IS AUDITING GUIDELINE
BUSINESS CONTINUITY PLAN (BCP) REVIEW FROM IT PERSPECTIVE DOCUMENT G32

The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of the Information Systems Audit and Control Association® (ISACA®) is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IS auditing and reporting. They inform:
  - IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities as set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor® (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.
- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

CobiT® resources should be used as a source of best practice guidance. The CobiT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility as well as to achieve its expectations, management must establish an adequate system of internal control." CobiT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IT processes and consideration of CobiT information criteria.

As defined in the CobiT *Framework,* each of the following is organised by IT management process. CobiT is intended for use by business and IT management, as well as IS auditors; therefore, its usage enables the understanding of business objectives, communication of best practices and recommendations to be made around a commonly understood and well-respected standard reference. CobiT includes:

- Control objectives—High-level and detailed generic statements of minimum good control
- Control practices—Practical rationales and "how to implement" guidance for the control objectives
- Audit guidelines—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met
- Management guidelines—Guidance on how to assess and improve IT process performance, using maturity models, metrics and critical success factors. They provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
  - Performance measurement—How well is the IT function supporting business requirements? Management guidelines can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
  - IT control profiling—What IT processes are important? What are the critical success factors for control?
  - Awareness—What are the risks of not achieving the objectives?
  - Benchmarking—What do others do? How can results be measured and compared? Management guidelines provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

A **glossary** of terms can be found on the ISACA web site at *www.isaca.org/glossary*. The words audit and review are used interchangeably.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his/her own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

The ISACA Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary. The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Any suggestions should be e-mailed (standards@isaca.org), faxed (+1.847. 253.1443) or mailed (address at the end of document) to ISACA International Headquarters, for the attention of the director of research, standards and academic relations. This material was issued on 1 July 2005.

1. BACKGROUND

1.1. Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, “During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.”

1.2. Linkage to CobiT

1.2.1 High-level control objective DS4, *Ensure continuous service*, states, “Control over the IT process of ensuring continuous service that satisfies the business requirement to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption.”

1.3 Reference to CobiT

1.3.1 Selection of the most relevant material in CobiT applicable to the scope of the particular audit is based on the choice of specific CobiT IS processes and consideration of CobiT’s control objectives and associated management practices. In a BCP review from an IT perspective, the most relevant processes in CobiT are classified below as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 Primary:

- PO9—Assess risk
- AI6—Manage changes
- DS1—Define and manage service levels
- DS4—Ensure continuous service
- DS10—Manage problems and incidents
- DS11—Manage data
- DS12—Manage facilities
- DS13—Manage operations

1.3.3 Secondary:

- PO4—Define the IT organisation and relationships
- PO8—Ensure compliance with external requirements
- PO7—Manage human resources
- AI5—Install and accredit systems
- DS2—Manage third-party services
- DS5—Ensure systems security
- DS9—Manage the configuration
- M1—Monitoring the process

1.3.4 The information criteria most relevant to a BCP review are:

- Primary—Effectiveness, efficiency, availability and compliance
- Secondary—Confidentiality, integrity and reliability

1.4 Purpose of the Guideline

1.4.1 In today's interconnected economy, organisations are more vulnerable than ever to the possibility of technical difficulties disrupting business. Any disaster, from floods or fire to viruses and cyberterrorism, can affect the availability, integrity and confidentiality of information that is critical to business.

1.4.2 The primary objective of BCP is to manage the risks for an organisation in the event that all or part of its operations and/or information systems services are rendered unusable and aid the organisation to recover from the effect of such events.

1.4.3 The purpose of this guideline is to describe the recommended practices in performing a business continuity plan (BCP) review from an IT perspective.

1.4.4 The purpose of the guideline is to identify, document, test and evaluate the controls and the associated risks relating to the process of BCP, from an IT perspective, as implemented in an organisation to achieve relevant control objectives, both primary and secondary.

1.4.5 This guideline provides guidance in applying IS Auditing Standard S6 Performance of Audit Work to obtain sufficient, reliable, relevant and useful audit evidence during review of the business continuity plan from an IT perspective. The IS auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

1.5 Guideline Application

1.5.1 This guideline is applied when conducting a review of BCP from an IT perspective in an organisation.

1.5.2 When applying this guideline, the IS auditor should consider its guidance in relation to other relevant ISACA standards and guidelines.

