable stationery?</i> - <i>output distribution area?</i> - <i>system development area?</i> <p><i>How are management alerted to unauthorised access?</i></p>	<p><i>Risks –</i></p> <ul style="list-style-type: none"> - <i>theft of data</i> - <i>theft of equipment</i> - <i>interference with equipment and data</i> - <i>malicious damage</i> <p><i>Risk assessment</i></p> <p><i>Typical risk areas</i></p> <p><i>Control in depth</i></p> <p><i>Monitoring and response – time to respond</i></p> <p><i>Testing controls</i></p>

Part 3

Information Security Management

Control objective	Controls	Workbook
<p>7. ICT facilities should be protected from environmental risks</p>	<p>How do management determine –</p> <ul style="list-style-type: none"> - which facilities need environmental protection? - what protection to apply? <p>Has adequate environmental protection been provided for –</p> <ul style="list-style-type: none"> - ICT facilities? - end-user accommodation? 	<p>Risks – system disruption and damage due to –</p> <ul style="list-style-type: none"> - fire - water - power failure - vibration, dust - power surges, lightning - electrical supply interference <p>Detection, alarm, response</p> <p>Typical controls</p> <p>Testing controls</p>
<p>8. Access to systems and data should be controlled on the basis of business needs</p>	<p>What determines –</p> <ul style="list-style-type: none"> - which individuals can access the system? - what they can use it for? <p>How do management -</p> <ul style="list-style-type: none"> - restrict physical access? - authorise physical access? - monitor physical access? <p>How do management -</p> <ul style="list-style-type: none"> - restrict logical access? - authorise logical access? - monitor system use? <p>How is access to key system facilities controlled? e.g. to the following profiles –</p> <ul style="list-style-type: none"> - SUPER USER - Operator - Engineer - Database Administrator <p>How is access restricted and monitored from –</p> <ul style="list-style-type: none"> - wide area networks? - dial-up connections? - the Internet? <p>Are access controls –</p> <ul style="list-style-type: none"> - sufficient/adequate? - documented & assigned? <p>auditable?</p>	<p>Risks – unauthorised access resulting in –</p> <ul style="list-style-type: none"> - alteration of – <ul style="list-style-type: none"> - data - software - system operation - deletion of software and data - system failure <p>Access control policy</p> <p>Ownership of controls</p> <p>Security profiles and least privilege</p> <p>Infrastructure systems</p> <p>Trusted and untrusted processes and networks</p> <p>Typical access controls –</p> <ul style="list-style-type: none"> - physical - logical <p>Firewalls</p>

Part 3

Information Security Management

Control objective	Controls	Workbook
<p>9. There should be controls to prevent and detect the introduction of unauthorised software</p>	<p><i>How do management prevent the introduction of unauthorised software?</i></p> <p><i>Consider the following possibilities –</i></p> <ul style="list-style-type: none"> - on PCs? - during software changes and updates? - over external connections? <p><i>How do management monitor software use?</i></p>	<p><i>Risks – damage to data and disruption to processing activities by -</i></p> <ul style="list-style-type: none"> - computer virus - Trojan Horse - Worms - mail attachments - unauthorised programs <p><i>Typical controls –</i></p> <ul style="list-style-type: none"> - virus checking - PC inspections - change and configuration management - code audit - restrictions on access to software development tools
<p>10. Business continuity plans should be available to protect key business processes from the effects of major disruptions, failures and disasters</p>	<p><i>Have management identified</i></p> <ul style="list-style-type: none"> - their key financial systems? - the maximum tolerable period they could exist without them? - suitable plans for recovering key systems in the event of – <ul style="list-style-type: none"> - prolonged failure? - denial of access or disaster? <p><i>What ensures that software and data can be recovered in the event of their being –</i></p> <ul style="list-style-type: none"> - damaged/corrupted? - made unavailable for use? <p><i>How do management ensure that data and software can be recovered in practice?</i></p> <p><i>What ensures that continuity plans remain workable?</i></p>	<p><i>Risks – unavailability of financial systems leading to loss of accountability.</i></p> <p><i>Risk assessment – identification of key systems, maximum tolerable unavailability, minimum time to recover. Backing up.</i></p> <p><i>Continuity strategies.</i></p> <p><i>Continuity plans – what they should include. Testing. Link to change management.</i></p> <p><i>Ownership</i></p>

Part 3

Information Security Management

Control objective	Controls	Workbook
<p>11. Information security should be reviewed regularly for compliance and effectiveness</p>	<p><i>How do management gain assurance that information security policies are being implemented effectively across the organisation?</i></p> <p><i>Is there an adequate mechanism for addressing deficiencies in information security implementation and compliance? For example, are weaknesses brought to top management's attention?</i></p>	<p><i>Risks – security failures due to –</i></p> <ul style="list-style-type: none"> - <i>inadequate policy implementation</i> - <i>non-compliance with procedures</i> - <i>new unmanaged risks</i> <p><i>Periodic review –</i></p> <ul style="list-style-type: none"> - <i>by System Owners</i> - <i>independent</i> - <i>role of ISO 9000 and BS7799</i> <p><i>Need for technical review skills. Control of audit tools.</i></p> <p><i>Reporting and remedial action</i></p>