United Nations A/62/477

General Assembly

Distr.: General
9 October 2007

Original: English

Sixty-second session
Agenda items 128 and 140

Proposed programme budget for the biennium 2008-2009

Administrative and budgetary aspects of the financing of the United Nations peacekeeping operations

Information and communications technology security, disaster recovery and business continuity for the United Nations

Report of the Secretary-General*

Summary

The General Assembly, in section XI of its resolution 59/276 of 23 December 2004, requested the Secretary-General to provide a detailed proposal for a global operational framework for information and communications technology (ICT) security, business continuity and disaster recovery, as outlined in his report on a strengthened and unified security management system for the United Nations (A/59/365 and Corr.1 and Add.1 and Add.1/Corr.1), and to submit the results of the analysis in his report thereon to the Assembly at its sixtieth session.

In section XV of its resolution 60/266 of 30 June 2006, the General Assembly requested the Secretary-General to submit at its resumed sixty-first session a comprehensive report on the proposed establishment of and justification for mission on site, mission in theatre and off site, and off-site and out-of-theatre redundant data centres for disaster recovery and business continuity in peacekeeping missions, as well as on a secondary active communications facility and a disaster recovery and business continuity centre for information technology.

Part one of the present report provides a detailed proposal for a unified Secretariat-wide global operational framework.

* The issuance of the present report was delayed to permit extensive consultation with various departments.

Part two of the report provides details on a separate, but related initiative to move the current United Nations Headquarters complex data centres to Long Island City and a site in the new North Lawn facility.

Part three of the report summarizes the resource requirements required for the implementation of parts one and two and also outlines the requested actions by the General Assembly.

Contents

Overview

1. The General Assembly, in section XI of its resolution 59/276 of 23 December 2004, requested the Secretary-General to provide a detailed proposal for a global operational framework for information and communications technology (ICT) security, business continuity and disaster recovery as outlined in his report on a strengthened and unified security management system for the United Nations (A/59/365 and Corr.1 and Add.1 and Add.1/Corr.1). In section XV of its resolution 60/266 of 30 June 2006, the Assembly also requested the Secretary-General to submit to it at its resumed sixty-first session a comprehensive report on the proposed establishment of and justification for mission on site, mission in theatre and off site, and off-site and out-of-theatre redundant data centres for disaster recovery and business continuity in peacekeeping missions, as well as on a secondary active communications facility and a disaster recovery and business continuity centre for information technology.

2. The present report has been prepared in response to both resolutions and its three parts may be summarized as follows:

(a) Part one presents a holistic view of disaster recovery and business continuity throughout the Secretariat in response to requests made by the General Assembly in its resolutions 59/276 and 60/266. Disaster recovery and business continuity initiatives at Headquarters, the offices away from Headquarters and field missions also address the important requirement of re-enforcing initial implementations through the putting in place of two major and centralized data centres, in the United Nations Logistics Base at Brindisi, Italy, and at a proposed secondary active site (“site B”), as outlined in paragraphs 8 and 9 and section VI below;

(b) Part two provides details on a separate but related initiative on transferring the current United Nations Headquarters data centre in the Development Corporation DC2 building to a facility in Long Island City. The transitioning phase of the capital master plan calls for a heavy reliance on the DC2 data centre, a facility built in the 1980s and inadequately equipped to handle a full-time mission critical function. Details of this proposed alternative approach are presented for the review of the General Assembly;

(c) Part three summarizes the resource requirements for the implementation of parts one and two and also outlines the requested actions by the General Assembly.

3. This report focuses only on the information technology component of disaster recovery and business continuity. Other aspects of business continuity as they relate to pandemic preparedness are conducted in a separate report submitted to the General Assembly (A/62/328).

