ICT Reference Group

Guidelines for Delivering as One in ICT at the Country Level

March 2014

Contents

1 Introduction

The purpose of this document is to provide guidance to Information, Communications and Technology (ICT) practitioners in UN Country Teams (UNCT) in identifying country-level opportunities for, and developing action plans to implement common initiatives.

These guidelines establish the foundation for country-level solutions such as collaboration, information and knowledge sharing. Recognizing that different technologies and processes are in use by various agencies at the country level, the goal of these guidelines is to focus on improving efficiencies in delivery of UN ICT services and leveraging ICT in support of core UN business needs.

Sharing ICT services among the various UN Agencies at the country level is not a new concept. Many Country offices are already sharing IT resources and equipment.

These guidelines are presented in the form of a process to be followed, as well as recommendations and lessons taken from Delivering as One countries. The approach is to harmonize ICT services, standards and processes of individual United Nations agencies, and at the same time ensure that existing returns from agency ICT investments are not only maintained but also maximized. These recommendations aim to facilitate the establishment of shared ICT services and resources at country level in the spirit of Delivering as One.

The ICT Reference Group, with the support and endorsement of the UN Development Group (UNDG) and the UN ICT Network, has prepared this document.

1.1 Background

The Quadrennial Comprehensive Policy Reviews (QCPR) encourage the UN System to continue to work to increase efficiency, effectiveness and coherence at the country level. To this end, the UNDG's ICT Reference Group has worked to support Delivering as One countries in their ICT harmonization initiatives.

Frequently, agencies implement and deploy ICT capabilities, services and infrastructures in parallel, each one customized towards each agency's governance, business processes and operating environments. Accordingly, a diverse array of technologies, assets and services are currently deployed at both Headquarters and country levels.

1.2 Business Perspectives of ICT

ICT is a strategic capability and mission critical service that enables the work of the UN at HQ and Country Levels.

While individual agencies may require the development of different global ICT services, every effort should be made for alignment and to seek common solutions where possible.

Delivering as One in ICT is a mandate for inter-agency cooperation to leverage existing agency investments in ICT infrastructure and resources. It does not aim for total consolidation, or to unnecessarily replace existing infrastructures and services. Rather, it is a framework for collaboration for the benefit of all, which will provide business-driven efficiencies based on industry best practices.

1.3 Key Benefits

The following are the major benefits to agency operations at country level for Delivering as One in ICT:

a) Improved overall ICT response to business needs. ICT collaborating at country level facilitates UN agencies to share existing or future business solutions, including ICT capacity, expertise and services, which are often scarce especially in developing countries.
b) Increased ICT value to the business. Cooperation leading to ICT service sharing results in better utilization of agency resources.
c) Synergies gained through collective strengths. ICT collaboration through sharing of expertise, volume procurement, and collective bargaining, generates economies of scale.
d) Enabled agencies with less ICT capacity, as they have the opportunity to access better services.
e) Improved business continuity posture. Through resilient infrastructures, Delivering as One in ICT will improve ICT business continuity of the collaborating agencies.
f) Inter-agency cooperation strengthens ICT staff skills and capacity at country level.

1.4 Risks

Due diligence process should be taken to mitigate the following risks:

a) Increased operational expense for agencies, without value-added services. Joint ICT projects should potentially substitute or enhance existing services whilst reducing operating costs.
b) Unsustainable ICT services and business solutions in the medium term, if they are set up only for the sake of cooperation. Sustainability issues should be considered in the business case for ICT services and business solutions, particularly the Total Cost of Ownership over a set period.
c) Lack of governance for ICT services and business solutions. Shared ICT services may involve pooling of funds, cost-recovery and sharing of ICT staff for the maximum benefit. The necessary governance, roles and responsibilities, agreements and agency commitments at global and country level need to be in place to underpin this cooperation.
d) Lack of commitment from the business for the ICT services and business solutions. Technology projects must be business driven and fully supported by the Country Teams, with early involvement of respective ICT working groups.
e) Inability of ICT services and business solutions to deliver guaranteed levels of service. Implementation of inter-agency service performance management must be addressed through governance mechanisms.
f) Additional stress to ICT staff resources in the country. Setting up shared services require different technical and business skill sets and these projects are typically implemented on top of existing workload of ICT staff. Adequate support needs to be put in place to provide ICT staff the necessary time, effort, training, and expertise to implement ICT projects.
g) Limited capacity at the level of the ICT Reference Group. If the number of Delivering as One countries is increased, the ICT Reference Group would require additional resources for scaling up.

1.5 General Strategy

Delivering as One (DaO) in ICT focuses on optimizing and leveraging ICT services and business solutions. As such, the general approach is to:

a) Setup the Country Team ICT working group and its governance to serve as forum for country-level ICT cooperation for operational, administrative and substantive solutions.

b) Assess existing and future needs and practices at the country level and how they can be supported through ICT services and business solutions, building the ICT component of the DaO roadmap, which identifies key ICT assets, spending and services common among UN agencies.
c) Identify the gaps/opportunities based on the ICT DaO roadmap.
d) Consult other DaO projects, documented guidance for common approaches and practices, lessons learnt as well as the ICT Reference Group for globally agreed standards.
e) Follow a business case approach; examine opportunities for optimizing ICT services through the interconnection of existing networks or the construction of new services to fill the gaps; design sustainable mechanisms for support, operation and maintenance of the services/solutions.
f) Follow a project-based approach with a formalized change management process.

2 Organizing for Delivering as One in ICT

2.1 Establishing UNCT Commitment

The value of ICT harmonization can only be realized if the benefits of such cooperation is clearly established and recognized at the agency level. Full support and commitment will then be provided. While remaining the prerogative of each agency, typically the UNCT and/or Operations Management Team (OMT) members appoint ICT focal points from each agency, and provide the necessary time and resources for these ICT focal points to meet each other and organize as a distinct, separate sector in the UN community. Business staff of agencies without country-level ICT focal points should consult regional or Headquarters ICT management regarding local participation in any shared solutions and services. Accordingly, agencies must include as part of ICT work plans objectives and goals that are consistent in supporting Delivering as One.

2.2 Establishing the Country Team ICT working group

UNCT commitment is clearly articulated by establishing the Country Team ICT working group (ICTWG), which serves as a forum for discussing ICT cooperation and harmonization. The ICTWG is composed of country-level ICT staff and related focal points of each agency, with clearly defined roles and purposes. Annex A defines a sample terms of reference and proposed modalities of operation of the ICT working group. The ICTWG must be given a clear mandate by the UNCT and asked to report to the OMT. A strong link between the ICTWG and OMT is considered best practice (e.g. ICTWG Chair is a member of OMT). Establishing clear Deliver as One goals in each team member's annual performance plan and review will encourage and provide maximum opportunity for cooperation.

The ICTWG should take the lead from the OMT for any UN House or shared premise ICT initiatives that may be planned, and which would impact the nature of the ICT opportunities or services being analyzed.

2.3 Role of the ICT Reference group

The ICT Reference Group is the forum where ICT departments discuss and agree on ICT policy questions posed by Delivering as One initiatives. The ICT Reference Group is the conduit for the ICTWG to address technology differences that hamper harmonization. As such, the ICT Reference Group provides business guidance in ICT matters, and technical guidance for projects that affect globally shared or corporate ICT services and business solutions, in harmony with corporate policies at the agency level.

The advice provided by the ICT Reference Group may be superseded by specific agency policies.

Support or information requests originating from the chair of the ICTWG should be directed to the ICT Reference Group (ict.reference.group@one.un.org).

2.4 Identifying ICT Opportunities and Gaps

2.4.1 Goals of Conducting Joint ICT Assessments

The ICTWG and the ICT Reference Group conduct joint ICT assessments on as-needed basis to gather information regarding agency ICT spending, architecture, assets, resources and operational issues. The goals are to obtain sufficient information to allow:

a) Shared understanding of UN country-level ICT services. This view highlights eventual gaps in ICT services to agencies, and identifies opportunities for sharing and collaboration.
b) Identification of common vendors and service providers. This will allow the ICTWG to assess opportunities for shared procurement of ICT supplies, assets and service contracts.
c) Identification of ICT needs of country programs and common business units. It is a shared responsibility of the ICTWG and the OMT to look at services needed by country programs and inter-agency business units. (See also Annex B)
d) Sharing of agency ICT spending and upgrade plans. The ICTWG may need to examine, with no prejudice to a given agency and with its consent, ICT current expenditures and agencies upgrade cycles for equipment, software and services, to evaluate if these could be synchronized and done in common to take advantage of shared procurement. This could lead to harmonization of services, hardware and software and possible cost reduction.
e) Shared understanding of UN ICT staff resources. The ICTWG will collect from the different agencies the current ICT profiles. Leveraging agencies' staff for end-user support, infrastructure development, special ICT projects and identification of ICT support gaps will be done in collaboration with each agency providing the staff. Training may be needed to achieve the above.

Note: Annex B shows sample formats for information that could be gathered during joint assessment. Analysis of ICT spending to identify potential optimizations opportunities should be as precise as possible. It is however acknowledged that it may be quite challenging to gather the details of all ICT costs. Nevertheless and whenever it is not possible to gather precise information, estimation models could be used, aimed at providing a realistic evaluation of overall costs, subject to validation by the concerned agency. More detailed analysis and spend research shall be performed once a candidate agency for reduction or optimization based on economies of scale has been identified and has agreed to participate.

2.4.2 Identifying Potential ICT Efficiencies and Value -Added Services

A thorough ICT assessment should yield enough information for the ICTWG to initiate discussions with agencies. Following is the list of some of the ICT areas that could be discussed:

a) Local telecommunications services (e.g. telephony providers, mobile telephony) and contracts - can be consolidated as one UN contract to take advantage of volume procurement and reduced group calling, taking into consideration individual contractual agreements with the service providers.
b) Private (VSAT, MPLS...) and public (Internet) connectivity - could be eventually consolidated, shared or replaced with other inter-agency alternatives, aiming at achieving reduced cost, increased reliability and availability of the links.
c) Shared data centre opportunities, facilitating hosting services and server virtualisation and consolidation.
d) End-user, basic ICT and desktop support services could be shared. A central unit could be set up to provide end-user support as a shared service. Participating agencies should agree and sign an Interagency agreement authorizing such services (Sample attached in Annex H)

e) Equipment procurement and maintenance contracts, joint contract management, vendor databases (e.g. UNGM) and LTAs, including piggybacking on existing LTAs, whenever contractually possible. The above will be coordinated with common procurement groups if applicable.
f) Shared business solutions and services, which facilitate the collaboration at the country level (e.g. shared resources booking, HR rosters, procurement tracking, etc.)
g) Contingency facilities and ICT standby inventory could be constructed as a central service to serve as the UN Country Office's standby capacity. A cost recovery system will need to be implemented to protect initial assets investments of all agencies and allow replenishment of stocks.
h) Security and day-to-day radio telecommunications services and infrastructure could be shared and managed as a shared service.
i) Provision and sharing of training resources inclusive of e-learning or training material could be shared among ICT staff to maximize knowledge transfer and leverage existing available resources.

2.5 Presenting the ICT Roadmap for UNCT Endorsement

The ICTWG shall draft the ICT Roadmap to be endorsed by the ICT Reference Group before submission at the local level. This endorsement will raise the awareness of the UNCT and ICTWG of ICT harmonization issues at the HQ level.

Once endorsed by the ICT RG, the roadmap should be presented by the ICTWG in collaboration with the OMT to the UNCT. The ICTWG shall seek to obtain the UNCT's endorsement and commitment to the ICT roadmap, which calls upon resources for conducting research that is more detailed, cost-benefit analysis and consultations with technical experts, vendors, agency Headquarters and the ICT Reference Group.

The ICTWG will then begin the next step, which is to draft a business case document to support the proposed changes.

3 Preparing for Delivering as One ICT Projects

3.1 Preparing the Business Case

A good Business Case needs to be realistic, accurate and practical. The Business Case is drafted by the ICTWG and must reflect demonstrated returns and benefits. The Business Case will be submitted to all agencies for validation.