1.6 Terminology

1.6.1 Acronyms:

- Business continuity plan (BCP)
- Business impact analysis (BIA)
- Disaster recovery plan (DRP)

1.6.2 Business continuity planning refers to the process of developing advance arrangements and procedures that enable an organisation to respond to an interruption in such a manner that critical business functions continue with planned levels of interruption or essential change. In simpler terms, BCP is the act of proactively strategising a method to prevent, if possible, and manage the consequences of a disaster, limiting the consequences to the extent that a business can absorb the impact.

1.6.3 The term BCP refers to the complete process of business continuity planning; it includes *inter-alia* business, technological, human and regulatory aspects.

1.6.4 The BCP defines the roles and responsibilities and identifies the critical information technology application programs, operating systems, networks, personnel, facilities, data files, hardware and time frames needed to assure high availability and system reliability based on the business impact analysis. A BCP is a comprehensive statement of consistent actions to be taken before, during and after a disaster. Ideally, BCP enables a business to continue operations in the event of a disruption and survive a disastrous interruption to critical information systems.

1.6.5 BIA involves the identification of critical business functions and workflow, determines the qualitative and quantitative impact of a disruption, and prioritises recovery time objectives (RTOs).

1.6.6 DRP, a key component of BCP, refers to the technological aspect of BCP—the advance planning and preparations necessary to minimise loss and ensure continuity of critical business functions in the event of a disaster. DRP comprises consistent actions to be undertaken prior to, during and subsequent to a disaster. A sound DRP is built from a comprehensive planning process, involving all of the enterprise business processes. Disaster recovery strategies include the use of alternate sites (hot, warm and cold sites), redundant data centres, reciprocal agreements, telecommunication links, disaster insurance, business impact analyses and legal liabilities.

2. AN OVERVIEW OF BCP FROM AN IT PERSPECTIVE

2.1 Components of BCP From IT Perspective

2.1.1 The IT component of BCP defines the response and recovery process that assures the availability of IT operations, reintegration of procedures, applications, operations, systems, data storage, networks and facilities that are critical to supporting the business process.

2.1.2 BCP components include the following:

- Identification—Identify potential threats and risks of the business.
- Prevention—Prevent or minimise the probability of the incident.
- Detection—Identify the circumstances under which the organisation determines entering contingency status.
- Declaration—Specify the conditions on which contingency is declared and identify the person(s) who can declare it.
- Escalation—Specify the conditions on which contingency is escalated and identify the person(s) and order of escalation in the event of contingency.
- Containment—Specify the immediate action required to contain or minimise the effect of the incident on customers, suppliers, service providers, stakeholders, employees, assets, public affairs and the business process.
- Implementation—Specify the complete list of actions to be followed to declare contingency status (such as offsite processing, backup recovery, offsite media and manuals, employee transportation, and distribution and provider contracts).
- Recovery—Recovery is the advance planning and preparations that are necessary to minimise adverse business impact (such as financial loss and image damage) and facilitate faster recovery and ensure continuity of core technology assets that support the critical business functions of an organisation in the event of disaster within an acceptable time frame. The key aspects to be reviewed are:
  - Resumption—Resumption of critical and time-sensitive processes immediately after the interruption and before the declared mean time between failures (MTBF)
  - Revival—Revival of vital and less time-sensitive processes is related to resumption of critical processes
  - Restoration—Repairing and restoring the site to original status and resuming business operations in totality, or putting in place a complete new site

    Relocation—Relocating to alternative site temporarily or permanently depending upon the interruption. Relocation may not be required in all kinds of interruptions.
  - Crisis management—The overall coordination of the organisation's response to a crisis in an effective, timely manner, with the goal of avoiding or minimising damage to the organisation's profitability, reputation or ability to operate

2.2 Elements of BCP

2.2.1 An essential element of BCP is risk assessment, which involves the task of identifying and analysing the potential vulnerabilities and threats, including the source. Risk assessment involves the process of identifying the potential risks to the organisation, assessing the critical functions necessary for the organisation to continue business operations, defining controls in place to reduce exposure and evaluating the cost of such controls. A risk benefit analysis—the outcome of the risk assessment—elaborates the potential threats and the related exposure together with the contingency and mitigation action required, and concludes by describing the benefits arising out of covering the risks.

