

## Part 2

### Computer and Network Operations

**Computers and networks shall be operated in a secure manner, and provide a sufficient level of service to satisfy business needs**

<b>Control objective</b>	<b>Controls</b>	<b>Workbook</b>
<p><b>1. Computer operations should be performed competently</b></p>	<p><i>How do management ensure that operators are competent to perform their tasks?</i></p> <p><i>Are roles and responsibilities for managing and operating computers and networks –</i></p> <ul style="list-style-type: none"> <li>- <i>clearly allocated?</i></li> <li>- <i>included in job descriptions and contracts?</i></li> </ul> <p><i>Have system operating procedures been approved by management? Are they documented?</i></p> <p><i>For example –</i></p> <ul style="list-style-type: none"> <li>- <i>starting up and shutting down systems?</i></li> <li>- <i>re-organising disc usage?</i></li> <li>- <i>backing up and restoring?</i></li> <li>- <i>transferring backups to remote store?</i></li> <li>- <i>scheduling batch processes and amending schedules?</i></li> <li>- <i>action to take for computer and network failures?</i></li> <li>- <i>migrating new and changed software into live use?</i></li> </ul> <p><i>How do management ensure that documentation is complete and up-to-date?</i></p> <p><i>What ensures that individual applications –</i></p> <ul style="list-style-type: none"> <li>- <i>can be operated correctly?</i></li> <li>- <i>that applications that do not run correctly are identified and remedial action taken?</i></li> </ul>	<p><b>Risks – process failure through -</b></p> <ul style="list-style-type: none"> <li>- <i>inadequate supervision</i></li> <li>- <i>failure to allocate tasks</i></li> <li>- <i>inappropriate operating procedures</i></li> <li>- <i>lack of written guidance</i></li> <li>- <i>deliberate system misuse</i></li> </ul> <p><i>The role of computer and network operations</i></p> <p><i>Allocation of roles and responsibilities. Job descriptions.</i></p> <p><i>Document management principles</i></p> <p><i>Operating infrastructure systems</i></p> <p><i>Operating application systems – job instructions, exception reports</i></p> <p><i>Infrequent processes</i></p>

## Part 2

### Computer and Network Operations

<b>Control objective</b>	<b>Controls</b>	<b>Workbook</b>
<p><b>2. All system operations should be authorised and serve legitimate business needs</b></p>	<p><i>What ensures that computer processes are authorised to be carried out?</i></p> <p><i>What role to senior operations managers play in authorising and reviewing computer and network operations?</i></p> <p><i>How would management detect unauthorised activities?</i></p> <p><i>Do all processes have a recognised owner? How would unrecognised processes be dealt with?</i></p>	<p><b>Risks –</b></p> <ul style="list-style-type: none"> <li>- wasteful use of computer time</li> <li>- theft of computer time</li> <li>- hacking, leading to risks to data integrity, availability and confidentiality</li> </ul> <p><i>Job planning and scheduling</i></p> <p><i>Logging and log review</i></p> <p><i>Process ownership</i></p>
<p><b>3. Financial stationery should be stored securely and its use accounted for</b></p>	<p><i>Does the installation use computer printed cheques, payable orders, licenses, permits, or any form of output that is valuable?</i></p> <p><i>How do management ensure that valuable output forms are not tampered with or stolen?</i></p>	<p><b>Scope -</b></p> <ul style="list-style-type: none"> <li>- tapes/discs/fiche/microfilm</li> <li>- important reports</li> <li>- cheques/payable orders</li> <li>- licenses/permits</li> </ul> <p><i>Secure storage</i></p> <p><i>Accounting for use including waste</i></p>

## Part 2

### Computer and Network Operations

<b>Control objective</b>	<b>Controls</b>	<b>Workbook</b>
<p><b>4. Centrally produced outputs should be distributed promptly to the correct recipient</b></p>	<p><i>How do operators know what outputs to expect?</i></p> <p><i>What ensures that outputs are complete?</i></p> <p><i>How do operators know who the correct recipients are?</i></p> <p><i>How are defective or unidentified outputs dealt with?</i></p> <p><i>What ensures that outputs are not duplicated?</i></p> <p><i>Are outputs awaiting distribution stored securely in relation to their value or sensitivity?</i></p>	<p><b>Risks</b> : output is -</p> <ul style="list-style-type: none"> <li>- incomplete</li> <li>- stolen</li> <li>- altered</li> <li>- not distributed</li> <li>- not distributed promptly</li> <li>- distributed to wrong destination</li> <li>- distributed more than once</li> </ul> <p><i>Report identifiers</i></p> <p><i>Distribution lists</i></p>
<p><b>5. There should a focal point for reporting, recording and resolving incidents and operational failures</b></p>	<p><i>What ensures that incidents that affect the quality of service receive attention?</i></p> <p><i>How do management decide what action to take on an incident?</i></p> <p><i>What ensures that problems are dealt with according to their impact on service delivery?</i></p> <p><i>What ensures that incidents selected for remedial action are fixed -</i></p> <ul style="list-style-type: none"> <li>- correctly?</li> <li>- in line with quality standards?</li> <li>- within an acceptable deadline?</li> </ul> <p><i>Are incident and problem statistics gathered, and if so what use is made of them?</i></p>	<p><i>Incidents and problems – definitions.</i></p> <p><i>Incident reporting, classification and recording.</i></p> <p><i>Brief discussion on –</i></p> <ul style="list-style-type: none"> <li>- problem management</li> <li>- change management</li> <li>- configuration management</li> </ul> <p><i>Escalation</i></p> <p><i>Analysis of incident statistics.</i></p>

