



SECTION H.4 – INTERNAL AUDIT SUPPORT TO THE MANAGEMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY RISKS

Introduction

The CGIAR Centers use information and communications technology (ICT) extensively for both scientific and business purposes, and ICTs are critical for effective global connectivity within and between the Centers, and with their partners and investors. Each Center governs its ICT policies and management, but there is a growing trend of collective action, harmonization and shared services among the Centers concerning ICT, and this is being actively promoted by the CGIAR Chief Information Officer (CIO) and the Center ICT Manager community. Some services have been jointly outsourced to external providers for some time and other services are now under similar consideration as the marketplace for these services evolves. ICT risks figure prominently in Center risk assessments as key risks which are highly dynamic and require close attention. It is therefore important that the overall internal audit coverage for a Center include assurance and advisory work related to these areas.

Ref.	Policy and Practice Requirements	IIA Standards and other references
H.4-1	<p>Policy: Internal Audit shall undertake or facilitate assessments of the Center’s management of ICT risks, either generally in support of the Center’s enterprise risk management system, or as focused topics in annual Center work plans</p>	
H.4-1:1	<p>Practice requirement:</p> <p>Internal Audit shall promote the use of common high level ICT business objectives for use in all Center enterprise risk assessment frameworks</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ At the CGIAR IT Managers meeting in ICARDA in 2005, the following high level ICT business objectives were agreed for the 	



	<p>purpose of structuring risk assessments:</p> <ul style="list-style-type: none"> ○ Maintain the availability, integrity and security of the Center's information resources (<i>Efficiency</i>) ○ Ensure the availability of IT systems and communications (business continuity) (<i>Efficiency</i>) ○ Ensure the Centre's ICT resources are used well (<i>Legal Compliance, Efficiency</i>) ○ Provide a quality ICT support service to the Centre (<i>Efficiency</i>) ○ Maintain the Center's ability to exploit innovations in Information Technology and Communications in the discharge of its mission (<i>Effectiveness, Efficiency</i>) <ul style="list-style-type: none"> ▪ Internal auditors should promote the use of these high level business objectives to organize ICT risk analyses in the Centers 	
<p>H.4-1:2</p>	<p>Practice Requirement:</p> <p>Internal Audit shall promote exchange of information with, and provide proactive advice to, the CIO and CGIAR IT Manager community of practice on ICT risk management issues relevant to the agreed ICT business objectives. The IAU will consult with the CIO on the best ways to operationalize this. This may include development and update of ICT-related Good Practice Notes, participation of auditors in the annual IT manager meetings, and in providing inputs to and facilitation of ICT-KM Program initiatives</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ In considering shared or common ICT risks and their mitigation, Internal Audit will take into account CGIAR System-level initiatives such as the Enterprise Security and Business Continuity Project. 	



<p>H.4-2</p>	<p>Policy: Internal Audit shall use the Control Objectives for Information and related Technologies (COBIT) Framework as the organizing basis for consideration of the design and effectiveness of Center ICT internal controls to address risks.</p> <p>Discussion:</p> <ul style="list-style-type: none">▪ The COBIT framework divides IT control processes into four domains:<ul style="list-style-type: none">○ 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 CGIAR IAU Good Practice Note on Management of IT Risks translates the relevant parts of the COBIT framework to the CGIAR environment. This should be the first point of reference for Internal	<p>COBIT Framework</p>
--------------	---	------------------------



	Auditors in developing terms of reference for audits of overall ICT risk management in the Centers.	
H.4-2:1	<p>Practice requirement:</p> <p>Internal Auditors shall consider as part of the planning of Center ICT audits, and ICT audit terms of reference shall clearly indicate, the scope of coverage in relation to whether the audits will include evaluation of:</p> <ul style="list-style-type: none"> ▪ Pervasive ICT controls - controls that focus on the overall management and monitoring of ICT in the Center. ▪ Network controls – relating to the availability and security of internet, intranet and extranet access ▪ Controls over the acquisition, implementation, delivery and support of ICT systems and services ▪ Operating system controls ▪ Application controls – relating to the availability, integrity and confidentiality of data processed and stored in particular applications such as financial systems, payroll systems, procurement systems, human resources management systems, research management systems or scientific databases ▪ End user computing controls – relating to controls over the use of spreadsheets and other user-managed software for business reporting and decision making and for storing and retrieving research data 	<p>ISACA Audit and Assurance Guideline G14: Application Systems Review,</p> <p>ISACA Audit and Assurance Guideline G11: Effect of Pervasive IS Controls</p>
H.4-2:2	<p>Practice requirement:</p> <p>Where the COBIT framework is supplemented by other external standards focusing on particular aspects, such as:</p> <ul style="list-style-type: none"> ▪ VallIT – framework for managing and 	<p>COBIT Mapping: Overview of International IT Guidance, IT Governance Institute 2004</p>



