



Good Practice Note No. 3

Management of Information Technology Risks: an Overview

Part of a series of notes to help Centers and their internal auditors review their own Center 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

This note provides an overview of the processes for managing information technology IT risks and controls. It draws on the results of audits conducted by the CGIAR Internal Auditing Unit and external sources of good practice in this field.

Some of the good practices documented in this note are already being implemented in most, if not all, Centers, some are goals of Centers but are not yet implemented, and some may provide new ideas for Centers working on improving their management of IT.

It is also hoped that this note will stimulate discussion about the utility of and format for harmonizing practices and systems among Centers.

This note represents a broad, but not deep, analysis of IT management issues. This is the first edition and it is hoped that, with feedback from Centers and some experience with its use as an assessment tool and good practice reference, it can be improved. Also, some aspects of IT management identified in this note are or could well become the subject of more focused individual good practice notes.

This note discusses the following good practices:

PLANNING AND ORGANIZATION

- Articulate an IT strategy that is integrated into Center strategic and operational plans
- Create and regularly update an information architecture model
- Maintain a technological infrastructure plan. This may be part of an IT operating plan
- Regularly convene a planning or steering committee to oversee IT activities



- Ensure that all IT responsibilities are clearly defined and sufficiently staffed or outsourced
- Identify IT coordinators in organizational units within the Center to facilitate communication with the central IT group
- Adopt a budget format that would allow for IT spending across the Center to be planned and monitored
- Disseminate IT policies and procedures on the Center intranet
- Develop an IT security policy that can be a component of a Center's overall security policy
- Develop an IT security awareness program for Center staff and visitors
- Establish, as part of general policies on intellectual property, policies with regard to in-house or contract-developed software
- Adopt human resource management processes that promote a competent, ethical, continually improving IT team that can back each other up during absences
- Establish a systematic IT risk assessment framework, which could be a subset of an institutional risk assessment framework
- Adopt a general project management framework for IT projects
- Document IT procedures in a format that assists IT and other staff to implement them consistently
- Adopt a system development life cycle (SDLC) methodology for developing, acquiring, implementing, and maintaining IT systems and related technology.

ACQUISITION AND IMPLEMENTATION

- Ensure that the SDLC methodology fully addresses the process of identifying, specifying, and approving requirements
- Apply standard procurement procedures consistent with CGIAR guidelines to IT-related procurement
- Design and implement test plans and retain documentation of results
- Ensure that all system development is accompanied by adequate user support materials
- Prepare and monitor implementation plans
- Prepare and monitor data conversion plans
- Apply formal processes for new system acceptance and transfer to production
- Implement a formal approach to system change management



DELIVERY AND SUPPORT

- Implement service-level agreements
- Formalize the management of third-party service providers
- Implement system availability plans
- Promulgate and periodically test IT disaster recovery plans as part of overall Center business continuity plans
- Utilize available security features to adequately secure logical access to IT network resources
- Require all devices using the Center network to be registered
- Connect visitor laptops and wireless devices to the Center network through login to a Vnet or quarantined area protected by a firewall
- Establish and implement centralized, standardized procedures for managing user accounts
- Apply restrictions on network access commensurate with business needs and risk factors
- Implement adequate firewall products to protect connections between the Center and public networks
- Test firewalls on a regular basis using a range of software test tools in a controlled, formal manner and document the results
- Ensure that IT chargebacks are supported by a costing system that promotes economical use of IT resources
- Follow a structured, monitorable process for managing user queries through a help desk
- Establish procedures to record and track changes in configuration items
- Subscribe to continually updated virus detection and remedy software
- Establish and enforce clear policies restricting the use of personal and unlicensed software
- Establish and maintain an official software inventory that supports license compliance
- Define and implement a problem management system
- As part of disaster recovery plans, establish a defined data backup strategy applicable to headquarters and outreach locations
- Ensure that there are appropriate physical controls over access to servers
- Employ a gas fire-suppressant system in server rooms and place water sensors in both ceiling spaces and under false floors of the room. Place smoke detectors in the ceiling space, as well as on the ceiling, as this is where fires commonly spread.



- Implement appropriate fire safety organization and training as part of Center-wide fire safety arrangements
- Periodically check to ensure that protection for IT equipment from power interruptions and power surges is being adequately maintained

MONITORING

- Develop and monitor IT performance indicators

Acknowledgments

This note has been prepared solely for use by CGIAR Centers and their internal auditors. The note follows the structure of and refers to parts of the Control Objectives for Information and Related Technology (COBIT) Framework, copyright 1996, 1998 and 2000 Information Systems Audit and Control Foundation. For more on this Framework, visit www.isaca.org. The Internal Auditing Unit was assisted in the preparation of this note by Mr. Gerry Reardon, an internationally experienced New Zealand-based IT audit consultant on assignment with the Unit. We thank CGIAR Center IT managers and staff who provided input and advice on the preparation of this note.



Good Practice Note No. 3

Management of Information Technology Risks: an Overview

INTRODUCTION

Effective management of information and related information technology (IT) is becoming critical to organizations given the

- Increasing dependence on information and the systems that deliver this information;
- Increasing vulnerabilities and a wide spectrum of threats, such as cyber threats and information warfare;
- Scale and cost of the current and future investments in information and information systems; and
- Potential for technologies to dramatically change organizations and business practices, create new opportunities, and reduce costs.¹

Management processes that govern information technology should support the following objectives:

- Efficient and effective support of the Center's operational strategy
- Integrity, protection of confidentiality, availability and recoverability of the Center's electronic information resources
- Economical delivery of IT resources
- Adherence to Center policies and procedures

Centers may have specific requirements or characteristics as far as IT management is concerned. However, one can discern certain general principles, drawn from global sources on IT risk management

¹ Control Objectives for Information and Related Technology (COBIT), Executive Overview



and control, as well as practiced within the CGIAR system. These notes attempt to capture these principles in succinct form, as good practices, to provide a benchmarking tool.