A typical business case will take no longer than 30 days to prepare and it should contain at least the following sections:

a) Executive summary
    1) Existing ICT services and business solutions
    2) Common needs applicable to all agencies
    3) Solutions for meeting those needs
    4) Gaps based on identified needs and existing services and solutions
    5) Primary benefits (savings, resilience, availability, simplification etc…)
    6) Value Statement and Total Cost of Ownership (TCO)
    7) Recommendations and deliverables
b) Vision and Organizational Objectives
    1) Link to programmatic, operational and strategic (HQ) objectives
    2) Validate the linkages (Data collection, Surveys, meetings, etc.)

c) Purpose/Problem Statement, Sponsor and Stakeholder Statements
d) Situational Assessment
    1) Country ICT Assessment (commercial options and capacity in the country)
    2) Regional ICT Assessment (commercial options and capacity in the region)
    3) ICT Assessment of UN country offices
e) Critical Assumptions:
    1) Full support from the HQ, UNCT, OMT and ICTWG
    2) Approval of this business case is required to release funding for the project to proceed
    3) The presence of ICT experts during the detailed design and installation phase is critical. The ICTWG shall describe and define the needs in terms of expertise.
    4) Following business case approval a joint interagency procurement instances will be carried out.
    5) Training for the UN ICTWG members will be required to ensure the system can be maintained by UN ICT personnel.
    6) Clear processes must be documented, and agreed upon by all UN agencies, to define the service agency by whom the ICT services and business solutions will be managed prior to project implementation.
    7) Same arrangements apply to the shared funding model as well as to the change management process.
    8) In line with Delivering as One principles, all agencies are expected to participate and support the project once validated. In general, the more agencies use the shared services, the better are the return on investment and overall value of the project. However it may also be the case that not all agencies will need all of the shared services, in that case, partial services option should be made available.
    9) It should be acknowledged that for the shared project to work, it is highly important to provide the commitment or opt out option as part of business case development, to allow the project to dynamically adapt to changing environment or conditions.
    10) Green field approach is neither appropriate nor acceptable as most, if not all, agencies already operate proprietary services and infrastructure.
f) Critical Risks:
    1) Each UN agency will continue to maintain its parallel ICT services at country level.
    2) Service agency imposes their standards.
    3) There will be cases where, due to operational or other reasons, agencies may opt out at a later stage from using part or all of the shared services.
    4) Country-related limitations in the use of specific technologies/solutions.
g) Statement of Business Requirements should be gathered with consultation with the business owners at the agency level.
h) Analysis of Solutions/Scenarios :
    1) This will differ from one situation to another depending on the business needs.
    2) For each of the solutions, benefits and cost saving will need to be assessed and reported.
    3) All applicable options should be included into a comparative review matrix (technical, cost, impact, staffing, initial investment, recurrent costs etc…) with the recommended choices.
i) Sustainability Plan: Long run sustainability will need to be demonstrated by the UN ICTWG prior to any investment towards Delivering as One project(s), and more details are provided in the chapter below.

A number of sample Business Cases are available from the DaO countries, and can be taken from the UNDG website (http://www.undg.org).

3.2 Assessment of Sustainability Issues

The cost and management issues around any shared ICT Service developed or deployed through Delivering as One ICT projects must be analyzed and considered. Deploying ICT services and business solutions often results in significant on-going costs, with fixed and variable elements. The on-going costs will be shared by the participating agencies on pro-rata basis (effective number of users for the proposed services which may differ from the number of staff for a given agency) and validated by the participating agency before enrolment.

This initial investment and the on-going costs must be amortized through demonstrated returns enabled by the ICT services and business solutions, over a business cycle to be agreed upon by participating agencies. Such an analysis must use a Return on Investment model to ensure that management, operating and maintenance costs are factored in.

Among the key sustainability factors that must be considered are these:

a) Maintenance and operational costs: costs of internal staff, vendor support costs, equipment replacement costs in case of breakdown, equipment replacement costs at end of life, annual license costs, etc…
b) Cost-sharing mechanism: a clear mechanism for cost-recovery and sharing must be setup for shared services.
c) Support structure: the support structure is defined in section 5 below. The support structure strategy may take one of the forms below and as endorsed by the UNCT including inter alia but not limited to:
    - Support through a service agency
    - Outsourcing support (Common tendering for support services through a designated coordinating agency)
    - Shared local service center (UN staff)
d) Exit strategy - an exit or opt-out strategy needs to be agreed to accommodate cases where agencies opt out of the shared services once these have been deployed, together with its impact on the sustainability of the solution. Opt-out options will need to adapt to convenience and non-performance.

3.3 Leveraging Business and ICT RG

The ICTWG can leverage local financial expertise e.g. from the local UN finance staff to validate the financial calculations of the Business Case. Concerned agencies may request, at their discretion, the validation of the business case at other levels.

The ICT RG can be contacted if there are questions about consistency with other approaches and consistency with interagency corporate policies and standards.

3.4 Gaining UNCT Approval for Business Case

The ICTWG circulates the Business Case to be endorsed by the ICT Reference Group before submission at the local level. Once endorsed by the ICT RG, the ICTWG needs to circulate the Business Case to the OMT/UNCT for review and endorsement before any investment or implementation are done. A presentation highlighting the major items in the Business Case needs to be made to ensure that the ICT project will be thoroughly discussed within the UNCT. This will also ensure that any eventual

investments and course of action have the full knowledge, buy-in and support of the entire UNCT and the agencies community.

3.5 Funding ICT DoA projects

The ICT projects of Delivering as One countries have been funded as one-time investments sourced from change management funds available to the Resident Coordinator's Office (RCO). Other sources of funding may be investigated, including direct donor funding or multilateral donations. Agency Headquarters typically have no funds allocated for Delivering as One ICT projects, as these are country-level initiatives, but this can be investigated by individual agencies as a part of the project.

4 Implementing Delivering as One ICT Projects

This section describes the high-level recommendations for implementing Delivering as One ICT projects. There are no hard and fast rules for implementing inter-agency projects. However, best practice recommends that a project-based approach be used. Project implementation should not begin until financial commitment and approval is given, as described in the above sections.

4.1 Identifying the Project Manager

The project manager (PM) may be chosen for their experience in managing projects, from

- the service agency,
- a different agency
- an external institution.

The PM has the overall responsibility to organize, implement and complete the project, ensuring that the business and technical goals of the project are met upon completion.

Depending on the size of the project and on whether the PM is selected from a UN agency, she/he will typically need to give up some of her/his normal duties. It is recommended that the PM's position is partially or fully funded (external PM) by the ICT project during project implementation.

4.2 Project Methodology and Project Plan.

The PM is responsible for creating the project plan in consultation with the ICTWG. The project needs to be managed using either PRINCE2 or PMBOK project methodologies.

4.3 Project Governance

OMT and UNCT should be represented on the project board according to the specific project methodology.

Project funds received by the project service agency needs to be accounted for at regular intervals to the UNCT and through internal/external auditing. At the closure of the project, project financials need to be formally reported upon by the project manager to the project board. A thorough evaluation, by the project board, of the overall project, will be undertaken to ascertain that the project goals and deliverables have been achieved to the full satisfaction of the beneficiaries. This constitutes the official closure and handover of the project.

4.4 Gaining Commitment

UNCT agencies participating directly in the ICT project will need to make time and resource commitments to ensure project success. The project should only start when validation at all levels described above is done and the funds for the project have been secured from agencies or external source of funds as described in Section 3.4

4.5 Technical Guidance

Inter-agency technical projects are often diverse, complex or require new technologies. In most cases, country-level ICT resources may need assistance in preparing technical designs or assessing feasibility of new services. The technical guidelines section of this document (Section 6), outlines recommendations needed to make design decisions with respect to ICT infrastructures and services at country-level. Some guidelines are in the nature of general principles and would need to be analyzed and applied on a case-to-case basis. Other guidelines are more prescriptive, as they reflect practical rules that need to be configured in shared infrastructures.

It should nevertheless be acknowledged that while similarities may occur across different projects, these remain unique to the existing setup at the country level and their design should reflect this specificity.

Going beyond written guidance, the ICT RG can facilitate identification of resources that can provide detailed technical guidance. The required assessment can take place remotely or through missions and ensures that inter-agency technical designs have the benefit of knowledge from senior ICT staff typically supporting global environments.

5 Supporting Shared ICT services and business solutions

Delivering as One ICT projects result in the deployment of shared ICT services and business solutions. It is important that sustainability issues are considered and planned for before project implementation. (See Section on sustainability issues)

The service management model and financial model are two key elements that need to be identified when planning for service operation. This will answer questions such as who is going to manage the services after they are implemented and how are the services going to be funded.

5.1 Defining the Service Catalogue

The ICTWG and project manager will need to decide together on the best way to manage any services deployed by the DoA ICT project. The United Nations has adopted the IT Infrastructure Library (ITIL) as the standard for service management. The points set out here apply ITIL concepts as the framework for recommendations.

It is highly recommended that the ICT project deliver an Inter-agency Service Catalogue for all services identified and deployed by the project. A Service Catalogue is a document describing in business terms a description of services being delivered, their benefits, expected levels of services and costs.

A sample Inter-agency Service Catalogue under development for the pilots is shown in Annex C. The Inter-agency Service Catalogue should be distributed and presented to the UNCT and other potential service customers.

The Inter-agency Service Catalogue needs to be owned and sponsored by the UNCT under the stewardship of the ICTWG, as any changes to it will likely involve changes to existing services already agreed through inter-agency decision making framework.

5.2 Defining the Service Management Model

ICT services and business solutions require proper on-going maintenance and support in order to deliver the expected benefits.

To this end, DoA ICT projects need to define how the ICT services and business solutions are going to be maintained and operated once the initial development project is over. Properly run services typically have well identified and equipped service managers to operate the service. The service manager must be

chosen to clearly identify accountabilities and bring the service development process forward. Annex D shows sample terms of reference for the service manager.

Choosing the appropriate service management model is a task for the ICTWG. The selected service management model will need to be presented, discussed and endorsed by the UNCT as part of the business case, as this will carry with it customer, resource and financial commitments needed to operate the inter-agency shared services.

The ICTWG should discuss the options for service management (detailed below) with UNCT and together make the final decision.

5.2.1 The Service Agency Model

The Service Agency model identifies an agency to operate one or more shared services setup by the DoA ICT project. Management arrangement including cost associated with operating the service will have to be agreed upon between the UNCT and the Service Agency, which may include the development of a new MoU. The criteria for the choice of the Service Agency are defined in Business Case Section above.

The advantages of the Service Agency model are:

a) Easy to set up
b) Potential for reduced management overhead
c) Can use existing agency financial mechanisms for cost-recovery
d) Can leverage agency resources for service peak/surge capacity needs
e) Build up on an existing infrastructure if possible (multiple agency service provider given existing capacity and expertise)
f) Potential for Long Term service delivery and sustainability

The Risks are:

a) Staff assigned to manage the service may prioritize agency-specific duties over shared service tasks
b) Changes in Agency presence and capacity may dilute the ability to deliver service

The selection of the Service Agencies should be done using the following criteria:

a) Agency with significant country-level ICT presence and/or expertise. Agencies may elect to adapt their ICT presence based on project needs;
b) Agency with significant level of services and infrastructure;
c) Agency with significant volume of operations and inherent lead role;
d) Agency having full support of local country representative to Delivering as One goals;
e) Agency able to dedicate a portion of its ICT resources (bearing in mind a) above) to support the Delivering as One project.

5.2.2 Common Operations Service Centre (SC) Model

The Common Operations Service Centre model creates a new inter-agency unit at country-level to take responsibility to operate one or more shared services setup by the Delivering as One project. The shared services are managed by the SC staff, which may be composed of inter-agency staff on rotation from UNCT agencies, or by local service contractors. Charge backs and cost-recoveries are carried out by the service centre, which imposes only the necessary expenses required to operate the service.

The designated coordinating agency implementing the project will propose an operational model where the following is defined:

a) The rotation / affectation of the inter-agency staff for the common services
b) The charging model for the participating agencies
c) The financial impact of the charging model on the actual salaries

The advantages of the SC model are:

a) Managing, Support and delivery of services is well identified and is independent of any single agency
b) Potential for enhanced collaboration among the technical support team
c) Consolidated view of service provision in country

The Risks are:

a) Unfamiliar approach at country level
b) Agency resistance to this approach and Policy restrictions
c) Accountability framework not in place
d) Undefined Linkage with the existing regional/global service centres of individual agencies
e) May incur higher resource overhead
f) Additional facilities and working space required

5.2.3 Outsourcing

The ICTWG can recommend to the OMT/UNCT the option to outsource to a third party the provision of selected ICT services and business solutions, if this capacity is available in the private sector at the local level. The third party can take the responsibility to setup the overall project and operate/manage one or more shared services.

The advantages of the outsourced model are:

a) On-demand capacity for delivering the services;
b) Economies of scale;
c) Availability of the necessary skillset regardless of the technologies involved;
d) Clearer costing model.

The Risks are:

a) Third party access to UN sensitive information and networks
b) May Incur higher expenses to operate the service
c) Lack of third party local capacity to manage such projects
d) Weak governance which could lead to decrease in quality of service
e) Agencies IT policies and standards may not be met

5.3 Defining the UN Service Agreement

The Inter-agency Service Catalogue is the basis for making an Inter-agency UN Service Agreement (UN SA) between service manager and the UNCT. The UN SA should contain all the services mentioned in the Service Catalogue. It is the basic written agreement between the service manager (whether Service Agency or Service Centre) and its clients – the UNCT and RC Office – defining the key service targets and responsibilities for both parties. The production of the UN SA and its endorsement by all participating agencies should occur before the final agreement on the common services.

