

# Business Continuity Planning

## AUDIT PROGRAM & INTERNAL CONTROL QUESTIONNAIRE

### The Information Systems Audit and Control Association

With more than 23,000 members in over 100 countries, the Information Systems Audit and Control **Association**® (ISACA™) is a recognized global leader in IT governance, control and assurance. Founded in 1969, ISACA sponsors international conferences, administers the globally respected CISA® (Certified Information Systems Auditor™) designation earned by more than 25,000 professionals worldwide, and develops globally applicable information systems (IS) auditing and control standards. An affiliated **foundation** undertakes the leading-edge research in support of the profession. The **IT Governance Institute**, established by the association and foundation in 1998, is designed to be a "think tank" offering presentations at both ISACA and non-ISACA conferences, publications and electronic resources for greater understanding of the roles and relationship between IT and enterprise governance.

### Purpose of These Audit Programs and Internal Control Questionnaires

One of the goals of ISACA's Education Board is to ensure that educational products developed by ISACA support member and industry information needs. Responding to member requests for useful audit programs, the Education Board has recently released audit programs and internal control questionnaires on various topics for member use through the member-only web site and K-NET. These products are intended to provide a basis for audit work.

E-business audit programs and internal control questionnaires were developed from material recently released in ISACA's *e-Commerce Security Technical Reference Series*. These technical reference guides were developed by Deloitte & Touche and ISACA's Research Board and are recommended for use with these audit programs and internal control questionnaires.

Audit programs and internal questionnaires on other subjects were developed by ISACA volunteers and reviewed and edited by the Education Board. The Education Board cautions users not to consider these audit programs and internal control questionnaires to be all-inclusive or applicable to all organizations. They should be used as a starting point to build upon based on an organization's constraints, policies, practices and operational environment.

### **Disclaimer**

The topics developed for these Audit Programs and Internal Control Questionnaires have been prepared for the professional development of ISACA members and others in the IS Audit and Control community. Although we trust that they will be useful for that purpose, ISACA cannot warrant that the use of this material would be adequate to discharge the legal or professional liability of members in the conduct of their practices.

September 2001

**Business Continuity Planning  
Audit Program/ICQ**

<b>Get Preliminary Information</b>	
<i>Procedure Step: Policies</i>	
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Determine and obtain copies of all applicable policies for disaster recovery and business continuity, if any.</li> </ul>	
<i>Procedure Step: Get Applicable Documentation</i>	
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Obtain a copy of the organization's disaster recovery plan.</li> <li>• Obtain a list of implementation team members list.</li> <li>• Obtain a current copy of the organization chart.</li> <li>• Obtain current inventory list.</li> <li>• Obtain a copy of agreements relating to use of backup facilities.</li> </ul>	
<i>Procedure Step: Control Questionnaire</i>	<p><i>Objective:</i> To verify that the disaster recovery plan is adequate to insure resumption of computer systems in a timely manner during adverse circumstances, is in line with the current business continuation plan, and reflects the current business operating environment.</p>

## **Business Continuity Planning Audit Program/ICQ**

### ***Details/Test:***

- Is there a disaster recovery plan?
  - If a plan exists, when was it last updated?
- What are your procedures for updating the plan?
- Who is responsible for administration or coordination of the plan?
- Is the plan administrator/coordinator responsible for keeping the plan up-to-date?
- Is there a disaster recovery implementation team (i.e., the first response team members who will react to the emergency with immediate action steps)?
- Where is the disaster recovery plan stored? (Verify that key team members have copies of the plan at home as well as at the office).
- Where are the implementation team contacts list stored? (Suggest each key team member should have contact names and addresses of all other key team members both on his person and at home, as well as in the office - contact numbers should include home and mobile as well as office number)
- Where is the backup facility site?
  - Are there alternate sites? (Be suspicious of loose arrangements with local businesses!)
- What is your schedule for testing and training on the plan?
- When was the last drill performed? (Consider the adequacy of the test - a "desk test" is unlikely to reveal many potential problems)
- Did the drill include use of the backup facilities?
  - If not, when were the backup facilities last used?
  - If over 1 year, how has the organization determined that its programs can still run on the backup equipment?
- What was the outcome of the drill?
  - How did it improve preparedness?
- What critical systems are covered by the plan?
- Does the plan clearly indicate priorities for system restoration, based on risk to the business in particular?
  - Does the plan allow for the restoration within pre-determined "business critical" time frames? (I.e. If certain systems are down for longer than a predetermined time, restoration after this time may be useless if the business has already gone under.)