For the purpose of analysis, this note has adopted the framework used in the Control Objectives for Information and related Technologies (COBIT)—an internationally recognized framework for thinking about IT controls. This breaks the subject down into four main domains:

- Planning and organization – the identification of the way IT can best contribute to the achievement of the business objectives; how the strategic vision is planned, communicated, and managed; and the organization of the IT functions put in place.
- Acquisition and implementation—to realize the IT strategy, IT solutions need to be identified, developed, or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain.
- Delivery and support—this domain includes security, continuity aspects, training and user support services, as well as the actual processing of data by application systems.
- Monitoring—assessment of IT activities over time for their quality and compliance with control requirements, including management oversight and assurance functions.

The COBIT framework is designed to cover all IT activities in all types of organizations and contains 34 high- level control objectives and some 318 detailed control objectives under these domains. This note focuses on a subset of those that have greatest relevance to CGIAR Centers, combines some in condensed form, or highlights particular aspects relevant to the Centers.

PLANNING AND ORGANIZATION

STRATEGIC PLANNING

Good practice

Articulate an IT strategy, which is integrated into Center strategic and operational plans

Center management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the Center’s strategic and operational plans to help ensure that the use of IT is aligned with the mission and business strategies of the organization.



Box 1. Coverage of IT strategic plans

There is no generally accepted standard to follow here. Sources of best practice suggest that strategic plans should consider the following:

- future directions for hardware and software acquisition,
- a strategy for application system ('develop-our-own' or purchase),
- knowledge management,
- intranet and extranet direction,
- use of consultants,
- IT initiatives to support the organization's mission and goals,
- opportunities for IT initiatives,
- re-engineering of IT initiatives to reflect changes in the organization's mission and goals,
- technological evolution,
- (changed) regulatory requirements,
- business process re-engineering,
- staffing (changes), and
- in- or outsourcing.

The main thing to emphasize, and this comes through loud and clear from all sources, is that the business plan must drive the IT plan. Sources suggest the avoidance of 'motherhood' statements such as "The IT department will continue to provide an efficient and effective service to users, etc....."

IT strategies, when approved by senior management, can also serve to document management decisions in addressing particular activities, applications, systems, or technologies.

In Centers reviewed to date, IT strategy had been addressed but at different levels of detail: from a brief insert (included with other non-IT items) in the Center's Strategic Plan, to quite a detailed discussion of many aspects of planned IT activity, set out in 3-year rolling plans.

DEFINING THE INFORMATION ARCHITECTURE

Good practice

Create and regularly update an information architecture model



COBIT gives attention to the following aspects:

- The IT function should create and regularly update an information architecture model, encompassing the corporate data model and the associated information systems. The information architecture model should be kept consistent with the IT long-range plan.
- The IT function should ensure the creation and continuous updating of a corporate data dictionary, which incorporates the organization's data syntax rules.
- A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined.
- Management should define, implement, and maintain security levels for each of the data classifications identified above the level of "no protection required."

TECHNOLOGICAL DIRECTION

Good practice

Maintain a technological infrastructure plan. This may be part of an IT operating plan. The IT function should create and regularly update a technological infrastructure plan, which is in accordance with IT long- and short-range plans. Such a plan should encompass aspects such as systems architecture, technological direction, and migration strategies.

The technological infrastructure plan should be assessed systematically for contingency aspects (i.e., redundancy, resilience, adequacy and evolutionary capability of the infrastructure).

IT management should ensure that hardware and software acquisition plans are established and reflect the needs identified in the technological infrastructure plan.

Based on the technological infrastructure plan, IT management should define technology norms in order to foster standardization. Corporate standard operating systems, desktop systems, and server configurations should be planned and implemented across Center sites (headquarters and outreach offices) to establish and maintain system compatibility across the Center. This should take into account CGIAR-wide agreed standardization plans.

INFORMATION TECHNOLOGY ORGANIZATION



Good practice

Regularly convene a planning or steering committee to oversee IT activities

Best practice sources suggest that committee membership should include representatives from senior management, user management, and the IT function. The committee should meet regularly and report to senior management.

Two Centers reviewed to date had established institutional IT committees in the past. However, both appeared to be defunct at the time of the audit review. Another Center relied on a general senior managers' committee to handle IT policy and strategic planning. In one case, a large regional office had its own local IT oversight committee. Some of the reasons given for the IT committees being in abeyance included a) the committee being too large and unwieldy; b) difficulty in forming a quorum due to extensive travel of members; c) members being seconded to other urgent tasks; and d) terms of reference inappropriate to the proper functioning of the committee.

Good practice

Ensure all IT responsibilities are clearly defined and sufficiently staffed or outsourced

Box 2. Functioning of IT oversight committees

It is generally accepted that this type of committee functions better and is more effective when the terms of reference are kept simple, with a focus on the setting of high-level IT policy and procedures. If there is extensive application system development going on in the Center, then the committee's terms of reference would include prioritizing requests for new system development; allocating funding, and increases in extra funding over a certain amount or percentage of the original grant; a watching brief over progress of system development; and the power to abort a project that had run off the rails, or was seen to be no longer viable or useful. These committees are less useful when they get bogged down in day-to-day IT operational issues.

In this regard, IT management is no different than other Center functions. COBIT gives attention to the following aspects:

- Appropriate quality assurance, systems, controls and communication expertise should exist within the IT organization or outsourced, depending on the size of the Center's IT function and expertise available in the local markets of the headquarters and outreach office host countries.
- Management should formally assign the responsibility for assuring both the logical and physical security of the organization's information assets.



- Management should create a structure for formally appointing data owners and custodians. Their roles and responsibilities should be clearly defined.
- All information assets (data and systems) should have an appointed owner who makes decisions about classification and access rights.
- Those assigned IT roles and responsibilities should have sufficient authority to exercise them.
- IT staff should have clearly defined position descriptions that delineate both authority and responsibility, include definitions of skills and experience needed in the relevant position, and suitable for use in performance evaluation.
- Segregation of duties should be maintained between various IT functions. In the case of CGIAR Centers, this should be applied to the extent practicable for relatively small organizations.
- Where IT functions are outsourced, management should implement relevant policies and procedures for controlling the activities of consultants and other contract personnel to assure the protection of the organization's information assets.
- There should be adequate structures for coordination, communication, and liaison between the IT function and various other interests inside and outside the IT function (i.e., users, suppliers, security officers, risk managers).