Part one
Secretariat disaster recovery and business continuity

I. Introduction

4. In its resolutions 59/276 and 60/266, the General Assembly requested the Secretary-General to submit to the Assembly the results of technical studies relating to information and communications technology (ICT) security, disaster recovery and business continuity planning and to report on disaster recovery and business continuity in field missions and on the establishment of a secondary active communications facility. The present report addresses these matters and identifies the requirements for the development and implementation of a global operational framework to enable the Secretariat to respond effectively to emergency situations that may impair the operations of critical elements of its ICT infrastructure and facilities.

5. Major enterprise application initiatives such as enterprise resource planning (ERP), customer relationship management (CRM) and enterprise content management (ECM) will be implemented as part of an enterprise approach to the provision of automated solutions and utilized throughout the Secretariat. These centrally hosted and managed systems will require robust and fault-tolerant infrastructure.

6. The organizational scope for this proposal is global, covering the United Nations Logistics Base, all peacekeeping missions, all special political missions, United Nations Headquarters in New York, the United Nations Offices at Geneva, Vienna and Nairobi, the regional commissions, and the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia, the International Criminal Tribunal for the Prosecution of Persons Responsible for Genocide and Other Serious Violations of International Humanitarian Law Committed in the Territory of Rwanda and Rwandan Citizens Responsible for Genocide and Other Such Violations Committed in the Territory of Neighbouring States between 1 January and 31 December 1994, and the International Court of Justice. The major focus of the Secretariat's approach to disaster recovery and business continuity and the subsequent resource implications relate to the two major data centres that will host enterprise applications and provide backup capabilities to all offices away from Headquarters and field missions. At the same time, United Nations Headquarters is providing organizational leadership, through coordination, standards and increased consolidation of data, to the rest of the Secretariat.

7. The current level of capability with respect to ICT disaster recovery and business continuity differs among the offices enumerated above. Most notably, neither United Nations Headquarters nor any of the seven offices away from Headquarters or Tribunals are compliant with respect to the most critical applications of their respective crisis management plans, as outlined in section IV. Resolving this deficiency is a critical component of the overall disaster recovery and business continuity strategy. Field missions, are, by necessity, owing to their operational environments, well advanced in the implementation of disaster recovery and business continuity plans. Owing to the ever-present risk inherent in peace operations, disaster recovery and business continuity is a permanent consideration,

from the mission planning stages through mission liquidation. Owing to differences in environmental stability, the approach to disaster recovery varies with regard to the Secretariat, the offices away from Headquarters and field missions. as highlighted in the following sections.

8. The telecommunications hub located in the United Nations Logistics Base at Brindisi, Italy, acts as the fulcrum for all ICT activities of field operations. In an effort to ensure continuity in cases of widespread disruptions at the United Nations Logistics Base, the Department of Field Support is currently in the process of establishing a geographically remote secondary active telecommunications facility (hereinafter referred to as "site B") that will provide additional and complimentary capacity for the ICT infrastructure currently in place in the United Nations Logistics Base and will also be utilized by the Secretariat as a disaster recovery and business continuity site and to host enterprise applications. This combined solution is presented in part one.

9. The establishment of a secondary active telecommunications facility is pivotal to the successful implementation of the Organization's disaster recovery and business continuity strategy. It will provide the infrastructure necessary to secure operations in the event of widespread disruption of the ICT infrastructure upon which the Department of Peacekeeping Operations, the Department of Field Support,[1] and the United Nations Secretariat rely to ensure secure and reliable connectivity among the United Nations Secretariat, United Nations peace operations, agencies, funds and programmes. As United Nations peace operations evolve into integrated models requiring greater coordination among all United Nations entities, the increased reliance on Department of Peacekeeping Operations/ Department of Field Support ICT networks must necessarily translate directly into an increased need to guarantee the security and reliability of the ICT infrastructure that underpins the evolving, complex, integrated model of United Nations peace operations and activities. Information on this secondary active communications facility is presented in a separate section of this report.