## Business Continuity Planning Audit Program/ICQ

### *Details/Test (continued):*

- Does the plan indicate the operational requirements for each of the systems?
- What systems are not covered by the plan?
  - Why not?
- What equipment is not covered by the plan?
  - Why not?
- Does the plan operate under any assumptions?
  - What are they?
- What are the procedures for activation of the plan?
- Are inventories as they relate to your critical systems kept (including LAN servers and communication devices)? (Critically, are the procedures and practices for keeping them up to date sufficient?)
- If inventories are kept, where are they stored?
- Are there formal procedures that specify backup procedures and responsibilities?
- What functions/systems/components are covered under such procedures?
- What training has been given to personnel in using backup equipment and established procedures?
- Where is the off-site storage site?
- Are the responsibilities for each team documented?
- Are the restoration procedures documented?
- Does the documentation for each system to be recovered indicate the process flow and as well as the equipment that will be recovered? (i.e. for an application that makes use of desktop equipment for data entry and client server equipment for storage this should all be documented along with the software that will be required.

### **Backup Processes**

#### ***Procedure Step: Backup and Recovery***

##### *Details/Test:*

- Review the backup procedures followed for each area covered by the DRP.
- Determine if the backup and recovery procedures are being followed.

#### ***Procedure Step: Cross Training***

##### *Details/Test:*

- Interview IS personnel to determine if they have been cross-trained.
- Review training records to determine the amount of cross training provided.

### **Off-site Storage**

#### ***Procedure Step: Visit Off-site Storage***

##### *Details/Test:*

- Take a tour of the off-site storage facility. Determine if the facility is adequate.

## Business Continuity Planning Audit Program/ICQ

<b><i>Procedure Step: Rotation Practices</i></b>
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Compare the log of items stored at the facility with the items present at the facility.</li> <li>• Determine if the log is complete and up-to-date.</li> <li>• Confirm procedures to ensure that ALL data required by the business units to be sent to the offsite facility is actually sent and received - i.e. more than simply confirming that they hold what the log says they have received.) <ul style="list-style-type: none"> <li>- How often is the log reviewed for completeness?</li> <li>- Is this adequate?</li> </ul> </li> </ul>
<b>Disaster Recovery Plan</b>
<b><i>Procedure Step: Review Plans</i></b>
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Obtain and review a copy of the disaster recovery plan and the alternate site agreement.</li> <li>• Determine if they are complete and current, and if executive management has signed off on the plan. A key point would be provision for formal update reviews to be signed off (e.g. every six months). Just signing off the original plan would probably be insufficient control. <ul style="list-style-type: none"> <li>- Will all systems be recovered at one disaster recovery site?</li> <li>- If not how will the information be coordinated to ensure that it will be available at the other locations when necessary?</li> </ul> </li> </ul>
<b><i>Procedure Step: Review Responsible Parties</i></b>
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Determine who was responsible in developing the plan and if users and all facets of data processing were adequately involved in its development.</li> </ul>
<b><i>Procedure Step: Risk Assessment</i></b>
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Determine if a risk assessment has been prepared and if it appears reasonable.</li> </ul>
<b><i>Procedure Step: Testing of Plan</i></b>
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Determine if executive management has approved the funding for an alternate data processing center and testing of the disaster recovery plan. <ul style="list-style-type: none"> <li>- Observe a test of the plan.</li> </ul> </li> </ul>
<b><i>Procedure Step: Review Results of Tests</i></b>
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Review the results of the test of the disaster recovery plan.</li> <li>• Determine if corrective action has been taken on any problems incurred during the test.</li> </ul>
<b><i>Procedure Step: Alternate Processing</i></b>
<p><i>Details/Test:</i></p> <ul style="list-style-type: none"> <li>• Visit the alternate processing site.</li> <li>• Assess its suitability and compatibility with the current computer facility.</li> </ul>

## Business Continuity Planning Audit Program/ICQ

### ***Procedure Step: Training of Participants***

#### ***Details/Test:***

- Interview users and/or IS personnel to determine if they have been trained in their responsibilities in the event of an emergency or disaster.
- Determine if they are aware of manual or alternate processing procedures that are to be used when processing is delayed for an extended period of time. (Note - a key point for successful recovery from major disasters is correct handling of press and publicity).
  - Has training included dealing with TV and newspapers etc. for selected team members, as well as training other team members and employees not to speak directly, but refer queries to the trained team members? This can be crucial in maintaining customer and financial confidence in the business.