Good practice

Identify IT coordinators in organizational units within the Center to facilitate communication with the central IT group

This is particularly helpful for organizing such things as surveys of users, for disseminating and monitoring the implementation of new IT policy or procedural requirements, and data collection on IT inventory or requirements. IT coordinators should be given terms of reference for their role.

MANAGING THE IT INVESTMENT

Good practice

Adopt a budget format that would allow for IT spending across the Center to be planned and Monitored

Center management should implement a budgeting process to ensure that



- An annual IT operating budget is established and approved in line with the organization's long- and short-range plans as well as with the IT long- and short-range plans. Funding alternatives should be investigated.
- IT costs are monitored using the Center's accounting system, comparing actuals to budgets.

Separate identification within the IT budget of key aspects such as IT security and disaster recovery would help ensure that these key aspects of IT operations are kept in view.

COMMUNICATING IT POLICIES

Good practice

Disseminate IT policies and procedures on the Center intranet

All Centers reviewed to date agreed on the utility of disseminating IT policies and procedures on their intranets. This would be for the benefit of all users and especially beneficial to outlying regional centers. One Center has prepared a very detailed policy document.

A particularly important document is a Network User Code of Conduct. This should be sufficiently clear and detailed to inform users of their responsibilities with regard to the use of Center network computing resources and alert them to the potential penalties for not following the code.

The Center's code should be applicable to outreach offices as well as headquarters. The code should be clearly identified as applicable to all network users, whether they are Center staff, hosted staff of other organizations, scholars, trainees, secondees, contractors, or other visitors.



Box 3. Minimum guidance to be included in an information security policy according to ISO17799:200 Information Security

- Definition of information security, objectives and scope, and importance of information security as an enabling mechanism for information sharing
- Statement of management intent and support
- Brief explanation of security policies, principles, standards and compliance requirements of particular importance to the organization
- Compliance with legislative and contractual requirements
- Security education requirements
- Prevention and detection of viruses and other malicious software
- Business continuity management
- Consequences of security policy violations
- Definition of general and specific responsibilities for information security management, including reporting security incidents
- References to more detailed documents that may support the policy

Security issues are discussed extensively among Center IT managers and staff on the CG_IT ListServ.

In some Centers, there might be sufficient information on security policy and procedure material from disparate sources to form a cohesive manual if collated.

Box 4. Linkage of IT and information security policies

A CGIAR Center's IT security policy should be driven by a general information security policy. A general security policy could map directly onto IT security procedures, even down to a quite detailed level. For example, a policy that states that all employees should have access to the internet (a threat in itself), could result in the first rule in the firewall rulebase being 'Grant access to the internet to all'. It must be re-emphasized that a promulgated information security policy should drive IT technical security strategies and not vice versa. If there is a vacuum in the information security area, IT management might well go using their own initiatives with technical solutions to meet the ever increasing threats to networks world-wide.

Security and internal control awareness among users of IT can be improved in varying degrees in all the Centers reviewed so far, though one Center's IT Unit has been particularly proactive, with management support, in this area. An ongoing series of Security Awareness Seminars for staff is recommended.

These could supplement network user codes of practice and cover the illegal use of software, access to nonbusiness areas of the internet (e.g. music, pornography, and hacker sites), and sanctions that might be



imposed on offenders. There is a heavy emphasis on this in the draft IT Strategic and Operational Plan of one Center reviewed.

Good practice

Develop an IT security awareness program for Center staff and visitors

A security awareness seminar could cover such topics as

- Physical access
- Preventing theft
- Access privileges
- Viruses
- Use of personal, pirated and downloaded software
- Hackers

A separate brief good practice guide on the contents of a seminar has been prepared to assist Centers implement a security awareness program.

Good practice

Establish, as part of general policies on intellectual property, policies with regards to in-house or contract-developed software

The importance of this will vary according to the level of software development commissioned by a Center. Where software is internally generated, IP experts recommend that a Declaration of Originality (Computer Software) should be completed in electronic form and filed centrally. This will evidence ownership of the software, and facilitate, especially where software development in a Center is highly decentralized, the establishment of a central digital asset inventory.



Box 5. A specific area for policy attention: management of e-mail

CCGIAR Centers, like other businesses, have embraced e-mail for the efficiencies it promotes. However, the lack of e-mail management can be a significant problem yet to be addressed for many organizations:

- Many e-mails are official company records that must be preserved and made accessible upon demand. Policies and procedures should ensure that adequate and well-organized e-mail records are maintained.
- E-mail has become the main entry point for viruses, spam, and breaches of privacy. According to industry estimates, between 65 and 90% of viruses are transmitted via e-mail.
- E-mail traffic gives rise to issues of network efficiency, spam, denial-of-service attacks, and junk mail.
- Wireless communication and increased reliance on web-based e-mail give rise to additional security issues.
- Legal liability issues, such as retention of information, sexual harassment, or the use of legal disclaimers in e-mail messages, need to be addressed
- Employees need to be educated that, while Centers may make allowance for them to use official e-mail for private purposes, the e-mails sent and received through Center networks are not private or confidential to the employees.

Adapted from an article by Robert Moody and Beth Serepca, "Auditing Employee Use of E-mail," Information Systems Control Journal, Volume 1, 2003.

MANAGING IT HUMAN RESOURCES

Good practice

Adopt human resource management processes that promote a competent, ethical, continually improving IT team that can back each other up during absences

The principles for managing IT human resources are no different from those that would apply across a Center. COBIT highlights the following aspects, from an IT perspective, for IT management attention:

- Regularly verify that personnel performing specific tasks are qualified on the basis of appropriate education, training and/or experience, as required.
- Encourage personnel to obtain membership in professional organizations and maintain continuing professional education.
- Clearly define roles and responsibilities for personnel, including the requirement to adhere to management policies and procedures, the code of ethics, and professional practices. The terms and conditions of employment should stress the employee's responsibility for information security and internal control.