10. Owing to the differing levels of disaster recovery and business continuity capabilities throughout the Secretariat, information on disaster recovery and business continuity at United Nations Headquarters and field missions is presented in separate sections within this report. Section II provides background information on disaster recovery and business continuity for the Secretariat as a whole; section III details the expected results of a successful implementation of disaster recovery and business continuity plans; section IV provides information on disaster recovery and business continuity at Headquarters, offices away from Headquarters and Tribunals; and section V details the implementation of disaster recovery and business continuity in field missions. Owing to the critical nature of the secondary active communications facility, information on the requirement for this capability and on the progress in selecting a suitable facility is presented separately, in section VI.

[1] The General Assembly has approved the restructuring of the Department of Peacekeeping Operations and the establishment of the new Department of Field Support, effective 1 July 2007.

II. Background

A. Alignment with information and communications technology reform initiatives

11. The proposal in this report is aligned with the ICT reform strategy that is currently being developed by the Chief Information Technology Officer for presentation to the General Assembly at its resumed sixty-second session in spring 2008 and complements the proposal on the enterprise resource planning system which will be submitted separately. One of the aims of the disaster recovery and business continuity proposal is to establish the requisite technical capacity for the implementation of enterprise resource planning and related systems. The proposed architecture is purposely designed to provide for a global enterprise resource planning architecture by building sufficient data centre capacity. The architecture is scalable and plans have been developed in accordance with and in consideration of both immediate requirements for disaster recovery and business continuity and the necessary provisions for future requirements as indicated in ICT reform proposals. It is also in line with the effort to build a stronger enterprise network throughout the Secretariat. Ensuring that all of the offices away from Headquarters adhere to the same network standards will facilitate the widespread use of the new disaster recovery and business continuity facilities.

B. A unified approach

12. The present plan reflects a unified approach to ensuring that all disaster recovery and business continuity activities are coordinated among Secretariat departments to maximize investment, leverage synergies in ICT assets across the United Nations Secretariat and achieve economies of scale. The Information Technology Services Division has recognized the potential for disaster recovery and business continuity throughout the entire Secretariat in the Department of Field Support ICT infrastructure. In this capacity, the Information Technology Services Division and the Department of Field Support are collaborating to identify opportunities and implement viable, scalable and cost-effective solutions so as to further leverage Department of Field Support initiatives for the benefit of the entire United Nations family. A global disaster recovery and business continuity framework is proposed for implementation through:

- Utilization of the United Nations Logistics Base as a backup centre for all mission- and enterprise-critical Secretariat systems

- Establishment of a secondary active communications facility that would be used to complement the United Nations Logistics Base, host Secretariat enterprise system solutions and provide the capacity to serve as backup centre for critical offices away from Headquarters and Tribunal departmental applications

- Remote access to services and data for all Secretariat duty stations through dedicated communication links to these facilities

C. Disaster recovery and continuity of operations

13. Information and communications technology (ICT) plays an integral role in the global operations of the Secretariat. The need to ensure timely and secure communications and information exchange within and between duty stations is central to meeting the core strategic, operational and tactical mandates of United Nations missions. Expanding field operations, changing business drivers, new technologies and the Organization's commitment to leveraging ICT has resulted in an analogous expansion of ICT infrastructure to support the increased reliance on ICT networks and systems used throughout the Organization. Ensuring that a robust and fault-tolerant ICT infrastructure is in place to continue or restart operations in the event of a natural or man-made disaster or disruption has become a necessary and permanent consideration.

14. Disaster recovery and business continuity strategies have been developed to facilitate continuous telecommunications and safeguard the Organization's data, which entail ensuring that resilient and agile ICT infrastructure is in place to facilitate continuity of mission-critical operations. In order to mitigate risks to ICT assets and infrastructure inherent in the Organization's operational environment, the Secretariat has adopted a strategy that encompasses two separate but related components; data backup (disaster recovery) and redundancy (business continuity). The proposed framework is purposefully designed to address these operational requirements.