## Part 2

### Computer and Network Operations

<b>Control objective</b>	<b>Controls</b>	<b>Workbook</b>
<p><b>6. Centrally produced outputs should be distributed promptly to the correct recipient</b></p>	<p><i>How do operators know what outputs to expect?</i></p> <p><i>What ensures that outputs are complete?</i></p> <p><i>How do operators know who the correct recipients are?</i></p> <p><i>How are defective or unidentified outputs dealt with?</i></p> <p><i>What ensures that outputs are not duplicated?</i></p> <p><i>Are outputs awaiting distribution stored securely in relation to their value or sensitivity?</i></p>	<p><b>Risks</b> : output is -</p> <ul style="list-style-type: none"> <li>- incomplete</li> <li>- stolen</li> <li>- altered</li> <li>- not distributed</li> <li>- not distributed promptly</li> <li>- distributed to wrong destination</li> <li>- distributed more than once</li> </ul> <p>Scope -</p> <ul style="list-style-type: none"> <li>- tapes/discs/fiche/microfilm</li> <li>- important reports</li> <li>- cheques/payable orders</li> <li>- licenses/permits</li> </ul>
<p><b>7. Offline media should be readable, stored securely and its use accounted for</b></p>	<p><i>What ensures that management know –</i></p> <ul style="list-style-type: none"> <li>- which storage units contain what data and program files?</li> <li>- the whereabouts of individual storage units?</li> <li>- that software and data held off-line can be read or recovered?</li> </ul> <p><i>What ensures that access to programs and data stored on off-line media is restricted to appropriately authorised staff?</i></p> <p><i>Are backup copies held in remote stores afforded adequate protection from unauthorised access?</i></p>	<p><b>Risks –</b></p> <ul style="list-style-type: none"> <li>- incorrect version used</li> <li>- loss, theft, modification</li> <li>- unavailability of data</li> <li>- media degradation</li> <li>- environment</li> </ul> <p><i>Tapes, magnetic and optical discs</i></p> <p><i>Secure storage</i>  <i>Media librarian</i>  <i>Media accounting and audit</i>  <i>Data held off-site</i></p>

## Part 2

### Computer and Network Operations

Control objective	Controls	Workbook
<p><b>8. Data stored within multi-user databases should be reliable and available for use when required</b></p>	<p><i>What ensures that the following are known –</i></p> <ul style="list-style-type: none"> <li>- <i>the description and meaning of items stored within the database?</i></li> <li>- <i>logical relationship between items?</i></li> </ul> <p><i>What ensures that the database and its associated applications remain compatible following changes to either of them?</i></p> <p><i>What ensures that any corruptions to data or to the logical database structure are promptly detected?</i></p> <p><i>Are changes to the database structure, or its contents or physical storage subject to change management procedures?</i></p> <p><i>What ensures that data items cannot be accessed or amended without proper authority?</i></p> <p><i>Is data backed up at a frequency sufficient to meet business needs? Has this been approved by the end users?</i></p> <p><i>How often is the database recovered from backup? Does recovery properly?</i></p> <p><i>How does management satisfy themselves that the database is being properly administered?</i></p>	<p><i>Discussion on risks –</i></p> <ul style="list-style-type: none"> <li>- <i>uncontrolled change</i></li> <li>- <i>unauthorised access</i></li> <li>- <i>unavailability</i></li> <li>- <i>backup, recovery and restart</i></li> <li>- <i>key staff</i></li> </ul> <p><i>Database Administrator function</i></p> <p><i>Change management</i></p> <p><i>Access to database utilities</i></p> <p><i>Supervision of activities</i></p>

## Part 2

### Computer and Network Operations

<b>Control objective</b>	<b>Controls</b>	<b>Workbook</b>
<p><b>9. The level of service provided should be consistent with business needs</b></p>	<p><i>Is the level of service to be provided to end users defined in a formal agreement?</i></p> <p><i>How do management monitor the level of service provided?</i></p> <p><i>Does the level of service provided meet defined targets?</i></p> <p><i>Is the level of service provided sufficient to meet business needs?</i></p> <p><i>Are the end-users consulted in setting service delivery targets?</i></p> <p><i>What procedures exist for addressing inadequate service delivery?</i></p>	<p><i>Service availability –</i></p> <ul style="list-style-type: none"> <li>- response times</li> <li>- volumes</li> <li>- help desk availability</li> <li>- time to respond to enquiries</li> <li>- time to fix faults</li> </ul> <p><i>Service level agreements</i></p> <p><i>Monitoring service levels</i></p>