The UN SA contains the following key elements:

a) Title, description, signatories and effective date of the agreement

b) Service conditions, support conditions, responsibilities of both Customer and Provider
c) Service hours, availability, reliability and performance conditions
d) Change requests and service continuity conditions
e) Charging and cost-recovery conditions, including details of charging formulas
f) Opt-in, Exit, opt-out and termination periods and options for participation in common ICT Services must be clearly defined to ensure maximum service and cost benefit for all involved in the common service.

Annex E shows a skeleton UN SA template taken from the ITIL standard, which may serve to provide substantive service information to existing memorandum of agreement formats currently in use.

The UN SA is drafted by the service manager (or project manager) and agreed within the ICTWG. It is explained and presented to the UNCT. The UNCT needs to review the agreement, and once approved, sign the agreement and carry out its side of the responsibility matrix.

5.4 Defining the Financial Model

The establishment of shared ICT services and business solutions at country level require a re-thinking of how such initiatives are going to be funded. While this is an area changing frequently, a proposal for items to consider is found in Annex F.

5.5 Service Management Board best practice

A service management board needs to be established to oversee the quality and composition of services provided through whichever chosen service management model.

Best practice recommends that, at the minimum, the service management board be composed of a service provider, customer and executive-level representatives. In the context of U.N. country operations, these are the service manager, business-level agency representatives and a representative from the RCO. In the interest of transparency and a balanced representation, the service management board cannot be uniquely composed of representatives from the same agency. The service management board recommendations are submitted to the UNCT for final decision regarding any changes to the shared services.

6 Technical Guidelines

6.1 Guiding Principles

1. light footprint by:
    a. leveraging corporate cloud solutions
    b. using outsourced services where available
    c. building sustainable infrastructure at the country office where no other option available
2. optimize connectivity, capacity and availibility
3. Support mobility
4. Wherever possible implement Green IT
5. Ensure Business Continuity and Disaster Recovery
6. Ensure compliance and consider streamlining of ICT Security
7. Use corporate federated authentication to support collaboration
8. Ensure cost effective communication

6.2 Reference architectures

Three broad architecture models (see Annex I) should be considered depending on business requirements and agency location.

Reference Architecture A: assumes integrated services in common premises and cloud based business solutions;

Reference Architecture B: assumes no common premises, no shared infrastructure and cloud based business solutions;

Reference Architecture C: assumes no common premises, some shared infrastructure and cloud based business solutions.

Consistent with the way business services are developing within participating agencies, (i.e. cloud based solutions) and guiding principles (6.1), reference architectures A and B are preferred over C.

6.3 Green IT Recommendations

6.3.1 Objectives

As an enabler of Green Business, Green IT has these objectives:

a) Facilitate the reduction of corporate travel
b) Enable tele-commuting
c) Improve, monitor and manage ICT power efficiency

6.3.2 Scope

The scope of Green IT has three dimensions:

a) IT Design
   - Increase power efficiency and handling
   - Design for the environment
   - Minimize infrastructure footprint (centralized hosting, cloud services, virtualization)
   - Reliable conferencing services
b) IT Operations
   - Manage IT energy usage, in the data centre and beyond
   - Implement green sourcing criteria (procurement)
c) Disposal
   - Recycle consumables and systems at end-of-life

These guidelines are meant as general recommendations. The ICTWG will need to discuss the best practice recommendations and use these to build their own action plan, ensuring that it is in line with Green Business initiatives.

Some of the quick wins for Green IT that can be adopted immediately are:

a) Enable power management on PCs and peripherals.
b) Use centralized multi-function printers with follow-me capability, with recycled paper and print double-sided.
c) Review recycling of consumables and durables.

6.3.3 Four Steps to Creating the Green IT Action Plan

a) Identify and prioritize goals

b) Assess your current situation
c) Find and execute some quick wins
d) Craft and communicate an action plan

The Green IT Action Plan should reflect your recognition that:

- IT assets outside the data center use (and waste) at least as much energy as those inside.
- Process, policy, and people are at least as important as technology architecture.

It should address 4 priorities:

- Revising processes and metrics.
- Optimizing existing assets.
- Revamping architecture and infrastructure considering centralized hosting, cloud services, and virtualization.

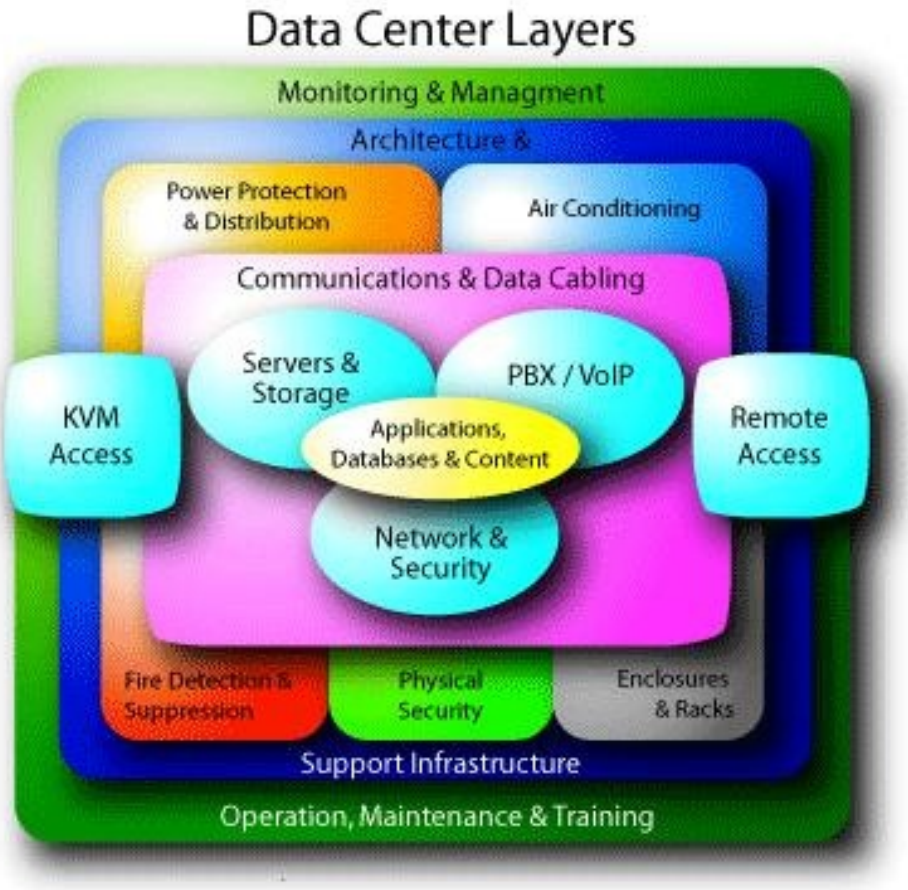
6.4 Data Centre Architecture

Three scenarios for datacenter architecture are foreseen:

1) single datacenter in common premises
2) multiple agencies non interconnected with own datacenter (common services via the cloud)
3) single datacenter with offices interconnected

We should be aiming towards the reduction of data centre services in favour of cloud and outsourced services. It It is important that a standardized design and “blueprint” be created that addresses related concerns and optimizes the economics of the data center. The data centre will include the common rack with shared “DaO”ICT infrastructure and agency specific rack space if needed.

The diagram below outlines the three fundamental layers of a Data Centre. This document intends to primarily provide guidance to One-UN and other UN common premise offices on the Architecture and Support Infrastructure layer which includes power, cooling, fire detection, security, and racks (as described in Annex G).



In the One-UN environment, centralized system hosting at corporate levels and cloud based solutions should be considered whenever possible. Locally, a centralized data-centre is advocated where feasible (and agencies are interconnected), as this ensures optimal economies of scale by minimizing infrastructure and support costs for all participating agencies. In order for disparate systems to function in a shared environment, it is important that certain basic standards are agreed and adhered to. Namely:

1. All equipment should be rack mountable
2. Data wiring labeling and device labeling should be standardized and implemented
3. Support responsibilities and accessibility to data centre facilities should be predefined and agreed
4. Critical data-centre components should be fault-tolerant
5. Agency network connectivity to data centre should be redundant
6. Green IT best practices should be implemented (Section 6.1)
7. Servers virtualized where possible

6.5 IT Security Architecture in Delivering as One

The rapid proliferation of network attacks in an ever-changing IT environment dictates a need for a change in network security postures. This has become increasingly evident in most network settings, which are designed to protect against directly formulated attacks and viruses, by utilizing a firewall and antivirus software.

The proposed guideline takes various aspects of the network, such as hardware, software, policies, and external expertise, and makes them active players and synergistic elements in the implementation

strategy. The full set of recommendations can be found in the LAN/WAN network architecture sections. The high-level principles are reproduced below.

6.5.1 IT Security Architecture Principles

IT Security is essential for safeguarding agency information and infrastructure, and for maintaining privacy and confidentiality of information and is not an option. Establishing common ICT services and interconnecting agencies' networks will require protecting all Information Systems connected to any agency network from intrusion, disruption, or exposure through malicious or accidental action using electronic means and caused by the common network components.

To ensure maximum security and effectiveness across all networked services, the security guidelines are based on the following key principles:

1) Protecting the edge to all agency networks against external security threats by:
    a. Minimizing the number of external access points to internal networks;
    b. Securing all access points by perimeter security systems and access controls;
    c. Securing internal network segments, which traverse external networks to at least the level of security provided by IPSec Secure Virtual Private Networking.
    d. Using firewalls to secure all agency-controlled devices, which connect to external networks in order to access the common network or shared components;
    e. Scanning the content of all network traffic entering or leaving internal networks for malware.
2) Protecting shared network resources:
    a. Servers and reverse proxies used to provide services accessible outside agency internal networks must be isolated to a Demilitarized Zone (DMZ).
    b. Scanning the content of all network traffic entering or leaving the shared network for malware.
3) Protecting Agency's own internal networks:
    a. Maintaining a current internal network security risk assessment and management plan in accordance to the agency's own policies and guidelines;
    b. Implementing security risk mitigation measures to address all identified high risk security threats;
    c. Implementing malware detection and removal software on all workstations and servers except where the internal security risk assessment indicates low security risk;
    d. Ensuring all security-critical patches for workstation and server operating systems, and security systems such as firewalls are installed in a timeframe consistent with the level of security risk.
4) Shared network security management and monitoring

The service agency or other entity agreed upon by represented agencies will maintain shared network security and demonstrate full conformance with industry best practices for the shared applications and services.

6.6 Network Architecture in Delivering as One

6.6.1 DaO Network requirements scenarios

The network solution for supporting a DaO site, will depend to a great extent on the physical layout of the agencies, their size and locations, based on the pilot locations experience, the following DaO premises scenarios can be expected:

a) One UN House, no separation between agencies (Reference architecture A): Programme and operations groups will formed and from staff members of different agencies, each group is located in one physical common working space
b) Individual Agencies Buildings (Reference Architectures B and C): Each agency occupies a separate building, in a DoA case, the building might be in one campus or compound, or they could be distributed within the city.