- Provide for sufficient cross training or backup of identified key personnel to address unavailabilities.
- Require personnel in sensitive positions to take uninterrupted holidays of sufficient length to exercise the organization's ability to cope with unavailabilities and to prevent and detect fraudulent activity.
- Ensure that IT personnel are subjected to appropriate background checks before they are hired, transferred, or promoted, depending on the sensitivity of the position.
- Implement an employee performance evaluation process, based on established standards and specific job responsibilities on a regular basis.
- Ensure that appropriate and timely actions are taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.

RISK ASSESSMENT

Good practice

Establish a systematic IT risk assessment framework, which could be a subset of an institutional risk assessment framework

External sources of best management practice, including COBIT, indicate that

- Center managements should establish a systematic risk assessment framework. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level, for new projects as well as on a recurring basis, and with cross-disciplinary participation.
- Regular reassessments should occur and risk assessment information should be updated with results of audits, inspections, and identified incidents.
- Risk assessment should be encouraged as an important tool in providing information in the design and implementation of internal controls, in the definition of the IT strategic plan, and in the monitoring and evaluation mechanisms.

There is no formalized risk assessment performed for IT in any of the Centers reviewed so far, apart from project risk assessments done by the consultants installing new financial applications in two of the Centers.

For each planned IT activity, the assumptions, constraints, and risks and how the risks will be dealt with (mitigate or accept) should be set out. The methodology used need not be specific to IT systems—a general risk assessment/ management methodology should work fine. Information is a vital asset in any



organization. The protection and security of information is of prime importance to many aspects of a CGIAR Center's business, and this has been recognized. It is therefore important that a Center implements a suitable set of controls and procedures to achieve information security and manage them to retain that level of security once it is achieved.

Sources for developing risk assessment include

- A general Australasian standard on risk management—AS/NZS 4360:1999. This is the first such standard of its kind in the world. This standard was adopted by both the Australian and New Zealand governments as a basis for public policies and procedures and may become the basis for an ISO standard in future. The standard is useful for establishing the basic methodology for risk assessment (see Box 6 below for a thumbnail sketch).

Box 6. Outline of AS/NZS 4360:1999

- Establish the context – break the analysis into business components (such as IT)
- Identify the risks
- Analyze the risks
- Evaluate the risks
- Treat the risks – avoidance, mitigation, acceptance
- Monitor and review
- Communicate and consult

- COBIT discusses IT risk management extensively. A summary is set out in Box 7 below.

While aiming for a reasonable, appropriate, and proportional system of controls and safeguards, controls with the highest return on investment (ROI) and those that provide quick wins should receive first priority. The control system also needs to balance prevention, detection, correction, and recovery measures.

- ISO/IEC 17799:2001 (Information Security Management). This provides a detailed source of information on potential security risks and how these should be mitigated. For more on this standard, see the section on implementing information security later in this note.
- COBIT – refer to Box 7 below.

Risk assessment is discussed further in a separate good practice guide.



PROJECT MANAGEMENT

Good practice

Adopt a general project management framework for IT projects

Box 7. COBIT references to IT risk assessment

COBIT suggests that IT-specific risk assessment can be viewed as six stages:

- Business risk assessment - Management should establish a general risk assessment approach that defines the scope and boundaries and the methodology to be adopted for risk assessment. The quality of the risk assessment should be ensured by a structured method and skilled risk assessors. Management should lead the identification of the risk mitigation solution and be involved in identifying vulnerabilities. Security specialists should lead threat identification and IT specialists should drive the control selection.
- Risk assessment approach— focus on the examination of the essential elements of risk and the cause/effect relationship between them. The essential elements of risk include tangible and intangible assets, asset value, threats, vulnerabilities, safeguards, consequences, and likelihood of threat.
- Risk identification—include qualitative and, where appropriate, quantitative risk ranking and should obtain input from management brainstorming, strategic planning, past audits, and other assessments. The risk assessment should consider business, regulatory, legal, technology, trading partner, and human resources risks.
- Risk measurement—qualitative or quantitative measures of the risks
- Risk action plan—identify the risk strategy in terms of risk avoidance, mitigation or acceptance.
- Risk Acceptance – formal acceptance of residual risks. Acceptance of certain risks may result from organizational policy, uncertainty incorporated in the risk assessment approach itself, and the cost effectiveness of implementing safeguards and controls. The residual risk should be offset with adequate insurance coverage, contractually negotiated liabilities, and self-insurance.

A general project management framework helps manage the risks of project failure.

COBIT recommends that a general project management framework should

- define the scope and boundaries of managing projects, as well as the project management methodology to be adopted and applied to each project undertaken. The methodology should cover, at a minimum, the allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, check points, and approvals.
- provide for participation by the affected user department management in the definition and authorization of a development, implementation, or modification project.



- specify the basis for assigning staff members to the project and define the responsibilities and authorities of the project team members.
- provide for the creation of a clearly written statement defining the nature and scope of every implementation project before work on the project begins.
- ensure that for each proposed project, the organization's senior management reviews the reports of the relevant feasibility studies as a basis for its decision on whether to proceed with the project.
- provide for designated managers of the user and IT functions to approve the work accomplished in each phase of the cycle before work on the next phase begins.
- provide for each project to have a project master plan to maintain control over the project throughout its life. This plan should include a method of monitoring the time and costs incurred throughout the life of the project. The content of the project plan should cover scope, objectives, required resources and responsibilities, risk management aspects (including test and other quality assurance plans and training plans), and arrangements for post-implementation review, and should provide information to permit management to measure progress.

Box 8. Why projects fail

- Poorly defined project objectives
- Lack of resources
- Poor project organization
- Incomplete requirements and specifications
- Inadequate testing
- Incorrect budgeting
- Mismanaged costs
- Misuse of system development methodologies
- Immature or poor technology infrastructure
- Inappropriate hardware

Extract from a presentation on project management prepared by ODAS Consulting.

Project planning efforts should be commensurate with the size of the project and its impact on the Center's business operations.



QUALITY MANAGEMENT

Good practice

Document IT procedures in a format which assists IT and other staff to implement them consistently

While IT procedures may not necessarily be documented in the format required of an ISO certification, they should, for quality assurance purposes, answer the basic questions of what, who, and how.

Two Centers reviewed are implementing quality management systems using the goal of ISO9001:2000 quality certification as an incentive. This ISO standard is the latest version of a general standard issued by the International Organization for Standardization for establishing a quality management system. It is applicable to any product or service delivery process. The implementing Centers have included all or some aspects of IT in the ISO coverage.