2.2.2 A risk assessment followed by a BIA must be performed to assess the overall financial exposures and operational effects resulting from a disruption in business activities. The BIA should identify and help to prioritise the critical business processes supported by the IS infrastructure including, but not limited to, a cost-benefit analysis of controls in different disruption scenarios.

2.3 Key Factors of BCP

2.3.1 The BCP must:

- Be understandable and easy to use and maintain.
- Provide management with a comprehensive understanding of adverse effects on business due to normal systems processing disruption, and the total effort required to develop and maintain an effective BCP.
- Obtain executive-management-level commitment to support and participate in the effort.
- Identify critical information resources related to core business processes.

- Identify methods to maintain the confidentiality and integrity of data.
- Assess each business process to determine its criticality. Indications of criticality include:
  - The process supports lives or people's health and safety.
  - The process is required to meet legal or statutory requirements.
  - Disruption of the process would affect revenue.
  - There is a potential impact to business reputation, including that of the customers.
- Focus the plan's attention on:
  - Disaster management
  - Minimising the effect of disaster, in the eventuality that the disaster is not manageable
  - Orderly recovery
  - Continuity of operations and key services
- Validate RTOs and recovery point objectives (RPOs) for various systems and their conformance to business objectives.
- Identify the conditions that activate the contingency plan.
- Identify which resources will be available in a contingency stage and the order in which they will be recovered.
- Identify the enablers (people and resources) required for recovery.
- Select project teams in accordance with technological and business environments to provide reasonable representation of core and critical functional areas to develop the plan.
- Identify the methods of communication between enablers, support staff and employees.
- Identify geographical conditions related to the recovery of operations.
- Define recovery requirements from the perspective of business functions.
- Define how the BCP considerations must be integrated into ongoing business planning and system development processes for the plan to remain viable over time.
- Implement a process for periodic review of the BCP's continuing suitability as well as timely updating of the document, specifically when there are changes in technology and processes, legal or business requirements. The BCP strategies may also be modified based upon results of risk assessments and vulnerability assessments.
- Develop a comprehensive BCP test approach that includes management, operational and technical testing.
- Implement a process of change management and appropriate version controls to facilitate maintainability.
- Identify mechanisms and decision makers for changing recovery priorities resulting from additional or reduced resources as compared to the the original plan.
- Document formal training approaches.

3. INDEPENDENCE

3.1 Professional Independence

3.1.1 Where the IS auditor has been involved previously in the design, development, implementation or maintenance of any process related to the BCP in an organisation and is assigned to an audit engagement, the independence of the IS auditor may be impaired. In the event of any possible conflict of interest, the same should be explicitly communicated to the organisation and the organisation's concurrence should be obtained in writing before accepting the assignment. The IS auditor should refer to appropriate guidelines to deal with such circumstances.

4. COMPETENCE

4.1 Skills and Knowledge

4.1.1 The IS auditor should provide reasonable assurance that the auditor has the required knowledge and skill to carry out the review of the BCP and its components.

4.1.2 The IS auditor should be competent to determine whether the BCP is in line with the organisation's needs.

4.1.3 The IS auditor should have adequate knowledge to review the aspects related to the BCP. Where expert inputs are necessary, appropriate inputs should be obtained from external professional resources. The fact that external expert resources would be used should be communicated to the organisation in writing.

4.1.4 A BCP review is essentially enterprise-specific, and for the review to be effective, the IS auditor must, at the outset, gain an overall understanding of the business environment, including an understanding of the organisation's mission, statutory or regulatory requirements peculiar to the organisation, business objectives, relevant business processes, information requirements for those processes, the strategic value of IS and the extent to which it is aligned with the overall strategy of the enterprise/organisation.

4.1.5 The IS auditor should undertake the development of a BCP or policies, testing and recovery plans, only if the IS auditor has the necessary knowledge, competence, skills and resources. The IS auditor should refer to appropriate guidelines to deal with such circumstances.

