



Good Practice Note No. 11

Business Continuity Management

Part of a series of notes to help Centers and their internal auditors review their own Center's internal management processes from the point of view of managing risks and promoting value for money, and to identify where improvement efforts could be focused.

SUMMARY

The purpose of this note is to provide a set of benchmarks to Centers for managing business continuity. The note draws on the results of a limited survey of external good practice (national and international standards and guidance material from various CGIAR member countries) conducted by the CGIAR Internal Auditing Unit, as well as the results of recent work and discussions with CGIAR Center and System Office staff.

A subset of a Center's overall risk management system is management to ensure resilience of operations in the event of a disaster affecting the people, infrastructure, genetic resource collections, knowledge, and information and communication systems of a Center.

Regardless of Centers can implement preventive controls to avoid the occurrence of disasters, they should implement impact minimization measures or "recovery" controls in case disaster-related risks eventuate. These include

- Insurance arrangements – to minimize the financial costs of losses from disasters
- Geographic distribution of research activities, often through partnerships with national agricultural research systems and other research organizations, so that they are not excessively concentrated in one particular geographic zone
- Planning of business operations, including alternative worksites and human resource management, in the event of relocation and suspension of operations
- Identification and backup of vital physical records and germplasm collections
- Identification and backup of electronically stored data and operating and application systems, and restoration of use of alternative communication networks



Together, these recovery measures comprise business continuity management. This note identifies the following good practices in this regard.

BUSINESS CONTINUITY PLANNING

- Establish a focal point with clear responsibilities for business continuity planning
- Identify and prioritize critical business processes for which business continuity measures should be formulated
- Document in a business continuity plan the Center's disaster recovery measures, policies, processes, and responsibilities
- Include in the business continuity plan how damage will be assessed
- Clearly document authority levels and circumstances for activation/implementation in the business continuity plan
- Periodically test, review, and update as necessary business continuity plans
- Cost the business continuity plan as a basis for securing the financial resources to implement the plan
- Consider automating the preparation and maintenance of business continuity plans

INSURANCE

- Establish responsibility within the Center to periodically review insurance strategies and, where external insurance is approved, ensure that coverage is adequate and up to date
- Ensure ready access to up-to-date insurance policy documents and insurer contact information in the event of emergencies

BACKUP OF PHYSICAL RECORDS AND GENE BANK COLLECTIONS

- Identify, as part of a "vital record" program, physical records that have enduring value to the continued operations of the Center and that should be copied in backup form in the event of the original being lost
- Arrange backup (safety) collections of genebank accessions to be maintained in suitable storage conditions



INFORMATION TECHNOLOGY AND COMMUNICATION DISASTER RECOVERY PLAN

- Identify, as part of a “vital record” program, those electronically maintained databases and business records that have enduring value to continued operations of the Center and that should be backed up in the event of primary copies being lost
- As part of an overall business continuity plan, include ICT disaster recovery plans (DRP) for restoring operating and application software and data, prioritized by the critical nature of the business processes being supported

Include, as part of an ICT DRP, a backup strategy at all locations for critical operating system and application software and data

Acknowledgements

This note has been prepared solely for use by CGIAR Centers and their internal auditors. The note draws on a number of internationally accepted standards and good practices which include business continuity or disaster recovery management, including

-the Control Objectives for Information and related Technology (COBIT) Framework, published by the Information Systems Audit and Control Foundation (for more information, visit www.isaca.org);

-the Business Continuity Management Good Practice Guide published by the Business Continuity Institute, a UK-based international professional body. This is available without charge from www.thebci.org; and

-ISO /IEC standard 17799:2001 “Information Security” and ISO standard 15489-1-2001 “Information and Documentation – Records Management – Part 1” (for more information, visit www.iso.org).

We thank CGIAR Center staff, the CGIAR CIO, and Mr. Gerry Reardon, IT audit consultant, who provided input and advice on the preparation of this note.



Good Practice Note No. 11

Business Continuity Management

INTRODUCTION

Enterprises should have a managed process in place for developing and maintaining business continuity throughout their organization. This can be seen as a subset of an enterprise's overall risk management system.

This Good Practice Note seeks to answer three critical questions about business continuity management:

1. What does business continuity management cover?
2. Why is it important?
3. What good practices should Centers consider when implementing or strengthening a business continuity management process?