An ISO9001: 2000-compliant organization adequately documents its processes, builds into those processes the basis for validating if the processes are being implemented, and has a system for methodically verifying or auditing implementation and identifying opportunities to improve the process.

Good practice

Adopt a system development life cycle (SDLC) Methodology for developing, acquiring, implementing, and maintaining IT systems and related technology

COBIT highlights the following aspects:

- The chosen SDLC should be appropriate for the systems to be developed, acquired, implemented, and maintained.
- In the event of major changes to existing technology, management should ensure that an SDLC methodology is observed, as in the case of the acquisition or development of new technology.
- Management should implement a periodic review of its SDLC methodology to ensure that its provisions reflect current generally accepted techniques and procedures.
- Management should establish a process for ensuring close coordination and communication between customers of the IT function and system implementors throughout the SDLC. This process should entail structured methods using the SDLC methodology to ensure the provision of quality IT solutions which meet the business demands.



- A general framework should be in place regarding the acquisition and maintenance of the technology infrastructure. The different steps to be followed regarding the technology infrastructure (such as acquiring; programming, documenting, and testing; parameter setting; maintaining and applying fixes) should be governed by and in line with the acquisition and maintenance framework for the technology infrastructure.
- Management should implement a process to ensure good working relationships with third-party implementors. Such a process should provide that the user and implementor agree to acceptance criteria, handling of changes, problems during development, user roles, facilities, tools, software, standards, and procedures.
- The methodology should incorporate standards for program documentation, which have been communicated to the concerned staff and enforced. The methodology should ensure that the documentation created during information system development or modification projects conforms to these standards.

The methodology should provide standards covering test requirements, verification, documentation, and retention for testing individual software units and aggregated programs created as part of every information system development or modification project.

- The SDLC methodology should provide standards covering test requirements, verification, documentation, and retention for the testing of the total system as a part of every information system development or modification project.
- The SDLC methodology should define the circumstances under which parallel or pilot testing of new and/or existing systems will be conducted.
- The SDLC methodology should provide, as part of every information system development, implementation, or modification project, that the documented results of testing the system are retained.
- The organization's quality assurance approach should require that a post-implementation review of an operational information system assess whether
- The project team adhered to the provisions of the SDLC methodology and
- The extent to which particular systems and application development activities have achieved their objectives.



ACQUISITION AND IMPLEMENTATION

IDENTIFYING AND SELECTING AUTOMATED SOLUTIONS

Good practice

Ensure that the SDLC methodology fully addresses the process of identifying, specifying and approving requirements

Information systems acquisition, development, and maintenance should be considered in the context of the organization's IT long- and short-range plans. COBIT highlights that the SDLC methodology should provide that, prior to approval of a development, implementation, or modification project

- the business requirements satisfied by the existing system and to be satisfied by the proposed new or modified system are clearly defined.
- the solution's functional and operational requirements are specified.
- alternative courses of action that will satisfy the business requirements, their technical feasibility, associated risks including security issues, and costs and benefits, are analyzed.
- a software acquisition strategy plan is defined to indicate whether the software will be acquired off-the-shelf, developed internally, through contract, or by enhancing the existing software, or a combination of all these.
- attention is paid to the enterprise data model, file format requirements, security requirements, and system auditability while solutions are being identified and analyzed for feasibility.
- the design specifications are reviewed and approved by the affected user departments and the appropriate levels of management.



Box 9. Items for consideration with regard to program specifications per COBIT

Detailed written program specifications should be prepared for each information system development or modification project. The methodology should ensure that program specifications agree with system design specifications.

Specifications should address

- Mandatory and optional requirements
- mechanisms for the collection and entry of data
- input requirements
- all external and internal interfaces
- interface between the user and machine: should be easy to use and self-documenting (by means of online help functions).
- processing requirements
- output requirements
- the internal control and security requirements
- provisions for routine verification of the tasks performed by the software to help assure data integrity, and which provide the restoration of the integrity through rollback or other means.
- requirements for user reference and support manuals (preferably in electronic format)

Good practice

Apply standard procurement procedures, consistent with CGIAR guidelines, to IT related procurement

For significant outsourcing (defined by Center procurement value thresholds), a request for proposal (RFP) should be used to document specifications, which are prepared in close consultation with users.

COBIT highlights the following aspects relevant to IT procurement:

- Contracts for programming services should stipulate that the software, documentation, and other deliverables are subject to testing and review prior to acceptance.
- Products should be reviewed and tested prior to their use and the financial settlement.
- Management should require that for licensed software acquired from third-party providers, the providers have appropriate procedures to validate, protect, and maintain the software product's



integrity rights. Consideration should be given to the support of the product in any maintenance agreement related to the delivered product.

An acceptance plan for facilities and technology to be provided is agreed upon with the supplier in the contract and this plan defines the acceptance procedures to be performed and the criteria.

Good practice

Design and implement test plans and retain documentation of results

The SDLC methodology should provide for the testing of developed or purchased applications, according to project test plans and established testing standards before user approval. Documented results of tests should be retained.

DEVELOPING USER AND OPERATION PROCEDURES

Good practice

Ensure all system development is accompanied by adequate user support materials

COBIT highlights that the SDLC methodology should provide for timely definition of operational requirements and service levels for users, preparation and maintenance of user procedures, and operations manuals, and adequate training materials.

INSTALLING AND ACCREDITING SYSTEMS

Good practice

Prepare and monitor implementation plans

An implementation plan should be prepared, reviewed, and approved by relevant parties and be used to measure progress of system development projects. The implementation plan should address site preparation, equipment acquisition and installation, user training, installation of operating software changes, implementation of operating procedures, and conversion.



Good practice

Prepare and monitor data conversion plans

The SDLC methodology should provide that, where systems are being replaced, a data conversion plan is prepared, defining the methods of collecting and verifying (and “cleaning” if necessary) the data to be converted (balance transfers of individual transactions) and identifying and resolving any errors found during conversion.

