



FIRST ITEM ON THE AGENDA

**Updated Information Technology
Strategy (2007–09)**

1. The Information Technology (IT) Strategy for 2007–09 was presented for decision to the Subcommittee at the March 2007 session.¹ The Subcommittee recommended that the PFAC approve the Strategy conditional upon the Office submitting an updated strategy in November 2007, taking into account the views expressed by the Subcommittee during the March discussion. The first part of this paper summarizes the Strategy already presented, and the second part provides the requested updates as well as additional details.
2. The governance, support and management section of the Programme and Budget proposals for 2008–09² defines the context for IT at the ILO, as technology is one of several internal services assisting the Office as it promotes and implements decent work policies and programmes. The IT Strategy has been prepared with a view to achieving targets linked to the following outcome and indicators as defined in the Programme and Budget proposals for 2008–09 framework:

Outcome 1	Improve utilization of ILO human, financial, physical and technological resources in supporting programme execution
Indicator 1.1	Percentage of users who report being “satisfied” or “very satisfied” with governance, support and management services in 2008–09 user surveys
Indicator 1.4	Time required to complete internal IT HelpDesk requests
Indicator 1.5	Access to IRIS functionalities – Finance, Human Resources, Oracle Grants Accounting and the enhanced Strategic Management Module – in the field

¹ GB.298/PFA/ICTS/1.

² GB.298/PFA/13.

Summary of the Strategy

3. Linkages. Unlike previous IT strategies which were presented as stand-alone documents, this Strategy is aligned with the substantive work of the Office and linked to other strategies which are currently being implemented. Implicit connections with the Human Resources Strategy³ exist in the areas of staff skills, competencies, recruitment and learning. Although the IT Strategy already contains explicit references to knowledge sharing, the results-based knowledge-sharing strategy before this session of the Governing Body provides additional details on the linkage between these two strategies.⁴ Further information on linkages is found in document GB.300/PFA/9/1.

4. The strategic context consists of the driving forces (“where do we want to be”), the status of technology at the ILO (“where are we now”), and the objectives (“what are the expected outcomes”).

5. Information and communications technology (ICT) governance is executed at two levels: policy and technology. The structures of policy governance are:

- (i) Governing Body: the ICT Subcommittee of the PFAC;
- (ii) the Office: the Information Technology Advisory Committee (ITAC) and the Change Control Board (CCB); and
- (iii) the UN system: the ICT network of the High-Level Committee on Management (HLCM), which eventually makes recommendations to the Chief Executives Board for Coordination (CEB) that decides on IT matters for the whole UN system.

The governance of technology is implemented by the Information Technology and Communications Bureau (ITCOM), the central IT support unit for the Office. ITCOM is also responsible for implementing the IT strategy and for all day-to-day operational matters related to IT.

6. The implementation road map contained in the IT Strategy includes 12 initiatives grouped in three categories:

- (i) programme execution services: Collaborative working, EDMS and IRIS;
- (ii) infrastructure: technology watch, infrastructure, connectivity, remote/mobile, security and staffing;
- (iii) governance, support and training.

The Strategy described each initiative and provided a list of main activities and main outputs associated with each of them.

7. Alignment of the IT Strategy with the Strategic Policy Framework (2006–09) is detailed by listing all the relevant issues which are addressed by specific IT initiatives. Similarly, alignment with the Programme and Budget proposals for 2008–09 is described by listing indicators and the applicable IT initiative.

³ GB.294/PFA/16.

⁴ GB.300/PFA/9/2.

Updates to the Strategy

8. During the March 2007 session, the ICT Subcommittee identified several topics in the Strategy which required clarification, including governance, security, extension of IRIS functionality in the field, results-based management and the potential impact of UN reform. The ICT Subcommittee also requested that the Strategy include further alignment with recommendations highlighted in the report of the External Auditor, as presented in the March 2007 session, and a further breakdown of costs for each of the 12 initiatives contained in the Strategy.
9. The remainder of this paper provides an update on each of these topics and becomes an integrated part of the overall ICTS Strategy paper, as approved in March 2007. An annual report on progress will be provided to the ICT Subcommittee starting in November 2008.