6.6.2 High Level Requirements to consider

A DAO site has the following potential requirements for its network:

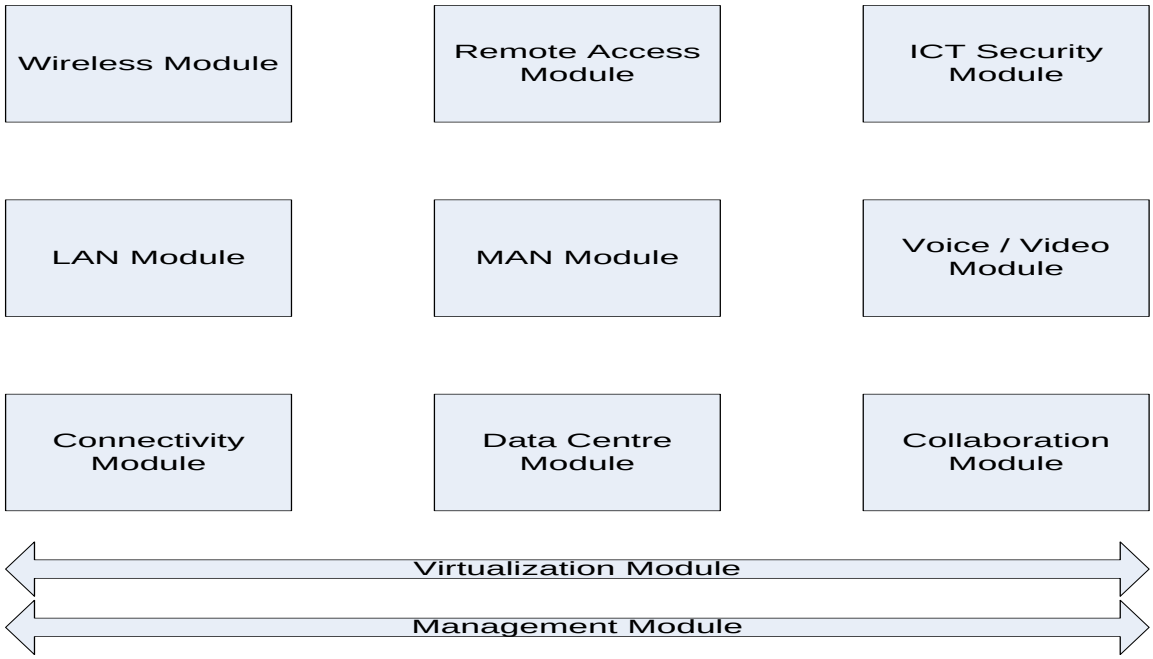
- Facilitate information sharing between users from different agencies, allowing programmatic and operational groups of the DaO site to work together and produce results effectively
- Provide network access to users that may be located in one building or distributed in multiple buildings. These users can use desktop PCs and mobile devices to access the network.
- Achieve separation of agencies' networks and isolation of each agency network traffic from other agencies, while allowing sharing of information and network resources
- Ensure that security standards of each agency are maintained within a DaO network, traffic between agencies should only be allowed through agencies own firewalls
- Enable mobility of DaO staff from different agencies, allowing network access to ICT services from any agency or location
- Provide network access to common devices like printers, photocopiers, badging systems, video surveillance systems, etc.
- Allow good quality video conferencing/web conferencing with HQ and remote locations of each agency
- Provide secure wireless connectivity to both UN employees and guests
- Provide secure remote access to employees working in the DaO site
- Support IP telephony and Voice over IP for the whole DaO site, while offering a good quality of service
- Enables reliable access to centralized and other cloud based services
- Ensure high availability of the network, given the number of supported users in a DaO site and the criticality of agencies business applications e.g. ERP
- Support implementation of end to end Quality of Service scheme across the network
- The network must be simple to manage, by a small team. Detecting, isolating and fixing faults must be easy and quick to ensure a short Mean Time to Repair (MTTR)
- Provide remote monitoring and operational support capability

6.6.3 Architecture and design concepts

In order to develop ICT standards for DaO sites which can be implemented in the different physical or business scenarios, the ICT infrastructure in broken into different modules, depending on each site requirements, some or all of these modules can be selected and used in building the ICT infrastructure for that site.

The modules could be either physical or virtual, they could be physically located within the DaO site, city, country or even in a remote location.

The following diagram demonstrates the possible ICT infrastructure modules for DaO sites



6.6.4 Metropolitan Area Network (Reference Architecture C)

The MAN is a potential option in implementing a common network in geographically separated DaO sites, the MAN inter-connects separate UN agencies' LANs that are geographically separated within the same city, it interconnects multiple infrastructure modules between agencies.

MAN Requirements

The key requirements for the MAN access module of DaO sites are:

- Security - A layer of firewall(s) must separate the site from the MAN
- High Availability - this translates in requirements for the MAN access links, the firewalls, which may be clustered, and the switching infrastructure
- Performance - The links should be able to sustain a high level of traffic, Differentiated traffic, both real-time and critical traffic, keep latency to a minimum.

Assumption

- MAN will carry all types of traffic including WAN, Internet and Voice
- Solution might be owned by the agencies and or provided by a network service provider.
- Wireless technology might require a license

MAN Connectivity Options

A number of connectivity options can be considered for implementing a MAN in a DaO sites:

- Fiber Optical Link: is a preferred option if feasible, reliable and cost effective due to its high performance
- Wireless Links: including WiMax and WiFi
- Leased Line: including Point to Point leased lines, MPLS, ATM, ISDN

- Public Switched: such as xDSL

6.7 WAN Connectivity in Delivering as One

The WAN interconnects various DaO agencies' LANs to remote destinations, either within each agency or outside. A number of different technologies may be used to communicate with remote destinations, including:

- Private Networks: VSAT, MPLS, Leased Lines,
- Public Networks: Internet, DSL, Cable, Satellite (VSAT)

The WAN access should provide the following functions:

- allow the site to access other agency sites via their WAN link(s)
- allow users and visitors of the site to access the Internet via a local internet access line
- allow people outside the DaO site to access web servers hosted in the site
- allow DaO users to remotely access the office via remote access service (e.g. SSL VPN or IPSec VPN)

Special consideration must be given to the following areas when planning the shared WAN connectivity for DaO sites

a) Security is an important aspect of the design, refer to section on IT Security Architecture for guidance.
b) High availability and redundancy are key requirements for the DaO sites, given the number of agencies supported by this module and the mission critical applications they use such as ERP systems
c) Performance optimization is an important function, given that “bandwidth” may be limited for cost reasons. This can be addressed at two levels, the Private WAN Class of Service (defined on VSAT or MPLS service routers), and can be complemented with agency specific Quality of Service (QoS) technology

6.7.1 Connectivity Options

6.7.1.1 Private Terrestrial Connectivity

This should be considered as an option for DaO offices, where feasible, reliable and cost effective, for the following reasons:

- Offers secure and private connectivity for each agency
- Ensures guaranteed predictable performance of each agency critical applications
- Has a lower latency than VSAT private connections, provided that Telecommunications backbones of the country are over optical fiber cables

A number of options can be considered for terrestrial connectivity these can be summarized as follows

a) Private MPLS Service:
Implementing MPLS service for shared private connectivity for agencies in a DaO site requires having a connection to the provider's MPLS cloud at the agency headquarters. There could be a situation where some agencies have established MPLS service with a global provider and can easily implement the service at their DaO offices, while other agencies may decide to use the Public Internet instead for their corporate applications.

b) International Private Leased Lines:
In some locations, IPLC may be a cost effective option, offering similar features as MPLS

6.7.1.2 Private IP VSAT

Private connectivity is a requirement for a number of UN agencies, Private IP VSAT should be considered where terrestrial connectivity is not reliable or cost effective, similar to private terrestrial connectivity, Private VSAT offers a guaranteed performance with established SLA for each agency. UN VSAT providers have a shared UN VSAT design, which offers the following features:

- Private path for each agency
- Guaranteed capacity per agency
- Ability to burst to higher capacity if not used by other agencies
- End to end quality of service for each agency's applications

6.7.1.3 Shared Internet Access

Offices should consider implementing a high availability shared Internet connection, by sharing higher bandwidth, agencies can burst to higher bandwidth than in can of individual lower bandwidth connections.

When sharing an Internet link the following features should be implemented:

- Guaranteed bandwidth per agency according to the number of staff
- Capability for each agency to burst to the full capacity of the connection if this capacity is not used by other agencies
- High availability, by implementing redundant Internet links, e.g. ADSL or SDSL backup link

Two options can be considered by the ICTWG:

- Local Internet Service Providers, this should be a preferred option especially if the international backbone of the provider is over optical fiber
- Low cost Internet VSAT: This can be considered if no reliable local ISP can be identified, special attention should be given to contention ratios, possibility of private bandwidth pools.

6.7.1.4 Redundant Connectivity

High availability of connectivity becomes a more critical requirement due to the consolidation of agencies' links into one or two shared connections. The redundant connectivity solution must satisfy the following requirements:

- Allow for allocating a guaranteed bandwidth for each agency, this allocation should be equal to each agency's primary connection bandwidth if possible and cost effective, otherwise it should at least be sufficient to support critical applications of the agency (e.g. ERP system and Email)
- Automatic fail-over in case of failure of the primary connection or load balancing
- Should usually be lower in cost than the primary connection
- Should result higher availability SLA with primary link provider (if possible)
- Can be used for off-loading Internet traffic from the primary link if possible

6.7.1.5 Backup Connectivity Options

A number of Backup Connectivity options can be considered in DaO sites depending on the availability of data communication services in the country:

a) MPLS Secondary Connection (High Availability Service)
b) Private IP VSAT Redundant Connection
c) Local ISP Connection
d) Internet VSAT

It is recommended that the backup connectivity not be dependent on any of the primary connectivity routes to avoid single-point-of-failure.

Considerations for selecting the appropriate backup connectivity option and features of these options are discussed.

7 Business Solutions

Business solutions in the ICT RG context are defined as information systems supporting DaO operations, collaboration spaces, public information portals/web sites.

The scope of these business solutions should not overlap with agency corporate systems (e.g.: ERP, travel, etc).

Discussions with the relevant local groups should take place to define which business solutions are required. Business solutions input could come from the following functional areas:

- Communication Working Group (CWG)
- HR
- Finance
- Common premises
- Admin services
- Procurement

7.1 Enabling access to business solutions

Federated Authentication is essential to access common business solutions. The recommended approach is for agencies HQs to adopt for the common Federated Authentication System.

Annex A: ICT Reference Group Terms of Reference (2014)

I. Background

1. Many organizations of the UN system maintain offices in locations away from their headquarters facilities, and utilize a variety of information and communication technology-based services to integrate these locations into their global operating environment. These remote offices play a particularly critical operational role for the development-oriented organizations, although almost all UN agencies, funds and programmes now maintain remote offices.

2. The UN Development Group (UNDG), an inter-agency body responsible for delivering coherent, effective and efficient support to countries seeking to attain internationally agreed development goals, including the Millennium Development Goals, provides overall coordination for operations at the country level. In the past, the UNDG has provided oversight for country-level ICT coordination through the ICT Working Group, which subsequently became the ICT Tasking Team. In late 2010, the UNDG reviewed its working methods and, as a result, moved from five standing Working Groups to two Working Groups and two Networks focused on critical elements of the UNDG strategic priorities: i) Resident Coordinator and leadership issues; ii) Crisis and transition issues; iii) Programming issues, with particular focus on the UNDAF roll-outs; and, iv) Joint funding and business operations issues with a particular focus on driving forward the implementation of an HLCM-UNDG plan for enhancing the harmonization of business practices at the country level.

3. The implementation of this new working method within UNDG created a void in coordinating ICT-related matters at the country level, which is essential in order to further support the development of the Delivering as One approach for inter-agency country operations, which has highlighted the need for agencies to work together, including joint facilities for delivery of support services like ICT. In addition, while the ICT Network of the Chief Executives Board for Coordination (CEB) works towards harmonization of ICT of UN agencies, no specific operational and technical group existed to address the unique issues related to ICT coordination faced by agencies in country offices.

4. A body, the Inter-Agency Country-Office Technology Advisory Group (ICOTAG), was created under the ICT Network to bridge this support gap and serve as reference point and provide coordination for ICT activities at the country level that benefit member agencies. The UNDG subsequently recreated specialist groups, including the ICT Reference Group, to support ICT coherence in the field. The ICOTAG assumed this role and aligned its name with the UNDG.

II. Objective

5. The Group advises on the coordination of country-level ICT activities of UN agencies where a harmonized approach can provide results and benefit the work programme of country offices while advancing the broad objectives of Delivering as One.

6. The Group identifies common areas of interest, prioritizes objectives, identifies resources, and oversees the development of the agreements, standards, guidelines and support arrangements toward harmonizing ICT activities in country offices, and ensures these activities align with common ICT strategic goals for participating organizations.

III. Activities

7. The Group performs functions in the following broad areas:

ICT Reference Group

a. In conjunction with relevant ICT Network and UNDG groups, establish inter-agency country office ICT standards that can be adopted by member agencies and that provide improvements in ICT services including, inter alia, in the areas of business solutions, Green IT, ICT Security and infrastructure.

b. Provide guidance on ICT investment, including appropriate cost-benefit analysis such as RoI and on mechanisms to address country-level common ICT service needs, and identify opportunities for synergies, harmonization and consolidation in the areas of, inter alia, business solutions, infrastructure, customer support, procurement and ICT Security.

c. Reviews all Group-initiated documentation (guidelines, mission reports, etc.) prior to distribution beyond the Group.

d. Promote the implementation and management of Delivering as One components as they relate to ICT as outlined in the standard operating procedures and ensure appropriate alignment with other working groups.

e. Respond or escalate to the ICT Network, and its sub-bodies, and the UNDG, any other country-level ICT issue.

f. Formulate and provide related trainings on ICT harmonization in interagency training forums.

IV. Membership, Appointments & Responsibilities

Membership

8. The Group is open to all agencies that participate in the CEB ICT Network. Agencies with a substantial field presence are encouraged to actively participate. Annex I contains the current membership.

9. The CEB Senior Advisor on Information Management Policy Coordinator (or the appropriate inter-agency ICT advisor from the CEB) shall participate ex-officio in the Group and provide a system-wide ICT perspective to the discussions.

10. A representative of the UNDG Development Operations Coordination Office shall participate ex-officio in the Group and provide a broad business requirements perspective to the discussions.

Appointments

11. Agencies shall nominate representatives to the Group based on their responsibility for supporting country-office ICT operations. Agencies may appoint up to three participants. Representatives should have experience in country-level ICT infrastructure architecture and operation and in the analysis and design of business systems.