Tests to be performed include comparing the original and converted files, checking the compatibility of the converted data with the new system, checking master files after conversion to ensure the accuracy of master file data, and ensuring that transactions affecting master files update both the old and the new master files during the period between initial conversion and final implementation. A detailed verification of the initial processing of the new system should be performed to confirm successful implementation. Management should ensure that the responsibility for successful conversion of data lies with the system owners.

Good practice

Apply formal processes for new system acceptance and transfer to production

Management should define and implement a formal process by which

- operations and user management formally accept the test results and the achieved level of security for the systems, along with the remaining residual risk;
- the user or designated custodian (the party designated to run the system on behalf of the user) validates its operation as a complete product, under conditions similar to the application environment and in the manner in which the system will be run in a production environment; and
- the system is handed over from development to testing to operations.

MANAGING CHANGES

Good practice

Implement a formal approach to system change management



IT management should ensure that all requests for changes, system maintenance, and supplier maintenance are standardized and are subject to formal change management procedures. Changes should be categorized and prioritized and specific procedures should be in place to handle urgent matters.

DELIVERY AND SUPPORT

SERVICE LEVELS

Good practice

Implement service-level agreements

External advice on best practice promotes the use of service level agreements to define the expected quantity, and quality of services delivered by the IT function, and constrains the demands of user departments to what the IT function can be expected to deliver within the available resources. The agreement should be adequately communicated and subject to periodic review.

MANAGING THIRD-PARTY SERVICES

Good practice

Formalize the management of third-party service providers

COBIT highlights the following aspects:

- Each relationship with a third party service provider should be subject to a formal contract before work starts.
- Management should ensure that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service (due diligence).
- The contract between the facilities management provider and the organization should be based on required processing levels, security, monitoring and contingency requirements, and other stipulations as appropriate.
- With respect to ensuring continuity of services, management should consider business risk related to the third party in terms of legal uncertainties and the going concern concept, and negotiate escrow contracts where appropriate.
- A process for monitoring of the service delivery of the third party should be implemented.

MANAGING PERFORMANCE AND CAPACITY



Good practice

Implement systems availability plans

Management should ensure the establishment of a systems availability plan, based on identified business needs and forecasts, to achieve, monitor, and control the availability of information services. The performance of IT resources should be continuously monitored and analysis should be conducted on system failures and irregularities. Modeling tools can be used to assist with the prediction of capacity, configuration reliability, performance, and availability requirements. Fault tolerance mechanisms, task prioritization and equitable resource allocation mechanism management should be implemented to help prevent resources from being unavailable.

SERVICE CONTINUITY

Good practice

Promulgate and periodically test IT disaster recovery plans as part of overall Center business continuity plans

No Center had a finalized, promulgated disaster recovery plan (DRP). However, in the case of one Center, the IT Manager had made a sound start in preparing such a plan, and could provide a good model. In another Center its ISO 9000:2000 documentation for IT addressed disaster recovery but was not a full-fledged plan on its own. Methodology for DRPs, in particular cost-benefit analysis, will be the subject of further research by the Internal Auditing Unit, and development of a standard DRP could be a suitable subject for collaboration between CGIAR Center IT teams.

A separate good practice note has been prepared to provide guidance on good practice with regard to disaster recovery planning.

SYSTEMS SECURITY

This section draws on two international sources of standards that address information systems security:

- The COBIT Framework used as the structure for this note. This can be perused for free at www.isaca.org
- ISO/IEC 17799:2001—Unfortunately the standard is not free but is available for purchase over the internet from local standards organizations. The Internal Auditing Unit has a license for one copy obtained from www.standards.com.au



These documents go into much detail (the ISO document is 65 pages) – only information security issues relevant to recent reviews are flagged in this note.

Box 10. Recommended elements of a comprehensive 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;
- 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;
- itemization of contracted service providers, services, and response expectations;
- 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

Require all devices using the Center network to be registered

Permitting unregistered hardware to plug into the network creates vulnerabilities for unauthorized intruders to exploit. Persons attempting to connect to the Center network using unregistered hardware should receive a message referring them to the IT department for registration.

Good practice

Utilize available security features to adequately secure logical access to networks



The logical access to and use of IT network computing resources should be restricted by the implementation of adequate identification, authentication, and authorization mechanisms, linking users and resources with access rules.

Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication and access mechanisms effective.

Various security features accompany purchased operating systems and applications. These should be reviewed and explicit decisions taken as to which of the available features should be activated, based on appropriately weighing risks and costs (e.g., there may be tradeoffs between logging features and system performance).

Important elements of logical security and some good practices, which should be considered with regard to their implementation, are summarized in Table 1 below.

Good practice

Connect visitor laptops and wireless devices to the Center network through login to a Vnet or quarantined area protected by firewall

All Centers reviewed allowed visitors to connect their laptops to the center's network, mainly so that the visitor can use the intranet and printers on the network. This circumvents the firewall barrier as the untrusted laptop is now within the network and could result in the network being exposed. All firewall administrators were aware of the security implications, but commented that there are a lot of scientific researchers and other guests visiting the Centers, and it has become accepted practice that these visitors should have this facility. However, one Center does have plans to quarantine these laptop users into a Vnet ('virtual network'). Wireless users will be controlled with the same method.

SECURITY ELEMENT	GOOD PRACTICE
System login	Must validate ID and password simultaneously Account locked after three consecutive incorrect password attempts Login messages should not identify operating system version or company Login messages should display warning message on trespassing
Passwords	Minimum password length - 6 characters for regular



	accounts; Eight characters for privileged accounts Forced change at initial login Passwords expire every 90 days for regular accounts; every 30 days for Privileged accounts Passwords not available for reuse for one year (12 passwords) Passwords stored encrypted Password strength tested regularly All accounts use passwords and no password is shared
User accounts	Individual user IDs Standard naming conventions Inactive accounts disabled after 45 days Delete account if no one requests to reactivate account for 60 days System accounts audited at least annually Noncorporate employees' accounts expire within 1 year
Information resource access control	Strong authentication exists for highly sensitive networks Access control list protection User sets special access file permissions
System logoff	Locked out if inactive for 20 minutes
Logging and auditing	Audit trails must be activated and record important data according to Policy: Audit should be set for restart, shutdown and system commands Audit trails must be reviewed regularly Alarms and actions activated Auditing records must contain user ID and actions Logs must be retained for 1 year, minimum

Good practice

Establish and implement centralized, standardized procedures for managing user accounts

Centralized, standardized procedures should be established to ensure timely action relating to requesting, establishing, issuing, suspending, and closing of user accounts. There should be a control process in place to review and confirm access rights periodically. Recent reviews indicate that Centers should pay particular attention to procedures for

- informing the IT group of user departures as well as arrivals. In relation to Center staff, this may form part of an exit process developed by the Human Resources group.