5. PLANNING

5.1 Scope and Objectives of the Review

5.1.1 The IS auditor should, in consultation with the organisation and where appropriate, clearly define the scope and objective of the BCP review. The aspects to be covered by the review should be explicitly stated as part of the scope.

5.1.2 For the purpose of the review, the stakeholders in the solution and recipients of the report should also be identified and agreed upon with the organisation.

5.2 Approach

5.2.1 The IS auditor should formulate the audit approach in such a way that the scope and objectives of the review could be fulfilled in an objective and professional manner.

5.2.2 The audit approach depends upon the phase of the BCP in the organisation.

5.2.3 The approach should consider that the BCP review is a team effort that includes active and stable members as well as discussions with user groups.

5.2.4 The approach should be appropriately documented and identify the requirements of external expert inputs, if appropriate.

5.2.5 Critical areas, such as prioritisation of business processes and technologies and results of a risk assessment, should provide reasonable assurance that the plan is effectively implemented as required.

5.2.6 Depending on the organisational practices, the IS auditor may obtain the concurrence of the organisation for the BCP audit plan and approach.

6. PERFORMANCE OF BCP REVIEW FROM IT PERSPECTIVE

6.1 Execution

6.1.1 The aspects to be reviewed and the review process should be decided, taking into account the intended scope and objective of the review as well as the approach defined as part of the planning process.

6.1.2 In general, the study of available documentation (such as BCP, DRP, BIA, business risk analysis and enterprise risk management framework) should be used appropriately in gathering, analysing and interpreting the data. While all of this information may not be readily available, there must be at a minimum a basic risk assessment analysis that defines critical business processes together with IT-based risks.

6.1.3 Main areas of risk of a BCP should include previously detected BCP weaknesses and changes introduced to the systems environment (such as applications, equipment, communications, process and people) since the last BCP test.

6.1.4 To identify any problems relating to the BCP that have been noted previously and may require follow-up, the IS auditor should review the following documents:

- Incidence reports
- Previous examination reports
- Follow-up activities
- Audit work papers from previous examinations
- Internal and external audit reports
- Internal test reports and remedial action plan
- Published Industry information and references

6.1.5 To identify changes to the systems environment, the IS auditor should interview the organisation's personnel and service providers, as well as analyse spending records and reports, inspect IT premises, review hardware and software inventories, and use specialised software to analyse appropriate data.

6.1.6 The IS auditor should consider in the review each of the following phases of testing:

- Pretest—A set of actions required to set the stage for the actual test
- Test—The real action of BCP test
- Posttest—The cleanup of group activities
- Postinvocation review—The review of actions following the real invocation of the plan

6.1.7 The test plan objectives should be reviewed to verify whether the test plan accomplishes the following:

- Verifies the completeness and precision of the BCP
- Evaluates the performance of the personnel involved in the BCP
- Appraises the training and awareness of the teams
- Evaluates coordination between BCP teams, DRP teams, external vendors and service providers
- Measures the ability and capacity of the backup site to meet the organisation's requirements
- Assesses retrieval capability of vital records
- Evaluates the state and quantity of equipment and supplies that have been relocated to the recovery site
- Measures the overall performance of the operational and processing activity of the organisation

6.1.8 BCP testing should be designed carefully to avoid disruption to the business processes. Appropriate areas of BCP testing should be identified as part of the annual review of risk, and duplication of efforts should be avoided. In reviewing the plan of a BCP test, the IS auditor should verify:

- Scope and objectives of the test plan
- Frequency, methodology and revisions to test plan
- Type, appropriateness and sufficiency of tests
- Applications
- Volume of data
- Business areas
- Network rerouting
- System vulnerability, penetration and incidence response
- Change, configuration and patch management
- Audit evidence criteria and requirements
- The test environment is representative of the operational environment and exceptions are documented
- Test effectiveness and its relation to risk assessment and business impact conclusions

6.1.9 In reviewing a postevent scenario, the IS auditor should verify:

- The cause and nature of disruption
- The extent of damage to personnel, infrastructure and equipment
- The severity of impact
- Mitigation exercises underway
- Services affected
- Records damaged
- Salvageable items

- Items that can be repaired, restored and/or replaced
- Insurance claims
- Processes affected
- Time to restore the IT process
- Action plan, restoration teams, roles and responsibilities

6.1.10 The inferences and recommendations should be based on an objective analysis and interpretation of the data.

6.1.11 Appropriate audit trails should be maintained for the data gathered, analysis made, inferences arrived at and corrective actions recommended.