12. The Chair of the Group shall be selected by its members. The Chair will serve a one year term with the possibility of renewal for one additional year upon agreement of the membership.

13. The Group shall practice agency rotation in its selection of the Chair; i.e. each agency participating in the Group shall be expected to serve at least one 1-year term before any other agency is asked to assume the Chair for a subsequent turn.

Responsibilities of the Chair:

14. The Group chair performs the following actions:

a. Coordinate the organization of regular and exceptional meetings, including preparation of the draft agenda, coordination of meeting logistics, meeting record keeping and circulation and validation of meeting reports.

b. Represent the group to the ICT Network, including presenting the activities of the group as a standing item on the ICT Network meeting agenda as well as escalating issues to the ICT Network as necessary.

c. Represents the Group to the UNDG, including presenting the activities of the Group as requested.

d. The agency represented by the Chair shall arrange to provide secretariat support to the Group.

Responsibilities of the members:

15. The Group members act in an advisory capacity. Member agencies are expected to participate regularly in meetings and follow up in a satisfactory manner with any assigned and agreed-upon tasks.

16. Members will convey to the ICT governing bodies of their respective agencies any recommendations of the Group and represent their agencies to the Group in a manner commensurate with the agency's ICT governing body's instructions.

17. Members will refer to their agencies' ICT governing body any substantive matters including coordination with other agencies, NGOs, or other entities. The Group, in its advisory capacity, will not commit agencies to any activity that the agencies' governing bodies have not explicitly agreed to.

V. Interfaces

18. The Group receives direction from the CEB ICT Network for all ICT-related matters. The Group also receives direction from the UNDG DOCO on all matters of country-office business requirements and priorities. The Group provides reports to the CEB ICT Network as well as the UNDG.

19. The Group will coordinate its work with other ICT Network sub-bodies and UNDG Networks and Reference Groups as appropriate.

VI. Procedures:

20. The Group shall meet on a regular basis every other month or as called by the Chair.

21. The Group decides issues on the basis of consensus, and only votes on issues of urgency that cannot be agreed-upon through a consensus. Each agency present shall constitute one vote. Ex-officio members do not vote, but contribute to the consensus decisions.

22. A quorum shall consist of a majority of the agency membership as indicated in Annex I.

Annex I – Group Members as of March 2014

- United Nations (represented by DFS)
- WHO
- UNDP
- UNHCR
- UNICEF
- UNFPA
- WFP
- UN Women
- FAO
- UNESCO

Annex B: Sample Information for Joint ICT Assessments

UN ICT staff (Example)

Name	Agency	Title	Position/Grade	Location	Phone Number	E-mail
Kouadio Herve Leon	UNHCR	Telecoms Technician	GL6	Abidjan	06 69 63 95	kouadioh@unhcr.org
Aye Gustave	UNHCR	IT Assistant	GL6	Abidjan	05 01 59 85	aye@unhcr.org

ICT skills(Example)

Name	Network	PC/Servers	Telephony	VSAT	Electricity and power supply
Kouadio Herve Leon	8 years experience	Basic	06 years experience in Alcatel 04 years experience in Telrad	Two years experience with Qkon iDirect installation certificate	Solar panels
Aye Gustave	8 years experience	Basic			

UN ICT Internet/WAN Connectivity

	Main Link				
	Provider	Type of Link(Private/ Public)	Latency+ Consentration Ratio	Bandwidth	Monthly Fees ($)
UNHCR	**EMC**	**Private**	**700ms**	**256/128Kb**	**$2200**
TOTAL MONTLY COST					

	Backup Link				
	Provider	Type of Link(Private/ Public)	Latency+ Consentration Ratio	Bandwidth	Monthly Fees ($)
UNHCR	**EMC**	**Private**	**700ms**	**256/128Kb**	**$2200**
TOTAL MONTLY COST					

UN ICT equipment per Agency

Agency name	Type	Number
LAPTOP	**IBM/HP**	**06/25**
PC	**HP**	**52**
PRINTER	**HP**	**15**
SERVER	**HP**	**02**
UPS	**APC**	**54**
SWITCHES	**Dlink**	**07**
ROUTER	**Cisco**	**01**
PBX System	**TELRAD**	**01**
Firewall	**Novell border manager**	**01**
TOTAL		**164**

UN ICT Applications platforms (systems): **(e.g. e-mail servers, collaboration tools, operating systems, Office suites, antivirus, web browser, backup and archiving solutions)**

Agency	Number of Users	E-mail Server	Data Centre Power Supply	Backup Power Supply	Data Centre UPS	Other Applications	Sub-Offices	Remarks
UNHCR	**69**	**Groupwise**	**CIE**	**UPS + Generator**		**Focus MSRP Progres**	**Guiglo Tabou**	

UN ICT – Enterprise Resources Planning software (ERPs)

Agency	Number of ERP Users	ERP	Bandwidth req. per user	Online / Local	Remarks	Expansion (planned implementations – if exist)
UNHCR	**15** **10**	**MSRP** **Focus**		**Online**	**High bandwidth dependence**	

Annex C: Sample Service Catalogue Template

Service Catalogue Categories:

ICT Infrastructure Services

- Common Data Centre Service
- Local Area Network:
  - Wired LAN
  - Wireless LAN
- Metropolitan Area Network
- Web Hosting Services
- Data Backup and Recovery

ICT Security Services

- Shared Firewall management and other security elements (ref. ICT Security Guidance document)

Connectivity Services:

- WAN Services: must include
  - Shared Private MPLS services
  - Shared Private VSAT services
  - IPSec over Internet
- Shared Public Internet Access must include
  - Local ISP
  - Internet VSAT (e.g. iDirect)
- Backup Connectivity Service
  - Suggest providing features of services that includes, different path, Auto fail-over, Active/Active load share or Active/Passive, options for backup links incl. MPLS, VSAT, Internet, etc..
- Remote User Access Service

Inter Agency Collaboration Services

- SharePoint
- Web conferencing
- Common UN Directory
- Instant messaging
- Shared Video Conferencing Services

ICT Reference Group

Telephony Services

- PBX management
- Voice Services
- Fax services
- Call Accounting
- Mobile voice services

Security Communications

- Hand-Held Management
- Fleet Management
- Radio Room

Common Help Desk Service

- Technical and user support areas covered

Service Catalogue Template (Used by WHO)

Service Description

TEXT

Standard Features

TEXT

Service Level Components

- Service level Indicators

No.	Service Indicator	Description	Baseline	Standard Target	Special Target (emergency)
01					
02					
03					

- Service Level measurement

No.	Source of Information	Measurement Process	Measurement Interval
01			
02			
03			

- Service Level Reporting

No.	Report	Description	Frequency
01			
02			
03			

- Roles & Responsibilities

Role	Responsibilities
Service Manager	

- Escalation Procedures

Role	Responsibilities

Pricing

- One time Costs

Description	Units	Rate

- Monthly recurring Costs

Description	Units	Rate

- Per Agency formula

Total Cost	Total Users	Per User Cost
One time		
Recurring		
Total		

Contractual Agreements

Role	Responsibilities
Service Provider information	
Contract duration	
Disconnection terms	
SLA penalties	

Related Services or User Documents

Service/Document	URL

Service Pre-requisites

Pre-requisite	Description

Annex D: Sample Service Manager Terms of Reference

Role

To implement and maintain the service management process to the level required by Agency Customers.

Role positioning

The role must be of an appropriate level to negotiate with Customers on behalf of the Service Management unit (whether service agency or local service operations centre), and to initiate and follow through actions required to improve or maintain agreed service levels. This requires adequate seniority and/or clearly visible management support from the UNCT.

Responsibilities

- Creates and maintains a catalogue of existing services offered to inter-agencies
- Formulates, agrees and maintains an appropriate inter-agency UN SA structure for the organization, to include
    - UN SA structure (e.g. service based or customer based)
    - UN SAs within the ICT service provider agencies
- Third party supplier/contract management relationships
- Negotiates, agrees and maintains the UN SAs with Agency Customers and/or ICT service provider agencies, including those for new/developing services
- Analyses and reviews service performance against the UN SAs
- Produces regular reports on service performance and achievement to the Customer and IT service provider at an appropriate level
- Manages the service staff under his/her direct supervision
- Manages the infrastructure lifecycle for all technical components under his/her direct operational responsibility

Annex E: Skeleton UN Level Agreement

UN LEVEL AGREEMENT FOR THE ABC SERVICE

This agreement is made between.....

And .....

The agreement covers the provision and support of the ABC services which..... (brief service description).

This agreement remains valid until superseded by a revised agreement mutually endorsed by the signatories below. The agreement will be reviewed annually. Minor Changes may be recorded on the form at the end of the agreement, providing they are mutually endorsed by the two parties.

Signatories:

Name..... Position..... Date.....

Name..... Position..... Date.....

Details of previous amendments:

Service Description:

The ABC Service consists of.... (fuller description to include key business functions, deliverables and all relevant information to describe the service and its scale, impact and priority for the business).

Service Hours

A description of the hours that the Customers can expect the service to be available (e.g. 7 × 24 × 365, 08:00 to 18:00 – Monday to Friday). Special conditions for exceptions (e.g. weekends, public holidays etc).

Procedures for requesting service extensions (who to contact – normally the Service Desk – and what notice periods are required). Details of any pre-agreed maintenance or housekeeping slots, if these impact upon service hours, together with details of how any other potential outages must be negotiated and agreed – by whom and notice periods etc. Procedures for requesting permanent Changes to services hours.

Service Availability

The target Availability levels that the IT Provider will seek to deliver within the agreed service hours (normally expressed as a percentage – e.g. 99.5%).

Agreed details of how this will be measured and reported, and over what agreed period.

Reliability

The maximum number of service breaks that can be tolerated within an agreed period (may be defined as number of breaks e.g. 4 per annum, or as a mean-time-between-failure (MTBF)).

Definition of what constitutes a 'break' and how these will be monitored and recorded.

Customer Support

Details of how to contact the Service Desk, the hours it will be available, and what to do outside these hours to obtain assistance (e.g. on-call support, third-party assistance etc). May include reference to Internet/Intranet Self Help and/or Incident logging.

Call answer targets (no of rings, missed calls etc).

Targets for Incident response times (how long will it be before someone starts to assist the Customer – may include travelling time etc). Definition is needed of 'response' – a telephone call back to the Customer? Or a site visit? – as appropriate.

Targets for Incident resolution (Fix) times.

Note. Both Incident response and resolution times will be based upon whatever Incident impact/priority codes are used – details of which must be included here.

Note. In some cases, it may be appropriate to reference out to third-party contacts of UN SAs – but not as a way of diverting responsibility.

Service Performance

Details of the expected responsiveness of the IT Service (e.g. target workstation response times, details of expected service throughput on which targets are based, and any thresholds that would invalidate the targets).

Functionality (if appropriate)

Details of the number of errors of particular types that can be tolerated before the UN SA is breached. Should include Severity Levels and the reporting period.

Change Management Procedures

Brief mention of and/or reference out to the organisation's Change Management procedures that must be followed – just to re-enforce compliance. Details of any known Changes that will impact upon the agreement, if any.

IT Service Continuity

Brief mention of and/or reference out to inter-agency Business Continuity Plans, together with details of how the UN SA might be affected. Details of any specific responsibilities on both sides (e.g. data back-up, off-site storage).

Security

Brief mention of and/or reference out to any applicable Security Policy (covering issues such as password controls, security violations, unauthorized software, viruses etc). Details of any specific responsibilities on both sides (e.g. Virus Protection, Firewalls).

Printing

Details of any special conditions relating to printing or printers (e.g. print distribution details, notification of large centralised print runs or handling of any special high value stationery etc).

Charging (if applicable)

Details of any charging formulas used, or reference out to charging policy document. Details of invoicing and payment conditions etc.

Details of any financial penalties or bonuses that will be paid if service targets do not meet expectations. What will the penalties/bonuses be and how will they be calculated, agreed and collected/paid (more appropriate for third-party situations).

Service Reviews

Details of how and when the service targets will be reviewed. Details of reporting that will take place and of formal review meetings etc. Who will be involved and in what capacity.

Glossary

Explanation of any unavoidable abbreviations or terminology used, to assist Customer understanding.

Amendment Sheet

To include a record of any agreed amendments, with details of amendments, dates and signatories

Annex F: Financial Model Proposal

Executive Summary

The Delivering as One ICT projects facilitated and will continue to facilitate the sharing of information and technical infrastructure leading to a common ICT approach and provide a platform for improved collaboration and communication between agencies. Such vision cannot be supported within current agency-specific financial models. A cost-sharing financial model must be defined to assure the sustainability of the essential project goals and achieve the long-term business objectives.

Sustaining Inter-Agency ICT Services

Inter-agency ICT projects implemented through Deliver as One have been typically funded with an initial investment through pooled funds garnered by the United Nations Country Team. The initial investment builds the necessary technical infrastructure and puts in place the operational environment needed to maintain the works implemented by the project. However it does not include the running or operating cost of the shared service, which could be funded typically by the cost-savings offset from current operational expenses or charges for new services that have been established through the project.