CGIAR Centers are subject to various risks to the continuity of their operations. Examples of events that could have a major impact on the Center operations include

- Physical disaster. Some Center headquarters or significant outposts are located in earthquake zones or areas subject to periodic severe weather.
- Civil disorder and political instability. In late 2002 WARDA had to evacuate its headquarters campus in Côte d'Ivoire due to civil war. Heightened terrorist activity in host countries could also affect operations in future.
- Deterioration in host country relations. Though this has not occurred so far, changes in the relationship between a Center and its host country may lead to a need to move operations. Though not likely to be sudden, actions such as stripping a Center of its privileges and immunities or placing significant limits on its scope of operations in the host country could trigger such a situation.
- Direct attacks on Center staff or infrastructure. In the past, Centers have experienced peaceful demonstrations and have not been subject to major internal sabotage of infrastructure. However, one cannot discount the possibility of future violent attacks, which may disrupt operations.
- Direct attacks on Center information technology and communications (ICT) systems. There is a heavy dependency of Centers on ICT to conduct day-to-day operations, all the more so as Centers become more decentralized and partnership activities become more widespread and complex. This,



together with the increasing level and sophistication of global cybercrime, has led to a growing risk of Center paralysis due to loss of ICT resources.

- Loss of key staff. Though not pleasant to contemplate, the sudden incapacity or worse of one or more key staff, through attacks or accident, remains another potential source of disruption to a Center's operations. An accident involving group travel or the loss of a staff member who holds unshared but critical knowledge are two scenarios in this category.

Though likely to have lesser impact than the examples above, equipment failure, laboratory emergencies and accidental fire, electromagnetic and other damage to Center infrastructure, including that supporting ICT systems, could also disrupt operations.

For some disaster-related risks, Centers will have or should be putting in place "preventive" controls to minimize the likelihood of risk. These include physical security controls, occupational health and safety controls, fire safety controls, and ICT network security controls. One could also include in this category the relationship management with the host country government and neighboring communities.

For some externally generated risks, there may be little in the way of preventive action that the Center can take if it wishes to continue operations in its current locations or according to its current modalities.

In either case, Centers also need to have impact minimization measures or "recovery" controls in case disaster-related risks eventuate. These include

- Insurance arrangement to minimize the financial costs of losses from disaster events;
- Geographic distribution of research activities, often through partnerships with national agricultural research systems and other research organizations, so that they are not excessively concentrated in one particular geographic zone;
- Planning of business operations, including alternative worksites and human resource management, in the event of relocation and suspension of operations;
- Identification and backup of vital physical records and germplasm collections;
- Identification and backup of electronically stored data and operating and application systems, and restoration of use of alternative communication networks.

Together, these recovery measures comprise business continuity management.

For a CGIAR Center, active business continuity management helps ensure resilience of operations despite the eventuality of a disaster affecting the people, infrastructure, genetic resource collections, knowledge assets, and ICT systems.

This Good Practice Note will focus on these recovery measures:



Box 1. CGIAR Data Resilience Project

The approved CGIAR ICT-KM Program includes a data resilience project, which has received World Bank funding to implement. The project document notes that the CGIAR is vulnerable to severe loss of its public good information assets due to natural disasters, civil unrest, and other calamities, and that, in many cases, Centers have not fully taken appropriate and adequate steps to protect this global public good from loss. The document notes that even when data are properly backed up off-site, there are often inadequate planning and procedures in place to ensure that Centers can be up and running, with access to its key information stores, in reasonable time frames. The Data Resilience Project seeks to address these problems directly by

- developing methodologies and best practices to ensure an adequate level of resilience;
- holding regional workshops to train key participants in the why and how of disaster preparedness;
- publishing guidelines, best practices, forms and checklists, and lessons learned from the implementations, for the benefit of all CGIAR Centers and their partners; and
- implementing certain measures of information technology business continuity in at least six CGIAR Centers.

Data resilience is a subset of business continuity planning. The CGIAR Data Resilience Project is expected to be launched in late 2004 and this Good Practice Note (current version) has been timed to provide information input into the project. Later versions of this Note will draw on outputs from the project.

BUSINESS CONTINUITY PLANNING

Due to the heavy dependence of organizations on ICT and its susceptibility to disruption from various sources, business continuity planning methodology and standards have tended to come from ICT-related sources. Nonetheless, these standards and good practice documents recognize that business continuity management practices should not be restricted to ICT-related areas and activities and that their implementation should not be driven by ICT.