6.1.12 The observations and recommendations should be validated with the organisation, as appropriate, before finalising the report.

6.2 Aspects to Review

6.2.1 Typically, the BCP should address the following key issues:

- Why should it be done?
- How should it be done?
- Who needs to do it?
- What needs to be done?
- When should it be done?
- Where should it be done?
- Under what policies, rules and standards should it be done?
- Who can change the plan and under what circumstances?
- Under what conditions is a disaster declared 'over'?

6.2.2 Organisational aspects should be reviewed to consider that:

- The BCP is consistent with the organisational overall mission, strategic goals and operating plans
- The BCP is routinely updated and considered current
- The BCP is periodically tested, reviewed and verified for continuing suitability
- Budget allocation is available for the BCP testing, implementation and maintenance
- Risk analyses are performed routinely
- A formal procedure is in place to regularly update the IT and telecom inventory
- Management and personnel of the organisation have the required skills to apply the BCP and an appropriate training programme is in place
- Measures to maintain an appropriate control environment (such as segregation of duties and control access to data and media) are in place in case of a contingency
- Enablers are identified and the individuals' roles and responsibilities are adequately defined, published and communicated. Typically, core teams such as the emergency action team, damage assessment team and emergency management team are constituted. The core teams will be supported by the offsite storage team, software team, application team and security team. There is an emergency operation team, network recovery team, communication team, transportation team, user hardware team, data preparation and record team, administrative support team, supplies team, salvage team, and relocation team.
- Communication channels are fully documented and publicised within the organisation
- The interface and its impact between departments/divisions within the organisation is understood
- Roles and responsibilities of external service providers are identified, documented and communicated
- Coordination procedures with external service providers and customers are documented and communicated.
- BCP teams have been identified for various BCP tasks, clearly establishing roles and responsibilities and management reporting that defines accountability
- Compliance with statutory and regulatory requirements is maintained

6.2.3 Planning aspects should be reviewed to consider that:

- A methodology to determine activities that constitute each process is in place as part of a key business process analysis
- The planned IS technology architecture for the BCP is feasible and will result in safe and sound operations if a business interruption impacts key IT processes
- A risk assessment and BIA were performed before the BCP implementation
- BIA includes changes in the risks and corresponding effect on the BCP
- The BIA identifies the key recovery time frames of the critical business processes
- There is a periodic review of risks
- There are appropriate incident response plans in place to manage, contain and minimise problems arising from unexpected events, including internal or external events
- An appropriate schedule is in place for BCP testing and maintenance
- An onsite test, simulation, triggering of events and their potential impacts should be performed
- A BCP life cycle exists and whether it is followed during development, maintenance and upgrade
- The BCP is reviewed at periodic intervals to confirm its continuing suitability to the organisation

6.2.4 Procedural aspects should be reviewed to consider that:

- Top management is a serious driving force in implementation of the BCP
- Top priority is provided for safety of employees, personnel and critical resources
- Resources and their recovery have been prioritised and communicated to the recovery teams
- Awareness is created across the entire organisation on the effect to the business in the event of a disaster
- Adequate emergency response procedures are in place and tested
- The people involved in the disaster assessment/recovery process are clearly identified and roles and responsibilities are delineated throughout the organisation
- Appropriate levels of training are conducted including mock test drills
- Evacuation plans are in place and are periodically tested
- Backup human resources are identified and available

- Cell, telephone or other such communication call trees are reviewed, tested and routinely updated
- Alternative communications strategies are identified
- Backup and recovery procedures are part of the BCP
- Backups are retrievable
- An appropriate backup rotation practice is in place
- Offsite locations (hot, warm or cold sites) are tested for availability and reliability
- Appropriate offsite records are maintained
- Confidentiality and integrity of data and information are maintained
- Media liaison strategies are in place, where appropriate
- The BCP is periodically tested and test results documented
- Corrective actions are initiated based upon test results
- There is adequate insurance protection