D. Potential disruptions

15. Disaster recovery and business continuity planning and implementation have gained prominence in the commercial, military and governmental sectors in recent years. In the commercial sector, estimates indicate that some companies spend up to 25 per cent of their budget on disaster recovery plans in order to avoid bigger losses. Of companies that have had a major loss of computerized records, 43 per cent never reopen, 51 per cent close within two years, and only 6 per cent survive long-term.[2] The Secretariat's ICT infrastructure and assets are subject to greater risks, as United Nations peace operations are often conducted within very unstable operational, social and political environments that are constantly under threat from both natural and man-made disasters and interruptions. The sphere of potential disruptions has expanded to include hacker attacks on networks, physical attacks on United Nations premises, and broad-based power outages such as those experienced on the east coast of the United States of America and in Italy in 2003. These interruptions can result from a number of accidental, malicious or environmental events such as:

1. Natural disasters including flooding, earthquakes and hurricanes
2. Fire
3. Power outages
4. Armed conflict/civil unrest
5. Organized or deliberate disruptions

[2] Steven Haag, Maeve Cummings and Donald J. McCubbrey, *Management Information Systems for the Information Age*, 5th ed. (New York, McGraw-Hill/Irwin, 2005).

6. System and/or equipment failures

7. Human error

8. Computer viruses/worms

16. The planned disaster recovery and business continuity approach is based on three considerations:

- **Prevention**: the establishment of robust security measures to prevent hacking, virus attacks and unauthorized physical access

- **Mitigation**: the limitation/containment of impacts resulting from a single incident through such initiatives as load-balanced ICT facilities

- **Recovery**: ensuring that suitable ICT facilities are available to restore critical data and infrastructure as and when required in the most cost-effective and operationally viable manner.

17. While the risk to telecommunications in the event of a disaster or disruption can be mitigated to a great degree through redundancy, securing and recovering critical data present a greater challenge. In order to meet this challenge, the Organization is ensuring that all critical data are backed up and secured and are easily accessible. However, this introduces a greater degree of complexity and places a considerable strain on communication links, given that data are often stored in multiple repositories located on servers in duty stations and within the theatres of operation of field missions. In the absence of Secretariat-wide enterprise systems, disparate data storage has evolved over time within United Nations offices and peace operations. The Secretariat is in the process of replacing these localized systems with centralized, enterprise solutions serving all duty stations hosted in site B and backed up in the United Nations Logistics Base. This solution will reduce local backup requirements, improve efficiency and ensure high availability.

18. The Board of Auditors reviewed the disaster recovery and business continuity plan of the Department of Peacekeeping Operations in 2004 and recommended that the Department should continue to implement the plan as a matter of priority. The report of the Board of Auditors on United Nations peacekeeping operations[3] was submitted to the General Assembly which, in its resolution 59/264 B of 22 June 2005, took note of the observations and endorsed the recommendations contained therein. Similar priority was emphasized by the Board of Auditors during its review of information and communications technology in the United Nations Organizations in New York in February 2007 when a recommendation was made to address single points of failure by establishing a contingency plan to ensure the continuity of telecommunications with offices away from headquarters in case of such failure.

E. Existing capability

19. The Secretary-General’s Crisis Management Plan for Headquarters, developed in April 2003 by the Emergency Task Force, provided policy direction and performance criteria for advancing the operational requirements for a collective disaster recovery and business continuity strategy. Assessment of the Organization’s

[3] *Official Records of the General Assembly, Fifty-ninth Session, Supplement No. 5* and corrigendum (A/59/5 and 59/5 (vol. II)/Corr.1), vol. II.

capability with respect to the Crisis Management Plan identified deficiencies in respect of measures that had not yet been implemented or funded. These deficiencies and the requirements for overcoming them are detailed in this report. The initial focus, however, was limited in scope, scale and function to addressing threats relating to scenarios one and two of the Crisis Management Plan. Under **scenario one: a limited impact emergency**, an incident or event within the United Nations complex or nearby causes an interruption in the normal course of business for a short period of time. Under **scenario two: the office site becomes unusable**, an incident or event within the United Nations complex or nearby disrupts the normal course of business for an unspecified period of time and calls for evacuation of the United Nations premises.