Box 2. Business continuity management as a strategic function

The Business Continuity Institute (BCI), a UK-based international professional body devoted¹ to promoting high standards of professional competence and commercial ethics in the provision of business continuity planning and services, notes that “today good business continuity management (BCM) fully recognizes that an organization’s resilience depends equally on its management and operational staff as well as technology and requires a holistic approach to be taken when establishing a BCM capability.” BCI has developed a new definition of BCM to reflect this:

“Business continuity management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.”



Good practice

Establish a focal point with clear responsibilities for business continuity planning

A common practice is for organizations to establish disaster recovery or business continuity committees at a very high level, which are responsible for the development of the business continuity plans, their implementation, and their invocation at the time of an emergency. At the same time, the business continuity responsibilities of other staff, including ICT staff, should be defined.

Good practice

Identify and prioritize critical business processes for which business continuity measures should be formulated

A business impact analysis (BIA) is the foundation of an effective business continuity plan. It must originate from the individual business/research areas and start with the identification of the significant inherent risks and critical threats to achieving business/research goals. This analysis should be undertaken systematically, as a sub-set of Center's broader risk management framework. The more a business continuity plan is defined in relation to the Center's critical business requirements, the easier it will be to explain to senior management and to secure adequate funding for its implementation.

Box 3. Process approach to business continuity planning

Focusing on continuity of prioritized business process and developing specific business process recovery plans consolidates a number of traditional continuity planning disciplines:

- Business operations resumption planning
- Crisis management planning
- Continuous availability planning
- IT disaster recovery planning

The scope of a BIA and the steps involved are described in detail in the BCI's "Good Practice Guide on Business Continuity Management". A BIA identifies

- those critical manual and automated business processes and assets with the greatest impact on the business in the event of a disaster
- the resources involved (e.g. people, technology, equipment/facilities, suppliers, materials)
- their dependencies and single points of failure (process risk analysis)



- business impacts (financial and non-financial) of failures
- the critical time frames in which processes should be restored, upon which tradeoffs between recovery and cost of recovery can be based. This is linked to the “risk appetite” of the organization for business process interruption. Processes should be narrowly defined for example, “financial processes” should be broken down into more detailed processes such as general ledger, cash management, and fixed asset management as recovery priorities will differ between them

In addition, the BIA assists in identifying alternative manual procedures, which may be used during service interruptions.

Good practice

Document in a business continuity plan the Center’s disaster recovery measures, policies, procedures, and responsibilities

Successful business continuity plans must be complete, current, and well documented. Specifically, the plan should describe the role of senior management; the business continuity committee, the recovery teams' responsibilities; plan testing; recovery alternatives; conditions and authorizations needed for activation of the plan, critical operational procedures; and other emergency information that persons may not remember in the middle of a disaster. The aim is to minimize the need for critical decision-making in a crisis situation and instead ensure that personal safety is addressed rapidly, and that critical operations are commenced in the shortest possible time. As with any business program, a business continuity plan must be operationally feasible.

A business continuity plan should provide for the “worst case” scenario of total destruction of a Center’s operating environment, though it more likely will be useful for lesser interruptions. Business continuity plans will typically assume that a sufficient number of Center staff is not incapacitated to implement and affect recovery.



Box 4. Laboratory emergency planning

Laboratory emergency planning is closely linked with laboratory occupational health and safety systems, a subject that is planned to be covered in a separate Good Practice Note. Laboratory emergency response plans will be a subset of general Center emergency response plans. However some laboratory-specific aspects include

- laboratory evacuation procedures, points of assembly away from the possible effects of hazards such as smoke or chemical fumes, and drills
- procedures for chemical spill and toxic fume clean up and injury response
- use of appropriate fire extinguishers, including those for solvent fires as well as electrical and solid fuel fires
- handling of radioactive material releases (where isotopes are used in laboratory research)

A modular format may be useful for a Center-wide business continuity plan, with components for the different critical business functions and locations (headquarters, outposts). A consistent philosophy and framework relating to development of the plan should be applied across the modules.

Good practice

Include in the business continuity plan how damage will be assessed

The business continuity plan should explain, in the event of failures, how the evaluation of damage and impact on operations will be performed. The procedures should allow that, for each failure, a competent person is responsible for assessing the damage caused and what extra damage could be caused.