- allocating user accounts to temporary staff, scholars, on-the-job trainees, secondees, hosted staff from other organizations, contractors, and other visitors. Individual guest accounts should be allocated centrally for visitors. In one Center, allocation of user accounts is being linked to a campus badge identification number.
- monitoring and suspending user accounts that have not been active for a defined period.
- ensuring that user accounts have an applicable, informative full name and description. This helps to spot extraneous, illegal user accounts that may have been created for ulterior motives.
- using naming conventions for all user accounts to identify those not meeting the convention. One Center reviewed generally uses first full name and surname initial (though there were some exceptions).
- Renaming the Administrator and Guest user accounts. These are two of the first accounts an intruder will attempt to use.

Good practice

Apply restrictions on network access commensurate with business needs and risk factors

Time restrictions on network access are generally felt in two Centers reviewed to be unenforceable and potentially discouraging of researchers working outside regular hours. However, the restrictions were being implemented successfully in one Center reviewed. Organization unit heads were asked to identify the network access requirements of their staff. Requests for unlimited access to all staff of a unit were reviewed by the IT department, and the history of login times maintained by the unit usually countered what appeared to be unreasonable requests for unlimited access.

No Center reviewed enforced workstation access controls due to the nature of the Centers' operations, with research staff often moving around the center.

Good practice

Implement adequate firewall products to protect connections between the Center and public networks

For connection from the Center's networks to the Internet or other public networks, adequate firewalls should be operative to protect against denial of service attacks and any unauthorized access to the internal resources; and should control any application and infrastructure management flows in both directions.



Two of the Centers reviewed so far employed self-contained 'black box' type Internet firewalls, while the third used a Microsoft (MS) software product (ISA firewall), which runs on a PC under a MS operating system. The black box type of firewall is considered superior as it has its own hardware and software and is isolated from the rest of the network and has no links with any other operating system. While not suggesting that MS's ISA not be used (it does score highly, in product reviews), the black box does add another layer of security.

Reviews of Centers to date indicate that attention should be devoted to ensuring that

- Firewall software rule bases are properly administered, in particular, in relation to rule sequencing, rule documenting, and audit trailing; and not running the firewall under Administrator.

Good practice

Test firewalls on a regular basis using a range of software test tools in a controlled, formal manner and document the results

One Center reviewed is not using well-known and heavy-duty software tools such as Retina Network Security Scanner, COPS, Tiger, Tripwire, Satan, and ISS to analyze the firewalls. However, in this case, the firewall administrator had experimented with some 'freeware' products but no formal, intensive testing has been performed. All three firewall administrators were aware of security threat guides, such as the SANS Top 20 Vulnerability List, which are being constantly updated as new threats emerge.

One Center subscribes to a third-party, remote testing facility which attacks their firewall on a regular basis, in a controlled test mode.

Good practice

Ensure IT chargebacks are supported by a costing system that promotes economical use of IT resources

IT CHARGEBACK

COBIT highlights the following aspects:

- IT management, with guidance from senior management, should ensure that chargeable items are identifiable, measurable, and predictable by users. Users should be able to control the use of information services and associated billing levels.



- IT management should define and implement costing procedures to provide management information on the costs of delivering information services while ensuring cost effectiveness. Variances between forecasts and actual costs are to be adequately analyzed and reported on to facilitate cost monitoring.
- IT management should define and use billing and chargeback procedures. It should maintain user billing and chargeback procedures that encourage the proper usage of computer resources and assure the fair treatment of user departments and their needs. The rate charged should reflect the associated costs of providing services.

HELP DESK

Good practice

Follow a structured, monitorable process for managing user queries through a help desk

COBIT highlights the following aspects:

- Procedures should be in place to ensure that all customer queries are adequately registered by the help desk.
- Help desk procedures should ensure that customer queries that cannot immediately be resolved are appropriately escalated within the IT function.
- Management should establish procedures for timely monitoring of the clearance of customer queries. Long outstanding queries should be investigated and acted upon.
- Procedures should be in place which assures adequate reporting with regard to customer queries and resolution, response times, and trend identification. The reports should be adequately analyzed and acted upon.

CONFIGURATION MANAGEMENT

Good practice

Establish procedures to record and track changes to Configuration items

COBIT highlights the following aspects:

- Procedures should be in place to ensure that only authorized and identifiable configuration items are recorded in inventory upon acquisition. These procedures should also provide for the authorized disposal and consequential sale of configuration items. Moreover, procedures should be in place to



keep track of changes to the configuration (e.g., new item, status change from development to prototype). Logging and control should be an integrated part of the configuration recording system, including reviews of changed records.

- A baseline of configuration items should be kept as a checkpoint to return to after changes.
- IT management should ensure that the configuration records reflect the actual status of all configuration items, including the history of changes. Procedures should ensure that the existence and consistency of recording of the IT configuration is periodically checked.
- IT inventory records should be integrated with, or reconciled regularly with, the Center-wide inventory and general ledger balances.

Good practice

Subscribe to continually updated virus detection and remedy software

Good practice

Establish and enforce clear policies restricting the use of personal and unlicensed software

This policy can be highlighted in a network users' code of conduct.

Periodic checks should be undertaken of the organization's personal computers for unauthorized software. Compliance with the requirements of software and hardware license agreements should be reviewed on a periodic basis.

Good practice

Establish and maintain an official software inventory that supports license compliance

Official software should be inventoried and properly licensed. Software asset management tools should be employed.

For in-house produced software, library management software should be used to produce audit trails of program changes and to maintain program version numbers, creation-date information, and copies of previous versions.