20. Funding for implementation of disaster recovery and business continuity measures has been uneven across the Secretariat. In general, the investments in the offices away from Headquarters have largely been limited to better data storage and off-site backup. Recent projects are aimed at building more redundancy and backup for local systems through the construction of secondary local data centres. For peacekeeping and political missions, the United Nations Logistics Base at Brindisi, Italy, provides disaster recovery capability. All the investments in disaster recovery and business continuity have yielded measurable results, affording, in most cases, 99 per cent availability of services as tested against “real-life” incidents, including the recent power outage affecting the north-east region of the United States. Likewise, the value of these investments has been evidenced on a global scale with a variety of incidents reported by various duty stations, such as the recent crisis in Lebanon.

21. The present proposal aims to fully utilize existing investments and extend the current capability while taking into account new ICT reform initiatives.

III. Expected results

22. Many of the duty stations included in the organizational scope of this project are not currently compliant with the requirements for scenarios three and four of the Crisis Management Plan. Under **scenario three: office locations and surrounding area become unusable**, incidents or events render much of office complex and the surrounding areas unreachable or unusable for an indefinite period of time. While some staff might be available to deliver critical functions, most physical infrastructure and support functions would be seriously impaired. Under this scenario, alternative worksites and staff accommodation may be needed on an interim basis. Under **scenario four: the duty station and large portions of the host country are affected by a major catastrophic incident**, incidents or events lead to widespread loss of life and destruction, rendering the region uninhabitable for an extended period of time. This scenario dictates that most functions would have to be resumed, at least for a temporary period of time, at alternative locations elsewhere in the world, involving alternate staff or the transfer of the affected office staff to these locations.

23. From an ICT disaster recovery and business continuity capability perspective, scenarios three and four envisage the following:

- The ability to maintain critical ICT services

- Ensuring continuity of key financial transactions
- Communications with the staff

24. The proposal in this report reflects certain underlying principles for global ICT operations. The proposal addresses the computing and telecommunication facilities that would be required to restart critical operations following a significant disruptive episode. The conditions under which such critical operations may restart are determined by two factors: (a) recovery time objective and (b) recovery point objective.

25. Recovery time objective is defined as the period following a disruptive event after which services covered by the disaster recovery and business continuity plans are targeted to restart. Recovery point objective is defined as the currency of the data at the time services are to be restarted. Recovery point objective is measured in terms of hours/days of data processing lost as a result of the disruptive event.

26. This proposal is based on ensuring a recovery point objective of 24 hours for all critical systems, both local and enterprise-wide. In other words, the processing loss at that point will not be greater than 24 hours. The rationale for selecting 24 hours is explained in section VIII below. For local critical applications, the recovery time objective will have to be determined by each office away from Headquarters and Tribunal based on their business impact analysis. The extent of a disruption may influence how quickly systems can be put back into service.

IV. Disaster recovery and business continuity at Headquarters and offices away from Headquarters

27. The report of the Secretary-General on the strengthening of the United Nations: an agenda for further change (A/57/387 and Corr.1) highlighted the fundamental role of ICT in the ongoing implementation of the reform process. The increasing reliance on ICT systems calls for a strategic and operational effort to ensure the security and continuity of these valued resources. The Secretary-General's report on the information and communications technology strategy (A/57/620) identifies several initiatives for addressing security policy and the technologies required to implement protection measures. The strategy also highlights the challenges to the Organization: As the Organization becomes increasingly interconnected electronically, both internally and within the United Nations system, as well as with civil society, it will be pushed to create a layered protection structure that is increasingly sophisticated, one that meets the demands of tens of thousands of users, while making sure that these resources remain available when needed.