A financial model based on agency cost-sharing is needed to enable local ICT teams to operate the infrastructure or solutions put in place by implementation project, ensuring that all the benefits of the shared services continue to be available to all participating agencies.

The financial model is developed in coordination with the United Nations Country Team and implemented by the service agency (the agency providing maintenance and operations services for the ICT services) or, if in place, a local shared service centre specifically set up to manage the shared infrastructure.

While keeping implementation and eventual operational costs to a minimum and simultaneously providing essential, highly available and high quality ICT services, three key items must be considered. These are: a treasury function for the handling of the funds, a budgeting process, including project and sustainability costs and considerations around cost recovery (as yet to be formalized) and finally methods for ICT costing itself.

These can be outlined briefly as follows:

1. Treasury Function
    a. Billing
    b. Receipts
    c. Reporting

    UNDP has developed a common services account to help facilitate cost sharing for services at the country level, though it is also not necessarily the case that the service provider manages the funds. Typically, under multi donor trust funds (MDTF) modalities, the Administrative Agency charges 1% for this service. More work needs to be done on administrative servicing and associated costs in terms of funds pass through, administration of the funds for the project and cost recovery.

2. Budgeting Process
    a. Implementation
    b. Sustainability & Maintenance (recurring operating costs)

In general, when developing budgets, it is not recommended to cost on a pay as you go basis but rather on annual or biannual costing. This reduces administrative overhead and complexity in both managing and maintaining the ICT services. It will be very difficult to maintain economies of scale in a piecemeal budgeting environment. It is strongly recommended that full commitment is made by all agencies for services and budgeted and paid on an annual or biannual basis. In addition, it is recommended that the budgeting process is clear, open and transparent about the services provider(s) full resource needs (admin support, HR support costs etc.) and that these items are included as line items in budgets. As a general principle, management costs should never be more than 7% and should preferably be less. Services must be priced based on the participation of clients in the project and opt in/opt out must occur at specific times; this is crucial for achieving critical mass, economies of scale, sustainability and business flexibility. This must all be agreed upon and signed off by the country team before starting any project. A favored approach is to budget for tightly bundled services and charge back to all. (Ask George about Atlas example.) A management framework will need to be in place for monitoring service to ensure overall quality and satisfaction with the project and it's maintenance.

3. ICT services

ICT services themselves have specific costing and maintenance implications. There is a large volume of available professional literature on this which does not need to be repeated here. However, in general, charging for ICT services follow the principles of full-cost recovery in which only the costs to manage, support and renew the services are charged to agencies and no mark-up is envisaged. In addition, it also acceptable to consider optional services (always keeping economies of scale and critical mass in mind) wherein prices are determined and paid based on usage of a whole service. In any event, direct funding is required to be shared by all to maintain the basic or foundation components of the infrastructure or solution.

Costing of services follow those defined by the IT Infrastructure Library (ITIL) standard. A total cost of ownership approach is used, taking into account these standard cost types:

- Hardware costs
- Software costs
- Staff costs
- Accommodation costs
- External service costs (costs paid to vendors)
- Transfer costs (costs from one agency or business unit to another)

For an initial sense of how the ICT costing was outlined for the pilot in Mozambique in 2008 and 2009.

MOZAMBIQUE CASE STUDY

This is an explanation of the Mozambique pilot project's financial model as a case study which can be implemented and developed to assure the continuity and sustainability of the ICT services offered. The financial model includes staffing, equipment replacement and maintenance costs.

Service Categories

Taking the Mozambique pilot as an example, shared ICT services are classified into Basic and Optional categories.

1) Basic services are those needed to maintain the basic or foundation infrastructure, and require subscription from sufficient number of agencies to maintain operational cost-efficiency. Such services are considered "standard" and as such are charged to all participating United Nations agencies. These are charged on a pro-rata basis based on the number of staff per agency.
2) Optional services are those that may rely on top of the Basic services, generally considered value-added services. These are independently subscribed by each agency, and are charged based on actual service cost.

Service Costs and Chargeback

Standard Services

Standard service costs are calculated independently, and costs apportioned following a reasonable metric. An example of how standard services are calculated and compared to commercial alternatives in the Mozambique pilot is shown in Table 1.

Table 1: Standard Service Cost Per Month

Service	UN as Provider	Commercial Provider	Agency Apportionment
UN Network	$1,500.00	$4,200.00	By number of staff
Contingency Site	$3,075.00	$20,000.00	By number of essential staff
Radio Room	$2,500.00	Not Available	By number of staff
Total	$7,075.00	$24,200.00	

Actual cost charge-back per agency is dependent on the actual number of essential and other staff that each agency has. This is calculated once a year based on the number of essential and other staff reported by each agency. The final reported staff numbers are then factored in to calculate the standard monthly charge-back for the year for each participating agency.

Optional Services

Optional services are calculated in a similar fashion. However, where services are charged, charge-back calculations depend on the capacity needs agencies require of each service. Table 2 shows a sample Optional Service Cost per Month, showing indicative commercial costs where available for comparison.

Table 2: Optional Service Cost Per Month

Service	UN as Provider	Commercial Provider	Apportionment
Inter-Agency VSAT	n/a	Inter-agency VSAT LTA rates	By bandwidth
Internet Access (ISP)	$8,682.00	$9,600.00	By bandwidth

Common Directory	$0.00	Not Available	
Data Backup	$0.00	Not Available	
Web Hosting	$0.00	$1,200.00	
Common ICT Helpdesk	$6,760.00	$12,600.00	By number of staff
Consultancy	Case-to-case	Case-to-case	

Cost Components for Standard Services

In the Mozambique pilot, the Standard services include these:

1) **UN Network Service**

This refers to the wireless telecommunications network connecting all UN agencies in the city and hub facility to host central infrastructure. Connecting to the UN Network allows agencies to access all shared solutions, take advantage of consolidated services and use shared connectivity back to agency Headquarters.

Cost Considerations

Costs are calculated to include all charges needed to support and maintain the network, and include equipment replacement, internal maintenance staff, vendor support and facilities expense. The total monthly cost is USD 1,500 in the case of Mozambique.

Sourcing Alternatives

Investigations of alternative commercial connectivity methods reveal that it will cost USD 4,200 per month to connect all agencies through a fibre-optic solution. This solution is limited by additional last-mile connectivity costs, and lack of clear vendor service availability guarantees.

2) **Radio Room Service**

This refers to the provisioning of radio room services to all United Nations radio units in the Maputo coverage area, in compliance of United Nations minimum operating security standards (MOSS).

Cost Considerations

The standard monthly recurring cost for the service is USD 2,500 which covers staff costs for operating during business hours. Base radio equipment costs and maintenance are covered by the agency having the installed radio base infrastructure and expertise, which is WFP for Mozambique. Hand sets are procured independently by agencies. Monthly operating costs go up to USD 15,000 per month in case the radio room has to be operational 24 hours 7 days a week, which is the case in higher security levels due to MOSS requirements.

Sourcing Alternatives

No commercial providers can be used, as this service can only be operated by internal UN resources due to the considerations of security and confidentiality.

3) Contingency Site Service

The service provides a backup office facility for business operations for at least 50 essential UN staff to be used in case of emergencies, in support of the UN Emergency Security Plan defined by the UN Security Management Team (SMT). The facility is equipped with all the necessary technical capabilities including VSAT and ISP connectivity and does not rely on local suppliers for these services, and is ready for emergency occupancy at any time.

Cost Considerations

Costs depend on facilities rental, basic utilities and staff. As staff costs are covered by the UN Network Service, the monthly recurring cost of this service is USD 3075, to be apportioned to agencies depending on the number of essential staff each agency has as defined in the Emergency Security Plan.

Sourcing Alternatives

This service can be provided by a commercial facility (e.g. hotel). However, even if such facilities are immediately available, they will not have the required UN infrastructure and connectivity. For comparison, the most economical option for such a commercial service in Maputo was USD 20,000 per month.

Cost Components for Optional Services

In the Mozambique pilot, these are the Optional services:

4) Internet Access Service

This provides basic Internet access services through a shared satellite-based (VSAT) ISP contract. The service is supported by vendor quality of service and availability guarantees.

Cost Considerations

Agencies are allocated bandwidth depending on individual requirements, as each agency has custom Internet access requirements per user, and varying numbers of users. For Mozambique, the total service cost per month is USD 8,682, to be shared between agencies. Specific agency cost depends on the allocated bandwidth for the agency and is directly related to the vendor's cost. As total bandwidth requirements increase, unit bandwidth charges to agencies decrease due to lower per unit cost.

Sourcing Alternatives

It will cost agencies USD 9,600 USD per month to get ISP services through local companies.

5) Inter Agency VSAT Service

This service refers to provision of corporate VSAT connectivity services from agency office to agency headquarters, and includes the last-mile connection from the VSAT point of presence (POP) of the VSAT hosting agency to the end-user agency.

Cost Considerations

In the case of Mozambique, the agencies involved take advantage of the inter-agency VSAT contract through EMC. The service cost will be as per the inter-agency VSAT contract, with each agency

planning the bandwidth as per internal needs. The cost for this service will be dealt with directly between the agency and the service provider EMC, or with the hosting agency providing VSAT POP services in case the sister agency approach is chosen by the end-user agency. The costs for last-mile connectivity between the end-user agency and POP agency are provided by the UN Network Service.

Sourcing Alternatives

Other inter-agency connectivity alternatives are possible beyond that provided by the inter-agency VSAT contract. However use of these and resultant costing will depend on the providing agency.

6) UN Common Directory Service

This provides a searchable white pages directory service for United Nations staff. This service is only available to staff members of agencies that have had their global directories shared by agency Headquarters in the common directory infrastructure.

Cost Considerations

This service is accessible via the Internet, and does not carry any country-specific cost.

Sourcing Alternatives

There are no alternatives to this service, with the exception of manually maintained local directories.

7) Data Backup Services

This service provides 1 Terabyte of data storage space apportioned in slots to each agency. The shared storage space is hosted in the shared data centre and is backed up to tape, and can be considered as an off-site information backup solution in support of agency business continuity plans.

Cost Considerations

Equipment, consumable supplies (tapes) and staff costs make up the cost components of this service. As initial equipment and consumables are covered by the implementation project and staff costs are covered by the UN Network service, there is no initial recurring monthly cost for the service per agency. However, agencies with larger backup requirements will be charged additional costs based on the cost of the backup tapes, hard drives and other equipment.

Sourcing Alternatives

There are no locally available commercial alternatives to this service that can ensure that backups are maintained in United Nations premises.

8) Web Hosting Services

The web hosting service provides web-server hosting and Internet connectivity for both internal (intranet) and external (Internet) use.

Cost Considerations

The cost components of this service include equipment, software, staff and connectivity costs. Initial equipment and software costs have been provided by the implementation project. Recurring staff and connectivity costs are supported by the UN Network and Internet Access services, respectively. Therefore, there are no envisaged recurring costs for this service for standard use. Use of web hosting facilities over and beyond the standard will incur additional costs, calculated on a case to case basis.

Sourcing Alternatives

Commercial rates and service guarantees vary for web hosting. The Mozambique UN website is charged USD 1,200 per month by a commercial provider.

9) Common ICT Helpdesk Services

This service provides end-user support for basic computing problems, including standard software issues and hardware repair.

Cost Considerations

The service cost components include the necessary support staff, their equipment and accommodation expenses. The service envisages assigning, on rotation basis, inter-agency staff to the common ICT helpdesk function, bringing with them agency equipment. Accommodation is already provided through the facilities paid by the Contingency Site Service. Direct costs amount to USD 6760 per month, assuming the service supports a population of 520 end-users each requiring on average between 1 to 2 requests or issues per month.

Sourcing Alternatives

Currently this service is costing agencies approximately USD 12,600 per month, counting salaries of 7 non-dedicated helpdesk staff. Smaller agencies without agency ICT staff lack technical support, and rely on goodwill from better staffed agencies for technical assistance on ad hoc basis. In comparison, commercial companies in Maputo charge more significant sums for technical support.

10) Consultancy Service

This service provides ad-hoc technical implementation and support services to agency ICT projects using agency staff.

Cost Considerations

Costs are charged on a case to case basis, depending on the policies of the agency providing the resources and the capacity of resources required.

Sourcing Alternatives

Technical support can also be sourced commercially, usually at higher rates than the typically transfer charges between agencies. On the other hand, commercial providers may have the industry or technical expertise required for the job that internal UN resources cannot provide.

Annex G: Data Centre Module

Location

Servers and UPS equipment for data centre's are getting denser and heavier every day. The load rating for all supporting structures, particularly for raised floors and ramps should be adequate for current and future loads. Considering the load bearing requirements, it is recommended that the data centre be located on the ground floor of the building, unless there are flooding concerns, in which case the data centre should be located on the floor immediately above flood water levels.