ICT governance

10. Reporting to the PFAC, the ICT Subcommittee was established in 2005 to “assist the PFA in the governance of the ICT policies of the Office and would review and discuss substantive ICT issues that have a direct impact on the budget, with a view to making recommendations for consideration by the PFA”.⁵
11. Within the Office, the Information Technology Advisory Committee (ITAC) was formed in 2001 to guide ITCOM in the execution of its mandate. ITAC advises on the strategic direction for the use of IT throughout the ILO, reviews the implementation of major IT investments and establishes IT standards based on the recommendation of ITCOM. Chaired by the Executive Director of the Management and Administration Sector (MAS), ITAC’s membership consists of representatives from each sector at the management level, as well as representatives from the management of major functional units at headquarters and a representative for the field. ITAC currently meets three times a year and all its documents are posted on the Intranet.
12. Also within the Office, the Change Control Board (CCB) is a key pillar of the governance of IRIS; it was established to review and prioritize IRIS development and support, as well as to ensure that adequate resources are allocated to support its decisions. The CCB is comprised of senior management members of the IRIS community including FINANCE, Human Resources, the Internal Audit Office (IAO), ITCOM, Partnerships and Development Cooperation (PARDEV), PROGRAM, and other MAS units as needed. The CCB is chaired by the Executive Director of the MAS. In addition to dealing with IRIS issues, the CCB reviews all future development of computer applications, before any work is initiated; this ensures that any new development does not replicate already existing applications and, if the new work is justified, that it will be compatible with currently established centralized applications such as IRIS and EDMS. The review process has already started for all applications developed within the MAS; the next step is to extend this review outside MAS and formalize it through ITAC.
13. In the UN system, the “Information, Communication and Technology (ICT) Network brings together those responsible for information and communications technologies across the organizations of the United Nations system. It reports to the High Level Committee on Management (HLCM) and meets bi-annually. It first met in May 2002, as part of the reorganized sub-machinery of the Chief Executives Board (CEB). It is the successor body to the Information Systems Coordination Committee (ISCC), which in 1993 succeeded the

⁵ GB.293/3/1.

Advisory Committee for the Coordination of Information Systems (ACCIS) which was formed in 1983. The Network provides advice to the senior management of the organizations in respect of the long-term strategic development of information systems technology and services. It also reviews information and telecommunications standards with a view to advancing best practices across the UN system.”⁶

14. The governance of technology implemented by ITCOM is based on two standards: Control objectives for information and related technology (COBIT) and the Information Technology Infrastructure Library (ITIL). Focused on the goals of the organization (“the business”), COBIT consists of 34 processes divided into four domains: (i) plan and organize; (ii) acquire and implement; (iii) deliver and support; and (iv) monitor and evaluate. The ITIL is focused on service delivery through five processes for service support and five for service delivery. ITCOM started working on establishing this governance framework in 2006; it is a resource-intensive undertaking which requires continued involvement from the management and the senior specialists of ITCOM.

Security

15. The growing importance of ICT for the ILO in achieving its main objectives requires implementation of an auditable technical IT governance (ITG) based on internationally adopted standards. The complexity of the ILO’s global ICT system, as well as the exchange of information with external entities, requires the adoption of a process approach to the IT Security Management System (ISMS) as a part of ITG. ISMS processes structured for the “Plan-Do-Check-Act” model will be implemented as the Office-wide collaborative effort, coordinated by ITCOM under the guidance of ITAC. The main objective of ISMS is to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to all interested parties.
16. The key ISMS processes are: establishing IT security policy, managing risk, implementing security controls, auditing, management reviews, and continual improvement.
17. The IT security policy for the Office is being developed in accordance with the leading international standard ISO/IEC 17799:2005 Code of Practice for Information Security Management. This document will merge and formalize the work that has been undertaken over the last few years and address the following areas: asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems; information security incident management; business continuity management; and compliance.
18. The Office has selected risk management as a process within the COBIT governance framework. The main objective is to conduct an organization-wide assessment of the potential security risks and to formulate a risk treatment plan for the information assets. The scope of the security risk assessment includes: assetization; determination of gross risk; determination of gross control; and residual risk assessment.
19. Existing security controls will be identified within the scope of the security risk assessment and their adequacy determined together with asset owners taking into account the value of the asset and the criticality of its operation. Based on the risk exposure and its severity, a risk mitigation plan will be developed to document the mitigation strategy by implementing new controls, strengthening existing controls, transferring or accepting risk. The action plan involves steps to be taken, time frame for completion and responsibility.

⁶ <http://ict.unsystemceb.org/>.