A. Focus of the plan

28. The focus of the project is directed towards protection measures for mission-critical ICT services. The following ICT assets are deemed mission-critical and are therefore the focus of the proposal:

- Systems that are deemed essential to enabling basic administrative functions, inter alia, personnel administration, payroll, recruitment, accounts payable, procurement, treasury and disbursement, budget formulation and allocation, procurement, insurance and travel. At present these services are mainly being addressed by the Integrated Management Information System (IMIS), which will be replaced by the enterprise resource planning system.

- Electronic communication systems: electronic mail and the associated Internet infrastructure.
- Data repositories: data produced by and under custodianship of the United Nations, representing information and knowledge critical to the mission of the Organization. The enterprise content management system will replace many existing systems such as the Official Document System of the United Nations (ODS), United Nations websites and other decentralized repositories.

B. Approach to implementation

29. The framework to be put in place will address two objectives: business continuity and disaster recovery. Business continuity encompasses the computing and telecommunication facilities that will be required to restart critical operations, following a significant disruptive episode, so as to ensure continuance of ICT services. Disaster recovery addresses the preventive and operational actions required to preserve critical business software applications and data in order to minimize losses in the event of a significant disruptive episode.

30. Most of the duty stations have acquired some protection for scenarios one and two. Annex I examines the deficiencies and the proposed remedies for all the duty stations included in the organizational scope of this project (United Nations Headquarters in New York, the United Nations Offices at Geneva, Vienna and Nairobi, the regional commissions, the International Tribunal for the Former Yugoslavia, the International Criminal Tribunal for Rwanda and the International Court of Justice). There is an ongoing effort by all these duty stations to close the identified gaps. The United Nations Office at Geneva is working with the International Computing Centre to build more backup and redundancy for its local systems. Similar projects are being carried out in the Economic Commission for Africa (ECA) and the Economic and Social Commission for Western Asia (ESCWA) with the construction of secondary data centres for the most critical systems. The proposal in this report is mainly focused on providing capability to sustain scenarios three and four with the goal of ensuring a recovery point objective of 24 hours for critical services while preparing the required infrastructure for enterprise applications.

31. Two disaster recovery sites have been selected to sustain this strategy: the United Nations Logistics Base and the proposed site B. By design, these facilities are situated geographically so as to ensure the visibility of all satellites currently utilized by the United Nations. Both sites would host the computing and data storage equipment capable of operating the ICT services that have been deemed critical to supporting business continuity operations. The United Nations Logistics Base and site B will form the basis for scenarios three and four disaster recovery and business continuity support for United Nations Headquarters and the offices away from Headquarters, which is the equivalent of the tier 3 approach for peace operations detailed in paragraphs 46-50 below.

32. Both centralized data centre sites (Brindisi and site B) will mirror one another in terms of data and will host computing and data storage equipment. These could be accessed remotely from any of the duty stations covered by the plan to operate critical enterprise applications. This set-up will provide both disaster recovery and business continuity for any critical enterprise applications hosted in this environment.

33. In addition, site B could serve as a disaster recovery site for all critical departmental applications used by the duty stations within the scope of this project. A detailed list, by duty station, of the applications that could benefit from this capability is provided in annex I. As part of this proposal, a recurrent amount is being requested so as to maintain the necessary communications from the offices away from Headquarters and the Tribunals to site B.

34. Both sites must be adequately supplied with infrastructure to support their roles. Equally, other duty stations must build and maintain an appropriate capability in order to make use of these facilities. While they are an essential part of the disaster recovery and business continuity capability, these infrastructure assets would not only be in constant use so as to ensure disaster recovery, if needed, but also enhance the quality of several existing services that relied on storage and telecommunication links.

C. Integration with previously funded ICT disaster recovery and business continuity and security projects

35. In formulating the initial proposals for the disaster recovery and business continuity system, global standards have been adopted for technologies, equipment and design to leverage economies of scale, bring down maintenance costs, improve maintainability and build a common pool of skills.