Most buildings are designed with data and electrical wiring runs done along the central core, as this provides protection from external elements. Furthermore, Ethernet twisted pair cables have a maximum recommended distance of 100 meters. Therefore, to reduce distances to floor wiring closets, enhance cooling, and address security concerns (e.g. theft and bombing) the optimal location of the data centre is close to the core or centre of the building.

Flooring and Wiring

As mentioned earlier, an important issue to be concerned with in the early stages of the data centre design is weight. It is important to know how much load, now and in the future will be placed on the raised floor so that a support grid and tiles with an adequate load rating can be ordered. Remember, once the raised floor is installed, it's going to stay there. Changing out a raised floor in an online data centre is a time consuming and costly job. There are three types of loads to consider:

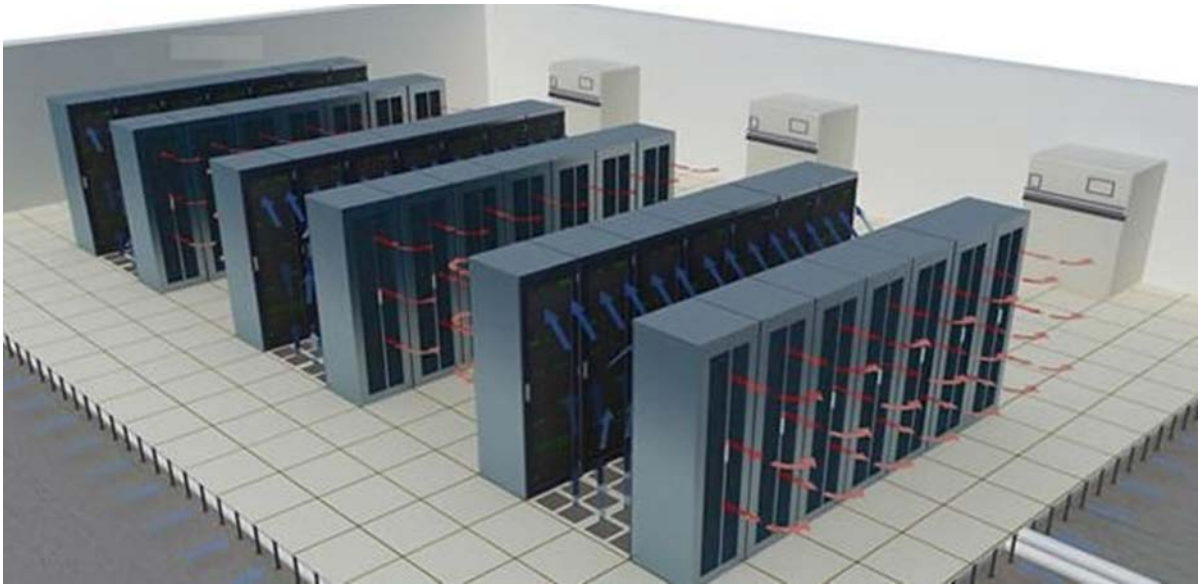
1. Point load. Most racks sit on four feet or casters. The point load is the weight of a rack on any one of these four points. For example, the maximum weight of a fully populated 42U server rack is 2000 pounds. So the load distribution is 500 pounds per caster. A floor tile must have higher than 500-pound point load, which means that for a 1-inch square area on the tile must be able to support 500 pounds on that 1-inch area without deflection of more than 2 mm.
2. Static load. Static load is the additive point loads on a tile. If you have two racks, each with a 500 pound point load, and each has one caster on a tile, this tile will have a 500 pound static load. The tile must be rated for at least a 1000 pound static load.
3. Rolling load. Rolling load should be close to static load and is usually only applicable to perforated tiles. Since it is possible that you might use your cool aisle to also serve as an aisle to move equipment, the perforated tiles will need to support the weight of two point loads of a rack as they are rolled along the aisle. If the perforated tiles cannot accommodate this load, they would have to be replaced with solid tiles every time a rack needs to be moved.

Cast aluminum tiles are strong and will handle increasing weight load requirements better than tiles made of other materials. Even the perforated and grated aluminum tiles maintain their strength and allow the passage of cold air to the machines. These tiles can handle a point load of 1,750 pounds even on a perforated grate with 55 percent air flow. The static load of the same tile is 3,450 pounds.

If at all possible, raised flooring of 12" to 18" is recommended (normally, the greater the number of racks, the higher the raised flooring should be to accommodate the additional wiring and cooling needs). Raised flooring enables all the power distribution to go under the floor, while all data cables go overhead in ladder racks. This reduces the risk of interference between power and data cables, and an electrical malfunction or fire is less likely to destroy data cables. Furthermore, floor tiles will not need to be removed whenever a new network cable is run. Cooling should also be directed through the raised flooring as it gives the opportunity to focus cold air specifically on the areas required.

Cooling

Hot aisle/cold aisle is an accepted best practice for cabinet layout within a data centre. The design uses air conditioners, fans, and raised floors as a cooling infrastructure and focuses on separation of the inlet cold air and the exhaust hot air. The racks are arranged into a series of rows, resting on a raised floor. The fronts of the racks face each other and become cold aisles, due to the front-to-back heat dissipation of most IT equipment. Air conditioners push cold air under the raised floor and through the cold aisle, Perforated raised floor tiles are placed only in the cold aisles concentrating cool air to the front of racks to get sufficient air to the server intake. As the air moves through the servers, it's heated and eventually dissipated into the hot aisle. The exhaust air is then routed back to the air handlers.



On average, 1 ton of cooling is required for each populated rack. So a data centre with 10 racks should have a 10 ton system. Rather than one 10 ton system, to ensure redundancy, three 5 ton units should be used. This way, should one unit fail (which occurs around once a year in a normal operating environment), the remaining units will provide adequate cooling for all equipment. Optimal temperature ranges are 20C to 25C (68F to 77F). Considering that AC units are difficult and expensive to install, it is recommended that cooling capacity be based not on the current number of populated racks, but on the maximum number of racks projected to occupy the data centre.

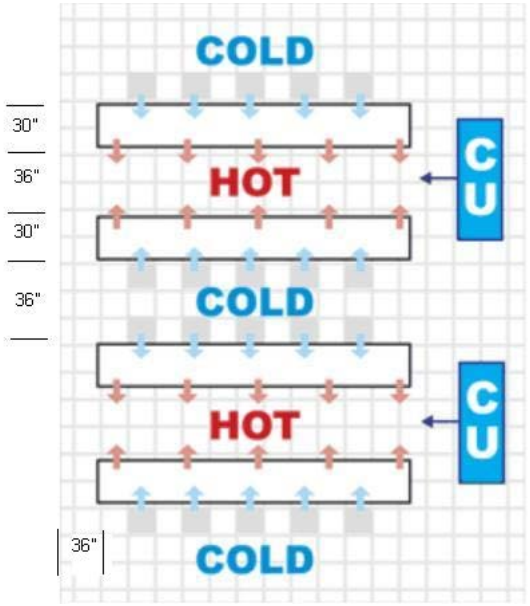
It is important that cooling units not be too powerful for the data centre, as they will have a tendency to shut off for extended periods, resulting in high levels of humidity. If a data centre room is too humid, condensation can build on computer components and cause them to short out. In addition, high humidity can cause condensation to form on the coils of a cooling unit, causing it to work harder to rid itself of the condensation, which in turn can lead to wasted cooling, also called latent cooling, and that costs money. Meanwhile, if humidity is too low, data centers can experience electrostatic discharge (ESD), which can shut down electronic equipment and possibly damage it. Optimal humidity levels are 40% to 60% and it is important that the cooling unit control both temperature and humidity. Having multiple AC units which can be switched on or off depending on the cooling and humidity requires is a good way to address these concerns.

If at all possible, the reduction and virtualization of servers will result in a number of significant advantages, with decreased cooling requirements as one of significant importance. Other advantages of virtualization are decreased power, cost, simplified application installation, and decreased space needs.

Room size

The ideal computer room size is determined by the maximum projected number of racks. The most common rack height for data centres is 42U and it is recommended that all server room racks be 42U or 78" (2 meters) tall to ensure standardization and uniformity. Considering a raised flooring of 18" and data cables in overhead ladder racks of 12", the ideal height for the server room should be 108" (9' or 2.74 meters).

The average depth of a server is 30" (76cm). Clearances of 36" (91cm) in the front, back, and sides (of the last rack) are recommended to facilitate installation, service, wiring, and cooling.



Power

Uninterruptible power supplies (UPS) should generally be installed in the bottom-most rack position. This stabilizes the rack and decreases the stress on the rack bolts and rails. The size of the UPS is dependent on the stability of the power and the availability of generators for long term power backup. If generators are available, 15 minutes backup power will suffice. If generators are not available or are unreliable, 30 minutes of backup power is recommended. On average, a 5KVA UPS per rack will provide 20 minutes of backup power. It is important to remember that larger UPS' are quite heavy and can easily weigh over 300lbs (140kg). This makes installation and replacement difficult and increases load bearing concerns. A 5KVA UPS will weigh around 200lbs or 90kg. If the number of racks exceeds 6, a central data centre UPS should be considered, as this will provide better economies. It is advantageous to have the UPS in a separate room adjacent to the data centre. UPS' do not have the same critical cooling requirements as other data centre equipment. They should not be installed on a raised floor and have inherent dangers that are best isolated from other equipment.

If incoming power is relatively stable, a UPS will be able to handle normal levels of fluctuation, but if there are frequent input voltage and load current changes, a voltage stabilizer is recommended to deliver

relatively constant output voltage. This will extend the life of the UPS and other equipment connected directly to the mains power.

Fire protection / Alarms

There must be controlled access to the data centre via security cards, biometrics or other auditable methods. Punch codes should be avoided, but if used, the codes should be changed frequently (monthly and/or whenever there is related staff turnover). Consider using security cameras within the data centre, current installation and cost make this a simple inexpensive solution.

Fire suppression systems will vary depending on local availability, and whether water or gas based, have related advantages and disadvantages. Water is the cheapest and simplest to install and maintain, but causes the most damage to computer equipment and increases the likelihood of electrical shock. For gas, Halon, a chemical suppressant, popular in the 1970s and 1980s, was banned in most countries in the late 80’s, is an ozone depleting substance and a physical hazard if staff are exposed for extended periods (10 minutes or longer). The most common waterless agent currently used is a gas called FM200. It is safe for people and it's totally benign to electronic equipment. Also, nothing can get inside and around components like a gas. The downside to FM200 is cost. It's more expensive than a sprinkler system and a little more expensive than Halon. Also, it doesn't have a totally clean environmental profile. While FM200 does not deplete the ozone, it is a greenhouse gas producer that contributes to global warming. A third system to consider for smaller data centres is a manually operated canister unit that staff can utilize in the event of an emergency. For these, a dry chemical or CO2 system is recommended. Regardless of the system, data centre managers need to have a plan in place, and should test discharge sequences, batteries, pull testing and the rest of the system.

Even more critical that a fire suppression system, are data centre alarms that monitor temperature, humidity, power, and smoke. All four are strongly recommended and should have the ability to send an alert via phone, email and pager, and provide online access to real-time reports that detail the current status of the AC system, UPS, and other items. Alerts should be sent to multiple recipients to ensure that all critical systems are covered 24/7.

Equipment Virtualization

File Server Virtualization

An effort should given to consolidating the File Servers of UN agencies in a DaO locations, implementing a shared data centre presents an opportunity for file server virtualization, for example using VMWare for Windows servers, this leads to more effective maintenance and support, lower cost of ownership and greener IT setup. One challenge for achieving this is the different server standards in agencies, although there are only two or 3 server brands currently used by most agencies and some may be more flexible in using other agencies' standards

Firewall Virtualization

Apart from the main Internet Firewall which protects the whole DaO site from the Internet threats, each agency has its own managed Firewall, consideration should be given to consolidating these Firewalls in one high availability Firewall with a virtual firewall configured for each agency. The same challenge as servers consolidation exists, same approach could also be feasible for Firewall consolidation.

Annex H: Common ICT Services MoU

MEMORANDUM OF UNDERSTANDING AMONG THE VARIOUS UNITED NATIONS ORGANIZATIONS WITH OFFICES IN THE ONE UN HOUSE _____ WITH REGARD TO COMMON INFORMATION TECHNOLOGY SUPPORT SERVICES

The various United Nations organizations listed in Annex I, herein attached, having offices in the One UN House in _____ (hereinafter the "Resident UN Organisations" and each a "Resident UN Organisation") have established a pilot for a "One UN Information Technology Support Team" ("IT Support Team") to provide integrated information technology support to the United Nations Country Team in _____ in the context of the "Delivery as One" pilot in _____;

WHEREAS, the Resident UN Organisations agree that respective staff members of the United Nations Country Team in _____ will be assigned to the IT Support Team through a separate agreement to be entered into by the assigning Resident UN Organisation and the UN Resident Co-ordinator, relating to their terms of engagement;

WHEREAS, it is now necessary to establish a framework under which the provision of common information technology support services by the IT Support Team to the Resident UN Organisations will be coordinated under the leadership of the UN Resident Co-ordinator.