Good practice

Clearly document authority levels and circumstances for activation/implementation in the business continuity plan

Depending on the severity of the failure, the resulting impact and the resulting action requirements, a Center may designate an individual, a business continuity committee, or certain levels of site management or corporate management to take decisions regarding the activation and implementation of the business continuity plan.

The principle of escalation should be documented in business continuity plans. The plans should be very clear as to who should be informed and in what circumstances. Certain decisions will only be taken at the highest levels of management.



Good practice

Periodically test, review, and update as necessary business continuity plans

ISO/IEC 17799:2001 notes that business continuity plans may fail because of incorrect assumptions, oversight or changes in equipment or personnel. They should therefore be tested regularly to ensure that they are up to date and effective. Such tests should also ensure that relevant staffs are aware of the plans. Center staff are generally committed and will perform beyond their normal expectancies in times of crisis, but if the plan has not been tested, there is a better than average chance that some of the procedures will not work. It is better for the plan's shortcomings to be revealed during a test than in a full-blown crisis.

The ISO/IEC standard notes that there are a variety of techniques for testing to ensure the plans will operate in real life as intended:

- table-top testing of various scenarios (discussing the business recovery arrangements using sample interruptions)
- simulations (training people in their roles)
- technical recovery testing (ensuring information systems can be restored effectively)
- testing recovery at an alternative site (running business processes in parallel)
- tests of supplier facilities and services (ensuring externally provided services or products will meet contract commitment)
- complete rehearsals

It may be more practical to test components of the plan progressively rather than everything at once.

It is important that a full debrief take place after each test and the plan modified where required.

Responsibility should be assigned for regular reviews of the plan. The ISO/IEC standard notes that changes in a number of areas would necessitate a plan update:

- personnel
- addresses or telephone numbers
- business strategy
- location, facilities, resources
- legislation
- contractors, suppliers, key customers
- processes (new, withdrawn)



- risks

Good practice

Cost the business continuity plan as a basis for securing the financial resources to implement the plan

Recoverability comes with a price tag, a rather large one, depending on whether all disaster scenarios are to be anticipated and how quickly resumption of key supporting ICT activities is required.

Recoverability costs, even under moderate scenarios, could still be relatively high given the overall unrestricted resources available for a Center. There are opportunities for recoverability cost sharing across Centers, which will be further identified and exploited as part of the CGIAR Data Resilience Project (discussed further below).

Box 5. ICT-related cost elements of a business continuity plan

- Costs of alternative or redundant hardware, software, and communications links
- Costs of service contracts related to disaster recovery e.g., offsite backup storage, offsite alternative facilities
- Costs of staff time related to disaster recovery plans (DRP) and maintenance
- Costs of related staff training
- Costs of DRP testing

Good practice

Consider automating the preparation and maintenance of business continuity plans

INSURANCE

Insurance is a form of risk sharing or transfer which reduces an organization's exposure to financial liability as a result of accidental losses or other events causing potential or actual liabilities. Financial liability may arise in relation to such things as

- costs arising from injuries or death of staff, contractors, and visitors while undertaking duties for the organization, being on the premises of the organization, or during travel on behalf of the organization or in an organization's vehicle



- costs of employing temporary or replacement staff in the event of incapacity of existing staff
- costs of replacing physical assets destroyed or damaged
- costs of compensating third parties for liabilities
- costs from loss of cash (including cash in transit) or property due to theft or internal fraud
- Costs associated with staff or their family members' illness. In some locations, insurance for nationally recruited staff may take the form of subscriptions to the host country's universal health or social security insurance programs.

Insurance is obtained to minimize the financial impact on business continuity in the event of certain defined disasters occurring.

In some cases, as a condition of insurance or to reduce the cost of insurance, the Center may be required by the insurer to implement certain preventive measures and have these subject to audit by the insurer or an independent inspection service.

Good practice

Establish responsibility within the Center to periodically review insurance strategies, and where external insurance is approved, ensure that coverage is adequate and up to date

Not all risks will be readily insurable or cost-effective to insure against (in some cases, self-insurance will be the appropriate option). Some risks, such as third-party injury insurance in relation to the operation of vehicles, may be compulsory to obtain according to local laws. Centers should systematically review, on a periodic basis, their insurance strategies, taking into consideration

- changes in the insurable risks
- cost-benefits of external insurance versus self-insurance
- potential for savings through shared insurance with other CGIAR Centers
- changes in local laws
- loss experience

One person within the Center should be designated as responsible for managing insurance.