6.3 Outsourcing of IS

6.3.1 Any adverse effect or disruption to the business of the service provider has a direct bearing on the organisation and its customers. Where the organisation has partially or fully delegated some or all of its IS activities to an external provider of such services (the service provider), which have an effect on the process of BCP, the IS auditor should review whether the service provider's BCP process conforms with the organisation's BCP and documented contracts, agreements and regulations remain with the service user.

6.3.2 The review should also verify that the agreement with the outsourced service provider includes a description of the means, methods, processes and structure accompanying the offer of information systems services and products as well as the control of quality.

6.3.3. The IS auditor should obtain an understanding of the nature, timing and extent of the outsourced services. The IS auditor should establish what controls the service user has put in place to address the business requirement of the organisation's business continuity *vis-à-vis* BCP of the service provider. The IS auditor should consider all the audit requirements stated above in reviewing an outsourced activity, in addition to :

- Whether the agreement provides open and unimpeded rights to audit the service provider, as considered necessary by the organisation
- Whether the agreement provides adequate protection for the organisation in case of disruption to the business of the service provider
- Whether the agreement provides continuity of services in the event of a disaster
- Integrity, confidentiality and availability of the organisation's data with the service provider
- Organisation personnel disgruntled over outsourcing arrangement/lack of loyalty due to outsourcing
- Access control/security administration at the service provider premises
- Violation reporting and follow-up by the service provider
- Network controls, change controls and testing at the service provider premises

7. REPORTING

7.1 Report Content

7.1.1 The IS auditor should produce reports on the processes, facilities and technologies involved in the BCP, the risks assumed and how those risks are managed in case of a contingency. Monitoring performance of the review is a key success factor. The report, produced as a result of the BCP review, should include aspects such as:

- The scope, objective, period of coverage, methodology followed and assumptions
- Overall assessment of the solution in terms of key strengths and weaknesses as well as the likely effects of the weaknesses
- Recommendations to overcome the significant weaknesses and to improve the solution
- The extent of compliance with CobiT's control objectives, associated management control practices and CobiT information criteria as relevant, along with the effect of any noncompliance
- Reasonable assurance on BCP process and relevant internal controls to ensure that IT systems can be recovered within an acceptable time frame in event of a disruption. The report should state the conclusions, recommendations and any reservations or qualifications.
- Recommendations regarding how the experience could be used to improve similar future solutions or initiatives
- Depending on the scope of the assignment, other topics

7.1.2 The report should be submitted to the the appropriate level of management and the audit committee if one is established.

7.2 Weaknesses

7.2.1 Weaknesses identified in the BCP review, either due to lack of controls, poor implementation or nonmitigation of associated risks to agreeable levels, should be brought to the attention of the business process owner and to IS management responsible for the implementation of the BCP process. Where weaknesses identified during the BCP review are considered to be significant or material, the appropriate level of executive management should be advised to undertake immediate corrective action.

7.2.2 Since effective BCP controls are dependent on the business continuity planning process and related controls, weaknesses in the related controls should also be reported.

7.2.3 The IS auditor should include appropriate recommendations in the report to strengthen controls to mitigate the associated risks.

8. FOLLOW-UP ACTIVITIES

8.1 Timeliness

8.1.1 The effects of any weaknesses in the BCP are ordinarily wide-ranging and high-risk. Therefore, the IS auditor should, where appropriate, carry out sufficient, timely follow-up work to verify that management action to address weaknesses is taken promptly.

8.2 Effectiveness

8.2.1 To provide reasonable assurance of the effectiveness of the review, the IS auditor should conduct a follow-up review to oversee that the recommendations have been carried out and verify the effectiveness of corrective measures implemented.

9. EFFECTIVE DATE

9.1 This guideline is effective for all information systems audits on 1 September 2005. A full glossary of terms can be found on the ISACA web site at *www.isaca.org/glossary*.

Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *standards@isaca.org*
Web site: *www.isaca.org*