20. The effectiveness of ISMS will be regularly reviewed by means of internal and external security audits, constant monitoring and logging of security events, annual risk assessments reviews and feedback from all interested parties. Management reports will be submitted to ITAC on a regular basis to ensure that the scope remains adequate and that improvements in the ISMS processes are identified.
21. Initial assessment covering information assets within ITCOM shows a strong management commitment to IT security, a high level of staff professionalism and determination, and reliable adequately scaled critical assets. Asset owners are mostly aware of vulnerabilities and weak links and have initiated upgrade plans within available resources. Areas which need improvement include: the physical environment of the main computer room; remote connectivity; disaster recovery plan; security controls on the desktop level; documentation; and IT security coordination with other departments (headquarters and field) to ensure policy compliance and cost containment. To summarize, the current overall IT security level can be considered as “intermediate”, taking into account the results of the initial assessment, the report of external audit, and the results of the IT security survey conducted by the UNICC.

Extending IRIS functionality in the field

22. **Prerequisites.** There are a number of general prerequisites that must be addressed at headquarters prior to extending IRIS functionality in the field. The major items are: the completion of the upgrade of IRIS to Oracle 12; the rewrite of the travel module; and the implementation of a formal IRIS support structure. The former items must be completed in order to avoid the requirement of significant retraining following deployment, and the latter is to ensure that field users have a single, consistent point of contact for support at headquarters.
23. **Connectivity.** The successful implementation and utilization of IRIS in the field is dependent upon the provision of adequate connectivity between external offices and the IRIS servers. The first step was to evaluate the existing connectivity; to this end, a study was conducted in 2004, then reviewed and updated in 2007. The study revealed that, currently, a number of external offices do not have sufficient connectivity to implement the full functionalities of IRIS; therefore, the connections to these offices must be upgraded prior to the deployment of additional IRIS functionality. Owing to the ongoing tendency for reduction in telecommunications costs, the Strategy is to upgrade connectivity for individual external offices on an as-needed basis, in line with the IRIS deployment schedule.
24. **Deployment tasks.** In relation to the specifics of implementing IRIS functionality in external offices, the high-level deployment tasks are: (a) consultation with the regions; (b) determination of the future operating models for the different types of external office; (c) determination of how individual procedures and tasks will be performed under IRIS; (d) design and build of additional IRIS functionality to support field operations; (e) performance of a conference room pilot to illustrate how IRIS can be utilized in the field; (f) set-up and delivery of training; (g) set-up and implementation of a support structure in the regions; (h) ongoing change management activities including but not limited to communications and expectations setting; and (i) selection of a pilot. These tasks are being coordinated and overseen by the Field Roll Out Task Team (FROTT) which meets monthly. The membership of the FROTT includes the senior management of the main functional units at headquarters, ITCOM, PARDEV, TURIN, the Staff Union Committee and IAO.

- 25. Consultation.** The first phase of consultations with the regions concluded in June 2007 with the completion of missions to Europe, Asia, Africa and the Americas; the mission to the Arab States is anticipated for late 2007. Each mission took the form of a workshop at which IRIS was presented and demonstrated to participants; detailed discussions were held to review current operations, ongoing issues and how IRIS functionality would support field operations in the future. The missions provided an opportunity to meet with over 150 representatives from external offices and to identify their expectations and concerns. Among the main items identified were: improved transparency and reporting; simplification and standardization of processes and procedures; and consistent application of rules and regulations. The principal areas of concern were: the possibilities of over-centralization; inadequate training and support; and job security.
- 26. Jakarta pre-pilot.** The IRIS pre-pilot for the Jakarta East project was implemented in July 2007 following a five-week training period. The post-live period was followed by the set up of a local support structure to maximize the autonomy of the project staff and Jakarta Office. The experiences from Jakarta are being closely monitored to ensure its success and also to provide key inputs to the strategy and approach for the implementation of IRIS in other external offices.
- 27. Risk management.** Extending IRIS to the field involves a number of significant risks; the management of these risks is monitored by the FROTT. The primary aspects of risk management involve identifying risks, determining the approach for managing risks and monitoring their potential impact and ongoing status. Risks are recorded in a risk log which is reviewed and updated regularly at FROTT meetings; necessary actions to mitigate the risks are taken accordingly. The most significant risks going forward are in the areas of: resources, connectivity, training and support and managing change.
- 28. Roll-out schedule.** Considerable progress has been made already in the roll-out of IRIS to external offices. This includes the deployment of the strategic management (SM) module (2004–05), initial training in the regions (2006 and the first half of 2007), the implementation of IRIS for a large technical cooperation project in Jakarta (July 2007) and the implementation of professional personnel actions (PAs) in Bangkok for the Asia region (August 2007). Further work currently under way includes a detailed review of operational procedures in the field and headquarters. The field structure review and UN reform are proceeding in parallel and could have an impact on the Strategy and schedule for the deployment of IRIS to external offices. IRIS data is being provided as input to the field structure review to support analysis and proposals are being elaborated regarding operating models for IRIS in the field for consideration by the field structure review team.
- 29. Pilot.** At present, the focus is on the implementation of a fully functioning pilot external office. The FROTT established the following seven criteria to determine the most suitable location for a pilot:
- (i) strong management buy-in;
 - (ii) sufficient staff capacity;
 - (iii) a wide variety of operational and administrative activities;
 - (iv) adequate technical infrastructure to support the daily use of IRIS;
 - (v) rapid, cost-effective access to IRIS expertise in the event that significant problems occur;
 - (vi) a low number of dependent offices to reduce the impact of any problems; and