The review should take into account all locations where the Center operates. While insurance options for risks at headquarters may be well researched, they may not always be so well assessed for outpost locations. The officers in charge or administrative managers in outpost locations may be tasked with



researching insurance options, but this should be monitored by the designated “insurance manager” in headquarters.

Good practice

Ensure ready access to up-to-date insurance policy documents and insurer contact information in the event of emergencies

This should be the responsibility of the “insurance manager” within the Center and, in the case of outpost locations, the officer in charge or administrative manager. Copies of insurance policies and contact details for outpost locations should be available in headquarters, and copies of insurance policies and contact details for headquarters should be kept in a designated outpost location.

BACKUP OF PHYSICAL RECORDS AND GENE BANK COLLECTIONS

Physical records and germplasm collections are the two most significant physical assets held by Centers that can be considered irreplaceable after loss if not properly “backed up” in some form.

Good practice

Identify, as part of a “vital records” program, those physical records which have enduring value to continued operations of the Center, and which should be copied in the event of the original being lost

ISO 15489-1-2001 “Information and Documentation – Records Management – Part 1” promotes the standardization of record management policies and procedures to ensure that appropriate attention is given to all records and that the evidence and information they contain can be retrieved efficiently and effectively, using standard practices and procedures. Records management in general will be the subject of a future separate Good Practice Note. However, there are some aspects of this ISO standard which are relevant to business continuity:

- there should be a process whereby records of enduring value to the organization are identified and protected for appropriate retention periods (including permanent retention);
- metadata should be developed for records, whatever the format in which the record is kept, to facilitate retrieval;
- records should be subject to appropriate handling and storage to facilitate their retrieval.

In the case of important physical documents, such as signed contracts, signed agreements, property titles, and registration papers, it would also be desirable to have these backed up as physical or electronic copies to enable retrieval of the information or evidence in case the original is lost.



Good practice

Arrange backup (safety) collections of genebank accessions to be maintained in suitable storage conditions

The international genebank collections held in trust for humanity represent a unique and important physical asset of many of the CGIAR Centers. Their loss would be significantly damaging to the work of the Center and (depending on the cause of loss) could represent noncompliance with its agreements with the FAO and fatally damage its reputation as a careful and reliable custodian.

Centers should implement safety backup collections to be maintained in suitable “black box” storage conditions in other locations, preferably in other countries. The relative ease of this depends on the form in which germplasm must be stored. For example, it is relatively easier to arrange safety collections for seed, than for in vitro or cryopreserved germplasm. The latter present more challenges in terms of storage media, requirements for regeneration, and presentation for quarantine purposes, and their storage is more expensive.

A number of Centers have exchanged safety collections of their genebanks with other Centers, and some Centers use the facility provided by the United States National Center for Genetic Resources Preservation in Fort Collins, Colorado, to store “black box” safety collections. The first phase of a Global Public Goods Rehabilitation Project, which has recently been funded by the World Bank, includes financial assistance to Centers to develop or improve safety collections. A campaign is now under way for the establishment of an endowment fund to provide long-term financial support for the maintenance of international crop genebank collections, including safety collections.

INFORMATION TECHNOLOGY AND COMMUNICATIONS DISASTER RECOVERY

Given the critical dependency of organizations on electronic records and computer systems, including databases, local area networks, internet, intranet, and email and the potential losses which could be incurred in the event of data loss or ICT systems being disabled for extended periods due to disaster, it is not surprising that a major aspect of business continuity management relates to ICT disaster recovery. Ensuring continuous ICT service for critical business processes is one of the high-level controls for delivery and support under the COBIT Framework.

Good practice

Identify, as part of a “vital records” program, those electronically maintained databases and business records which have enduring value to continued operations of the Center and which should be backed up in the event of primary copies being lost



The business continuity aspects of ISO 15489-1-2001 referred to above in relation to physical records also apply to electronic data. Centers should inventory all key databases and other electronic records, and identify appropriate backup strategies for them.