NOW, THEREFORE, each of the Resident UN Organisations signatories of this Memorandum of Agreement agree as follows

Article I

Purpose

1. The One UN House _____ ICT infrastructure relies on a common framework of IT support consolidation and clustering. It is developed on the premise that ICT resources will be shared by Resident UN Organisations occupying the One UN House in _____. To achieve this goal of sharing the services of the ICT staff of the Resident UN Organisations at a functional level, the endorsement of each Resident UN Organisation and the elimination of any barriers that would impede such implementation, especially on the policy level of access to local servers and devices, is required.

2. The purpose of this Memorandum of Understanding ("Memorandum") is to provide a framework under which all Resident UN Organisations agree for the IT Support Team to access each Resident UN Organisation's information technology system in order to provide common information technology support services as set forth in Annex II ("Common IT Services") to the Resident UN Organisations.

Article II

Provision and Administration of Common IT Services

1. The UN Resident Co-ordinator, through the IT Support Team, will be responsible for the direction and administration of the Common IT Services with respect to the One UN House as set forth in Annex II of this Memorandum.

2. The UN Resident Co-ordinator will enter into separate Service Level Agreements with the Resident UN Organisations which will establish the terms and conditions of the Common IT Services to be provided by the IT Support Team; the turn-around time on each service provided; and details of each service category as well as any cost recoverable.

3. The type of service to be rendered is set forth in Annex II of this Memorandum. Subsequent services may be added as a result of periodic review as provided for in Article IV below. Such additional services will be documented, sequentially numbered, and signed by the Resident UN Organisations and attached to this Memorandum thereby forming an integral part of this Memorandum.

4. The Common IT Services will be available to the Resident UN Organisations upon signing this Memorandum, and such services will be provided equally to all Resident UN Organisations.

5. The Resident UN Organisations will ensure that requests for services are submitted as per procedure outlined in the Service Level Agreement, and that the Common ICT Services are used solely for official purposes in accordance with the Viet Nam One UN ICT Use Policy

6. The Resident UN Organisations will provide the IT Support Team with any specifications, documentation, instructions, information, data, access to servers and other user facilities or equipment reasonably required by the IT Support Team in order to perform its obligations under this Memorandum and respective Service Level Agreement.

7. The IT Support Team will provide consistent and reliable services to the Resident UN Organisations in accordance with applicable regulations, rules and policies. Approaches and solutions shall be developed and offered in consideration of the environment that the requesting Resident UN Organisations operates as well as the Resident UN Organisation's needs and IT Support Team's capabilities.

8. All services provided by the IT Support Team are for the exclusive benefit of Resident UN Organisations, including any resulting title or other property rights, unless agreed otherwise.

9. The IT Support Team will provide any information and documentation requested by the Resident UN Organisations as per Viet Nam One UN ICT Use Policy.

Article III

Periodic Review

This Memorandum is subject to review in the last quarter of every year in order to:

1. determine the need for continuation, modification or termination of the agreement;

2. review performance and performance standards to evaluate the quality and timeliness of the Common IT Services and to make any required changes in performance standards;

3. make adjustments in any of the areas covered in the terms of this Memorandum as well as the Service Level Agreement.

Article IV

Termination

1. A Resident UN Organisations may terminate the arrangements set forth in this Memorandum as they apply to it, if it intends to relocate permanently its headquarters or offices out of _____.

2. A Resident UN Organisation seeking to terminate these arrangements shall give at least one month's prior written notice of its intention to terminate the arrangements to the Resident Co-ordinator.

3. Should a Resident UN Organisation terminate this Memorandum, the Resident Co-ordinator with the assistance of the IT Support Team will assist the Resident UN Organisations with the orderly transfer of shared IT support services.

Article V

Settlement of Disputes

Any differences between Resident UN Organisations, or between a Resident UN Organisation or Resident UN Organisations and the Resident Co-ordinator, shall be resolved by means of mutual discussions.

Article IV

Final Provisions

1. Any action required or permitted to be taken under this Memorandum may be to the following:

   For IT Support Unit: UN Resident Coordinator

   For Resident UN Organisations: authorized Representative of the Resident UN Organisation in the Country or any other authorized person indicated in the Service Level Agreement.

2. Each Resident UN Organisations may enter into these arrangements by authorizing its Representative in _____ to sign below on its behalf. Upon such signature the Resident UN Organisations shall be bound by the terms of this Memorandum.

3. This Memorandum will enter into force upon signature by the authorized representatives of the Parties and will remain in full force and effect unless terminated in accordance with Article IV.

Signed: _____

for _____

Signed: _____

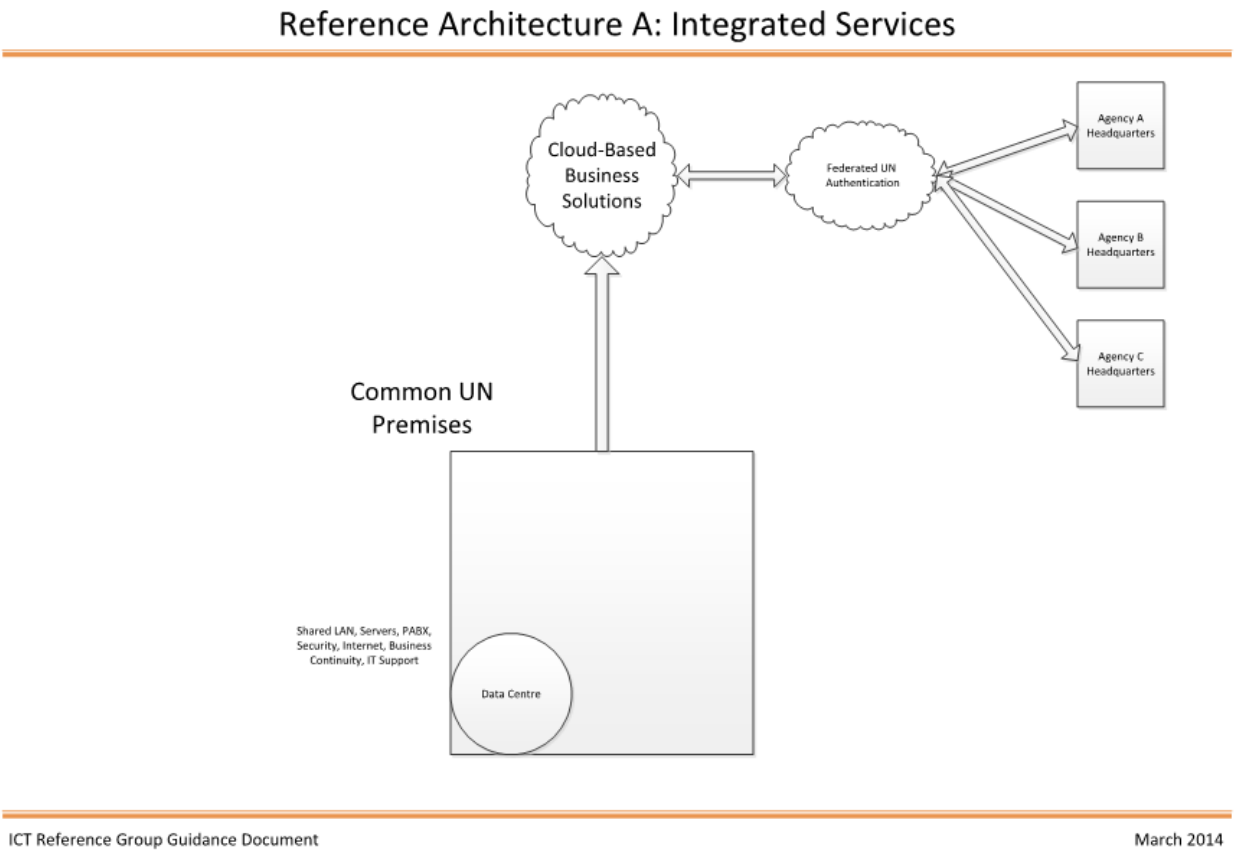
for _____

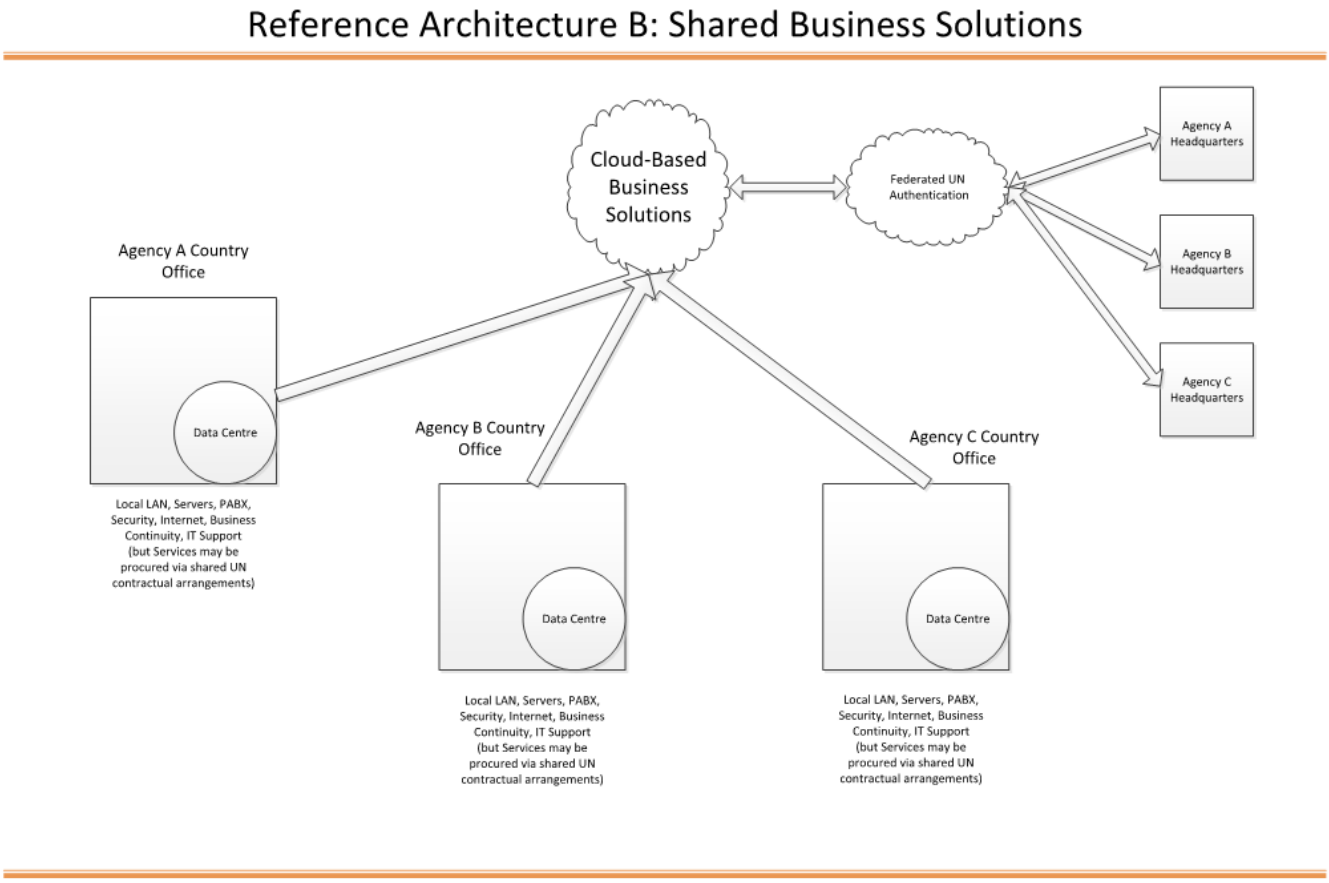
Signed: _____

for _____

Annex I: Reference Architectures

A – integrated services




Reference Architecture B: Shared Business Solutions
Cloud-Based Business Solutions
Federated UN Authentication
Agency A Headquarters
Agency B Headquarters
Agency C Headquarters
Agency A Country Office
Data Centre
Local LAN, Servers, PABX, Security, Internet, Business Continuity, IT Support (but Services may be procured via shared UN contractual arrangements)
Agency B Country Office
Data Centre
Local LAN, Servers, PABX, Security, Internet, Business Continuity, IT Support (but Services may be procured via shared UN contractual arrangements)
Agency C Country Office
Data Centre
Local LAN, Servers, PABX, Security, Internet, Business Continuity, IT Support (but Services may be procured via shared UN contractual arrangements)
ICT Reference Group Guidance Document
March 2014

C – shared business solutions with some shared network services