- (vii) low dependency on computer system-based interactions with dependent offices to allow operations to continue manually in the event of major problems arising.

Based on the above criteria, Budapest has been selected as the pilot office.

- 30. Timeline.** The following table presents the timeline for the major components of the extension of IRIS functionality in the field:

Major activity	Projected completion	Status
SM P&B	10-2004	Programme and budget module deployed
SM IM	04-2005	Implementation management deployed
SM IP	10-2005	Implementation planning deployed
SM IR	07-2007	Implementation reporting deployed
Consultation	06-2007	Completed
Prerequisites	06-2008	In progress
Deployment tasks	08-2008	Not started
Bangkok PAs	08-2007	Completed
Jakarta pre-pilot	09-2007	Completed
Connectivity	As required	Jakarta and Bangkok completed
Pilot	11-2008	In progress
Roll-out schedule	06-2008	Not started

- 31. Costing.** After the IRIS project ended in 2005, the IRIS system and its support structure were fully integrated into the normal operation of the Office, specifically into ITCOM, PROGRAM, FINANCE, Human Resources and Procurement. The extension of IRIS functionality to the field will require IT, functional, change management and staff development resources. These resources will be found within the existing budgetary allocations of the concerned bureaux and departments at headquarters and in the field.

Alignment with the External Auditor's report

- 32.** The Financial Report and Audited Financial Statements for 2004–05, which were discussed at the 295th(bis) Session (May 2006) of the Governing Body,⁷ contained several recommendations related to IT and IRIS. At the March 2007 session, the Office presented a follow-up to the report⁸ which described the actions taken in response to the External Auditor's report. The alignment of the IT Strategy with these recommendations is outlined in the table below: the relevant recommendations are listed along with the applicable strategy initiative.

⁷ GB.295bis/PFA/1.

⁸ GB.298/PFA/5.

Recommendation	Initiative
R8. Develop and implement an accepted good practice methodology for software development and control, such as COBIT	Governance
R1. Ensure that effective governance arrangements are in place at the start of all major projects, and that these provide for independent assessment. For all future IT projects the Information and Communications Technology Subcommittee of the PFAC considers reviewing and monitoring project progress against clear plans and milestones	
R2. Ensure that the full costs are realistically forecast at the outset of a project, with an analysis of the ongoing maintenance and upgrading, and provide a more detailed cost analysis to the Information and Communications Technology Subcommittee of the PFAC	
R4. Greater attention be paid to assessing the adequacy of parallel running and user acceptance testing prior to implementation	
R3. IT projects should include implementation criteria and formal procedures for system approval by users and senior management	
R11. Undertake a formal and objective post implementation review of project management and the achievement of project objectives	
R10. Seek independent assurance on the effectiveness of the new internal control and framework systems within IRIS	Governance, IRIS
R27. Investigate the potential use of IRIS in providing an effective monitoring control through standard exception reporting	IRIS
R7. Obtain standard assurance reports on the system control environment as an integral part of the service level agreement with the external IRIS infrastructure provider	
R12. Undertake a business process review to maximize improvements in control and efficiency which should flow from IRIS; and to inform training needs	IRIS, infrastructure
R9. Establish formal IT security policies to cover IRIS, including a comprehensive business continuity and disaster recovery plan	Security
R6. Continue to ensure that adequate system support and knowledge transfer mechanisms are in place for future IT projects	Support, training
R5. Evaluate the approach to training and development of IRIS users, to ensure that user needs are met and sufficient resources are made available to fulfil this need	Training

Budgeting for IT initiatives

33. IT resources in the ILO are decentralized at headquarters and in the field. ITCOM, the central IT unit, is primarily responsible for the IT Strategy of the Office, and all its work is dedicated towards IT; the sources of funding (A, B, C and D) and the breakdown of expenditures towards implementing the 12 strategy initiatives appear in the table below.