Good practice

As part of an overall business continuity planning process, include ICT disaster recovery plans for restoring operating and application software and data, prioritized by criticality of the business processes being supported

The COBIT Framework includes, as a key control, the preparation of a written disaster recovery plan (DRP).

According to COBIT, an ICT DRP should consider:

- criticality classification for critical business processes, databases, and electronic records, identify the supporting systems and applications currently in use, analyze the business impact of the computer operations, and determine the critical recovery time frames
- alternative processing procedures pending resumption of systems
- backup and recovery
- systematic and regular testing and training
- monitoring and escalation processes
- internal and external organizational responsibilities this should include responsibilities for maintenance of the plan
- business continuity activation, fallback, and resumption plans
- risk management activities
- assessment of single points of failure
- problem management



Box 5. Recommended elements of a comprehensive ICT system DRP

- emergency procedures;
- roles and responsibilities of various parties responsible for IT;
- listing of systems resources requiring alternatives (hardware, peripherals, software);
- listing of highest to lowest priority applications, required recovery times, and expected performance norms;
- escalation procedures based on the nature of the interruption and estimated recovery times. These will determine whether recovery will be initiated using alternative computers at the same location but independent of local area network (LAN) functioning, same location but using restored LANs, or using alternative sites;
- backup administrative functions for communicating and providing support services;
- various disaster scenarios and response to each in sufficient detail for step-by-step execution
- specific equipment and supply needs and sources;
- training and awareness;
- testing schedule and results;
- information on formal contract arrangements with vendors to provide services in event of disaster, including backup site facility or relationship, and response expectations, in advance of actual need;
- logistical information on location of key resources, including backup sites;
- key personnel contacts;
- reconstruction plans for recovery business resumption, alternatives for establishing alternative work locations once information systems resources are available.

Good practice

Include, as part of an ICT DRP, a backup strategy at all locations for critical operating system and application software and data

A backup strategy should be developed for software and for data stored in various modes centralized file servers under ICT unit control, decentralized file servers managed by user departments, desktop workstations, laptops, and PDAs. This should cover

- master and data files and operating and application software (and related documentation) to be backed up;
- number of file generations to be retained and rotation procedures;



- frequency of backup;
- on-site and off-site backup media storage locations, and related security. Generally backup strategies should include provision for storage outside the potential destruction zones;
- off site storage of backup logs to permit ready identification of the media to be used to restore files;
- periodic testing of the backup media, and limits on the number of times a tape or similar media is used for backup purposes;
- periodic testing of backup restoration process.

The BCI Good Practice Guide identifies three basic continuity models:

- The Active/Backup Model: an active operating site and a corresponding backup site. The model relies on relocating staff from the operating to the backup site and maintaining copies of technology and data.
- Active/Active (Split Operations) Model: relies on two or more geographically separate “active” sites that inherently back up for one another.
- Alternate Site Model: a backup site periodically functions as the primary site for a period of time.

Business process owners and IT function personnel should determine what backup resources should be stored offsite. Offsite physical storage facilities for backup media have been the traditional solution - these should be environmentally appropriate for the media to be stored and be secure. There are various offsite backup options which will be explored for feasibility on a CGIAR-wide basis under the CGIAR Data Resilience Project, including

- using alternate Centers to act as each others’ backup site: e.g., CIMMYT and IRRI are committed to establishing this, using each others’ head offices as backup sites via Internet2;
- using institutional offices located at alternate sites;
- using the facilities of third parties (e.g., CGNET);
- mirroring transaction by transaction, so that data are completely up-to-date at the time a disaster strikes. Many software licenses permit this at no extra cost;
- mirroring periodically (e.g., nightly);
- keeping offsite transaction logs; and
- maintaining periodic data backups and the latest software at an alternate site, for installation into production mode at that site when required.

Concurrent ICT-KM projects on Second Level Connectivity and Research Networks (Internet2) are aimed at improving inter-Center telecommunications facilities, which will generate new opportunities to implement backup and disaster recovery of information with low recurrent costs. The Data Resilience



Project will explore these opportunities and will encourage Centers to standardize on hardware and software to facilitate the exchange of data and in particular, the ability to service each other as true backup sites in the event of serious emergencies and disasters.

Whatever arrangements are in place, Centers should implement procedures to ensure backups are taken in accordance with the defined backup strategy and that the usability of backups is regularly verified.

Exposure Draft: June 2004
First update: September 2005
Author: John Fitzsimon