	<p>optimizing the value return on ICT investments</p> <ul style="list-style-type: none"> ▪ IT Infrastructure Library (ITIL) – best practices in IT service management ▪ ISO/IEC 17799:2000 – Code of Practice for Information Security Management ▪ NIST 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems ▪ ISF Standard of Good Practice for Information Security ▪ Center for Internet Security benchmarks <p>Internal Audit shall also consider these in establishing appropriate benchmarks for controls for IT audits of these topics.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ While COBIT provides the most comprehensive overall ICT control framework, various other references provide more in depth information for certain areas and should be consulted where appropriate. ▪ Synthesis of CGIAR-applicable components of various international and national standards, as well as COBIT, is made in the CGIAR IAU Good Practice Notes on IT-related topics. These GPNs should be used as the benchmarks for internal audits in these areas. 	
<p>H.4-2:3</p>	<p>Practice Requirement:</p> <p>In the case of audits of the ICT business objectives: “Maintain the availability, integrity and security of the Center's information resources” and “Ensure the availability of IT systems and communications (business continuity), Internal Auditors shall consider:</p> <ul style="list-style-type: none"> ▪ Center compliance with, and extent to 	



	<p>which the Center exceeds, the minimum agreed CGIAR standards for ICT security and recovery being developed under the Enterprise Security and Business Continuity Project.</p> <ul style="list-style-type: none"> ▪ Maturity of the Center’s privacy framework governing the protection of personal information (see also Section H.2) ▪ Measures in place to physically protect the ICT infrastructure from damage or loss ▪ Contingency planning for loss of physical infrastructure in Center locations 	
<p>H.4-2:4</p>	<p>Practice Requirement:</p> <p>In the case of audits of the ICT business objectives: “Provide a quality ICT support service to the Centre”, Internal Auditors shall consider:</p> <ul style="list-style-type: none"> ▪ Adequacy and deployment of collective skills of the ICT team in the Center ▪ Client incident (problem) reporting and feedback loop ▪ Impact of outsourcing arrangements on service delivery 	
<p>H.4-2:5</p>	<p>Practice Requirement:</p> <p>In the case of audits of the ICT business objective: “Ensure the Centre's ICT resources are used well”, Internal Auditors shall consider:</p> <ul style="list-style-type: none"> ▪ Controls in place to ensure Center compliance with host country privacy laws and contractual obligations to protect confidential information from third parties ▪ Controls in place to ensure software compliance across the Center ▪ Controls in place to manage efficiently all significant ICT investment projects in the 	



	<p>Center, such as new application system acquisition/development and deployment</p> <ul style="list-style-type: none"> ▪ The systems in place to ensure efficient use of existing ICT resources and limit non-work related use of such resources, including internet bandwidth ▪ The scope for further efficiencies from standardization of hardware and software ▪ The scope for further efficiencies from outsourcing ICT functions such as seat management ▪ The scope for further economies of scale in joint communications facilities, hardware or software purchasing, coordinated through the CIO ▪ The scope for increasing use of cost-effective communication technologies such as web-based video conferencing and VoIP (internet telephony) as primary vehicles for one-to-one and group interaction <p>Discussion:</p> <ul style="list-style-type: none"> ▪ In making assessments in relation to this business objective, Internal Auditors should take into account the plans and results to date of relevant investments under the CGIAR ICTKM program. ▪ Center ICT strategies and policies should be reviewed to see if they adequately address efficiency issues 	
<p>H.4-2:6</p>	<p>Practice Requirement:</p> <p>In the case of audits of the ICT business objective: “Maintain the Center’s ability to exploit innovations in Information Technology and Communications in the discharge of its mission”, Internal Auditors shall consider:</p> <ul style="list-style-type: none"> ▪ The adequacy of the ICT infrastructure to achieve the level of communications, across the Center locations and with external 	



	<p>partners. This includes adequacy of bandwidth for high speed internet connectivity, deployment of Web2 technologies (interactive web collaborative tools) to promote information and knowledge sharing</p> <ul style="list-style-type: none"> ▪ The adequacy of support for a mobile computing environment for staff ▪ The scope for better integration of computing applications supporting Center business processes ▪ Adapting new technologies, and adoption of data standards and exchange mechanisms, to promote better access to and use of Center scientific databases <p>Discussion:</p> <ul style="list-style-type: none"> ▪ In making assessments in relation to this business objective, Internal Auditors should take into account the plans and results to date of relevant investments under the CGIAR ICTKM program. 	
<p>H.4-2:7</p>	<p>Practice Requirement:</p> <p>Where Centers individually or collectively outsource ICT services, Internal Auditors shall obtain an understanding of the nature, timing and extent of the outsourced services; and the controls the Center has put in place to address the business requirements</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ Internal Auditors should assess whether the roles and responsibilities of third parties are clearly defined, adhered to and the risks associated with the outsourced services are identified and assessed. ▪ PA2100-12 / ISACA Document G4 provides detailed guidance on the review of management of outsourced ICT services 	<p>ISACA Audit and Assurance Guideline G4: Outsourcing of IS Activities to Other Organizations</p>