ITCOM budget allocations	2006-07	2008-09
A. Regular budget		
Total staff	12 875 346	12 805 520
Total non-staff	8 703 290	9 491 725
Total regular budget	21 578 636	22 297 245
B. ICT investments (Part IV)		
	2006-07	2008-09 (est.)
EDMS deployment	500 000	345 000
Server replacements	170 000	50 000
Total Part IV	670 000	395 000
C. IT Systems Fund		
	2006-07	2008-09 (est.)
EDMS	147 317	80 000
WAN	87 194	185 000
D. PSI		
	250 000	250 000
Total allocations	22 733 147	23 207 245

ITCOM expenditures: IT Strategy (ITS) initiatives	2006-07	2008-09 (proj.)
ITS1: Collaborative working	626 365	666 998
ITS2: EDMS	1 214 783	1 337 036
ITS3: IRIS	8 485 221	8 159 635
ITS4: Technology watch	165 498	176 941
ITS5: Infrastructure	7 185 410	6 174 128
ITS6: Connectivity	570 989	705 935
ITS7: Remote/mobile	76 224	114 743
ITS8: Security	849 062	1 379 053
ITS9: Staffing improvements	36 374	39 235
ITS10: Governance	384 113	678 470
ITS11: Support	2 672 820	3 196 652
ITS12: Training	466 288	578 419
Total expenditures	22 733 147	23 207 245

Outside of the central IT unit, the following expenditures can be identified as being clearly dedicated towards IT:

	Support staff (2006-07)	Non-staff (est. 2006-07)
Headquarters	2 184 960	953 358
Field	1 897 724	625 096
Total	4 082 684	1 578 454
Total 2006-07	5 661 138	

34. There are some items and expenditures which are not specifically identified as "IT" in the ILO environment and are therefore not included in either of the above two tables. These are: infrastructure and support for conventional telephony (non-IT network, non-Internet), application development outside of ITCOM and functional support for IRIS.

Results-based management (RBM)

35. “The central principle of results-based management is that an organization must manage and measure its performance against the real-world outcomes to which it intends to contribute.”⁹ Tracking IT expenditures for each initiative of the Strategy, as in the above tables, is a very useful budget management and monitoring tool; however, it does not indicate that IT is “healthy” at the ILO and contributing towards the objectives of the Office. Two questions must be answered about the IT function at the ILO: (1) is it properly managed, effective and efficient; and (2) does it deliver towards the goals of the organization? The second question has already been addressed through IT-related indicators formulated according to the RBM framework of the Office; these appear in the Programme and Budget for 2006-07¹⁰ and 2008–09 (see paragraph 2 above), and in the knowledge-sharing strategy.¹¹ In addition to these indicators, under initiative 11 (Support) the IT Strategy calls for the introduction of service level agreements (SLAs) to formalize, standardize and manage the relationship with IT clients and users throughout the Office.
36. Addressing the first question requires a different approach. Some basic elements of RBM have already been incorporated into the IT Strategy: initiatives, activities and outputs have been formulated towards the goal of achieving the objectives of the IT Strategy. These elements are useful components of the strategy; however, as it is currently formulated, the Strategy is not yet fully compliant with the RBM framework of the ILO. In the case of IT, the high-level indicators, baselines and targets will require further refinement to ensure that IT objectives are being achieved efficiently, effectively and economically.
37. The IT profession has, for many years, been using standard governance frameworks, such as COBIT and ITIL described above, to ensure that IT is following best practices and implementing a management framework that is based on measurable indicators and results. ITCOM has committed to implement these industry standards. Starting in 2006, IT governance consultants reviewed and assessed all of ITCOM’s processes and scored each one of the relevant COBIT and ITIL processes on a “maturity level” scale of 1 through 5 where: 1 is “ad hoc”; 2 “defined”; 3 “documented”; 4 “controlled”; and 5 “measured”. ITCOM’s processes were all rated below 3, indicating that much work needs to be done. We are allocating resources towards this implementation, and we will be reporting in the future on baselines and targets for our COBIT and ITIL processes. Although this is an important undertaking, it cannot take priority over the more pressing operational issues of the IT infrastructure, IRIS, and the EDMS; nevertheless, the implementation is projected to be completed by the end of 2009.