PROBLEM AND INCIDENT MANAGEMENT

Good practice

Define and implement a problem management system

COBIT notes that such a system should ensure that all operational events, which are not part of the standard operation (incidents, problems and errors), are recorded, analyzed, and resolved in a timely manner.

The system should address such matters as emergency program change procedures, incident reports for significant problems, problem escalation, activation of the IT DRP, audit trail facilities which allow tracing from incident to underlying cause and back, emergency and temporary access authorizations, and emergency processing priorities.

DATA MANAGEMENT

Good practice

As part of disaster recovery plans, establish a defined data back up strategy applicable to headquarters and outreach locations

As part of disaster recovery plans, establish a defined data back up strategy applicable to headquarters and outreach locations

Procedures should be in place to ensure backups are taken in accordance with the defined backup strategy and the usability of backups is regularly verified.

Backup procedures for IT-related media should include the proper storage of copies of data files, software and related documentation, both on-site and off-site. In some Centers, the establishment of mirror sites, which allow for mutual backup, may be feasible. A process for rotating backup media that is physically stored should be established. Such backups should be stored securely (preferably in rated heat-resistant safes), and the storage sites should be periodically reviewed regarding physical access security and security of data files and other items.

One Center is taking advantage of a significant increase in Internet bandwidth by a provider to explore the feasibility of mirroring important scientific data over this connection to network storage outside the host country.



FACILITY PHYSICAL AND ENVIRONMENTAL CONTROLS

Good practice

Ensure there are appropriate physical controls over access to servers

Aspects to consider based on findings from Center reviews to date:

- Appropriate physical security over server room windows: all server rooms in the Centers reviewed had windows, either exterior windows, or windows overlooking other areas that had windows that were neither barred nor grilled.
- Server room door control: one Center used a programmable card key system; another planned to introduce this; the third had a manual key system only.
- Server room construction: generally, the server rooms were in cubicle type spaces and the walls were not slab-to-slab. All walls in the server room should be slab-to-slab to prevent intruders entering the room through the ceiling space.
- Server room identification: external best practice advice suggests that the location of servers should not be prominently signposted to avoid attracting the attention of intruders seeking to undertake malicious damage.

The ideal, secure environment for a server room and one that is often aspired to is what is known as a 'lights out' room, where the lights are switched off and the room is locked, and persons are excluded, apart from those performing equipment maintenance.

All Centers reviewed to date had their server consoles in the server room, which necessitated staff working in the room (though one Center is looking at software that would allow staff to operate the server consoles remotely). The advantage of having the server console in the server room is that it shares the same protection as the server: if it was placed outside, security would have to be also beefed up for that room.

Good practice

Employ a gas fire-suppressant system in server rooms and place water sensors in both ceiling spaces and under false floors of the room. Place smoke detectors in the ceiling space, as well as on the ceiling, as this is where fires commonly spread.



IT management should assure that sufficient measures are put in place and maintained for protection against environmental factors (e.g., fire, dust, power, excessive heat, and humidity).

Specialized equipment and devices to monitor and control the environment should be installed.

The main areas for attention identified from recent Center review are water and smoke sensors and fire suppression systems:

- Water sensors were not employed in any center, and smoke detectors were only used in the server rooms themselves and not in ceiling spaces.
- Two Centers had gas fire-retardant systems and these were considered satisfactory, although they had not been test fired (because of the cost involved in a test). These types of systems do have a high failure rate due to the gas either not reaching the required concentration level or not maintaining it long enough to be effective. This should not be a problem in the two Centers as the server rooms are relatively small in area. The third Center planned to install a gas fire-suppressant system in the near future, and the fire surveyors had already inspected the site.

Good practice

Implement fire safety organization and training, as part of Center-wide fire safety arrangements

This was an area that needed attention in all Centers reviewed to date. There were no promulgated and tested emergency evacuation procedures for any of the Centers. There had been no appointment of fire wardens for the area where the server room was located in two of the Centers. The third had appointed fire wardens, but no fire drill had been held for some time.

In no Center were there clear signs and instructions in the IT area (including the server room) telling people what to do in a fire or other emergency, and staffs were not trained in these procedures. No IT staffs in any Center were trained in the use of hand-held fire extinguishers.

Fire wardens should be appointed and fire drills held on a regular basis. Staff should be instructed in the use of hand-held fire extinguishers.

Good practice

Periodically check to ensure that protection for IT equipment from power interruptions and power surges is being adequately maintained



In general, uninterruptible power supply (UPS) equipment is a standard feature employed in Centers. Periodic surveys will help ensure that UPS equipment is being properly set up and maintained in place. UPS equipment with built in surge protection should be employed.

MONITORING

Good practice

Develop and monitor IT performance indicators

External sources of best practice identify the need to regularly monitor the IT benefits through high-level performance indicators. These should be in line with industry standards.

There were no systems of performance indicators to determine the effectiveness and acceptance of an IT unit's service function, employed in any of the CGIAR Centers reviewed (even those implementing ISO9000: 2000—this may be a missing element in the ISO 9000:2000 methodology).

Development of performance indicators may be a useful area for Center IT groups to coordinate on, to develop harmonized indicators.

A separate brief good practice guide on formulating IT performance indicators has been prepared to assist Centers think further about this aspect of IT management.

Box 11. Examples of potential IT performance indicators

- Extent of satisfaction with IT services and products
- Extent of awareness within the Center's research community of IT's support role
- The effectiveness of communication channels between IT and its users
- Effective integration of IT and financial planning, and research projects
- Effective integration of IT into management and administration across all spheres of the Center
- Level of reliability of equipment and services
- Extent of use of IT by the research community
- Success in meeting user needs as measured by objective means
- Maximum and average communication bandwidth usage
- Mean time for vendors to respond to call outs



Data should be collected for management information on performance against benchmarks. The dashboard format normally used to report network performance had been innovatively used to report other performance indicators in one Center reviewed.

The validity of measures used should be kept under review. This should include measures of IT customer satisfaction with regard to service levels. Appropriate action should be taken on management reports that identify areas for improvement.

One Center reviewed supplemented its dashboard with a detailed annual report to management on IT performance.

Exposure Draft: March 2003
(Adopted without change)
Author: John Fitzsimon