United Nations reform

38. Initiated by the Secretary-General, the reform of the UN system will strive for a “One United Nations” through a coherent approach for enhanced collaboration among organizations of the system and the consolidation of activities at all levels. In its report,¹² the High-Level Panel on United Nations System-Wide Coherence presented the case for

⁹ GB.297/PFA/1/1.

¹⁰ GB.292/PFA/8.

¹¹ GB.300/PFA/9/2.

¹² UN GA A/61/583.

reform by stating that the “United Nations needs to overcome its current fragmentation and to deliver as one.”

39. The “One United Nations – Catalyst for Progress and Change” report¹³ has mapped out “The Way Forward for the UN System”, in which knowledge sharing and Information Technology figure prominently. The ICT network of the Chief Executives Board will respond with a concrete set of proposals and initiatives towards the goal of “Delivering as One”. These initiatives address the following areas: ERP (enterprise resource planning) systems, common services (data centres and global networks); UN system portal; internationally recognized standards, common business case and costing; and UN system directory. To date, the first three areas have been developed into detailed proposals for further exploration through studies and working groups.
40. After much debate, the ICT network has concluded that the objective of a single ERP for the UN system is not feasible in the medium term. A large number of UN organizations have already implemented their own ERP solutions at great financial cost and major internal adjustments. However, the existence of the three dominant products – Oracle, PeopleSoft, and SAP (soon to become two dominant products) – used by UN organizations presents a major opportunity to harmonize the underlying business processes and ensure that they are based on common UN best practices. The ICT network will propose the formation of “UN ERP Exploitation Groups”, for the three products, supported by networks of experienced UN managers from each of the relevant functional areas and from IT. In the short term, it is expected that opportunities will be identified to share the costs of running ERP applications in common UN data centres, or through joint contracts with providers of outsourced and offshored solutions. In the longer term, it is hoped that a single UN best practice may evolve which would then be introduced across all ERP solutions, or ideally into a single ERP product.
41. The ICT network is initiating two studies to explore the feasibility and costs for common UN services in two areas: data centres and global networks. These two studies are being funded through voluntary agency-wide contributions, and the ILO has already committed to participate in the funding of both studies. Once they are initiated, ITCOM will be actively participating in both studies. The Office is already making use of the UN International Computing Centre (UNICC), a successful implementation of shared common IT services in Geneva, to host a disaster recovery configuration for essential services, such as email. With 50 offices located around the world, the ILO will be extremely interested in a cost-efficient global telecommunication network, should the feasibility study recommend that it be implemented.
42. The objective of the UN system portal is to “facilitate an improved and consistent image for the UN system through the introduction of standardized knowledge-sharing practices and a common communication platform.”¹⁴ The organizations, agencies, programmes, funds, and other entities that make up the UN system have been developing their web sites over the last few years, independently of one another. This has resulted in multiple sites presenting a mixed message and causing confusion for the general public: different “look and feel”; inconsistent organization and categories of the posted information; overlapping information across sites, duplication and slight variations of the same information; inaccuracies and outdated information, etc. The ICT network is building a business case for a unified UN system Internet presence implemented on a standard platform, and backed by inter-agency knowledge sharing. The expected benefits of this initiative include: a clear

¹³ <http://unsystemceb.org/oneun/>.

¹⁴ ICT network internal working paper.

message delivered to the public; an improved image for the UN system; enhanced visibility for all organizations; and system-wide efficiencies and cost savings.

43. Starting in early 2007, the ILO embarked on a knowledge-sharing (KS) initiative with UNDP. Specifically, the IT teams in both organizations have been designing and implementing a secure mechanism (using Federated Identity Management software) to share internal documents and data, including contact information of the staff in both organizations. This KS solution, which is expected to be operational by the end of 2007, will make it possible for ILO officials to have access to internal UNDP information; similarly, UNDP Resident Coordinators and country teams will have access to the knowledge and expertise of the ILO.
44. Under initiative 4 (technology watch) of the IT Strategy, the ILO will continue to actively participate in the ICT network to contribute expertise and resources towards the goal of “Delivering as One”.
45. *The Subcommittee may wish to recommend to the Programme, Financial and Administrative Committee to approve this updated Strategy.*

Geneva, 21 September 2007.

Point for decision: Paragraph 45.