36. A synopsis of previously funded projects with which the ICT disaster recovery and business continuity system would be fully integrated is presented in annex II. The integration of the proposed project with these previous activities will provide a fully functional ICT disaster recovery and business continuity system for the United Nations Secretariat.

V. Disaster recovery and business continuity in field operations

A. Disaster recovery and business continuity: a three-tiered approach

37. The disaster recovery and business continuity infrastructure for global field operations is based on a complementary scalable, three-tiered architecture designed to mitigate varying degrees of risk associated with field operations. The approach comprises on-site distributed data centres (tier 1); an off-site operational facility located in the mission’s theatre of operations in selected missions in cases where security assessments warrant (tier 2); and out-of-theatre data backup in the United Nations Logistics Base (tier 3). This three-tiered structure ensures that disaster recovery and business continuity solutions are proportional to the event causing the disruption. For example, in the absence of a distributed data centre (tier 1), all mission staff would have to relocate to an off-site location in the event of a small,

localized disruption to the operation of one data centre. Paragraphs 38-50 below detail the concept of operations for the three-tiered approach to disaster recovery and business continuity for field operations. Owing to their operating environments, most offices away from Headquarters and United Nations Headquarters do not require in-theatre, off-site disaster recovery and business continuity capability (tier 2), as explained below. This approach calls for the relocation of staff to a nearby secure facility to maintain local activities. This three-tiered approach is therefore specific to field missions. United Nations Headquarters, offices away from Headquarters and Tribunals require only the equivalent of tier 1 and tier 3 support.

B. Tier 1: In-mission, on-site (distributed data centres)

38. **Purpose**. At the mission headquarters, all mission data are stored in data centres (often referred to as “server rooms”). In the absence of distributed data centres, the partial or complete loss of the data centre would seriously impact the mission’s ability to continue daily operations. To mitigate this risk, a second, fully operational data centre that mirrors the capability, applications and data of the primary centre is established, with users evenly distributed among the centres. Thus, if one data centre fails, users will continue to have access to the mission’s core information and applications with minimal or no disruptions of day-to-day operations. The objective is to ensure resilience in the provision of information technology services by facilitating continuous access to the mission’s data and applications.

39. **Supporting technologies**. Software applications, up-to-date data files, and folder structures are hosted and accessed at each facility. This set-up is facilitated through various technologies such as mesh networking, clustering, load balancing and mirroring. High-availability clusters are groups of servers that are interconnected, thus improving the availability of services to the user. Load balancing operates by routing network traffic through clustered front-end servers that will distribute the traffic to a collection of back-end servers, thereby balancing the load on each server. Although implemented primarily for improved performance, this configuration also facilitates high availability.

40. **Illustrative example**. The data centres in Kinshasa (United Nations Organization Mission in the Democratic Republic of the Congo (MONUC)) are located in the main mission headquarters and the mission logistics base. During periods of civil unrest or backup generator failure during power outages, the main headquarters building located in the centre of Kinshasa becomes inaccessible for extended periods. During these periods, all mission data become inaccessible to the entire mission user community. Additionally, it is at these critical periods that staff safety and security are most at risk, while all important, accurate, relevant and timely information is inaccessible. With the introduction of the distributed data centre model, the load (data transmission) is distributed between the mission headquarters and the mission logistics base. Thus, all users can continue ICT operations when one of the sites is compromised, as communications will be seamlessly redirected to the operational site, greatly mitigating the risk to the operational integrity of the mission.

C. Tier 2: In-theatre, off-site (geographically redundant facility)

41. **Purpose**: In-theatre, off-site facilities are required in missions that are located in regions where the potential for civil unrest, military activity or natural disaster requiring the evacuation of staff is considered to be high. To provide this level of redundancy, an in-theatre, off-site facility would be established to ensure that a secure operating environment is available in the event of an incident requiring evacuation of mission personnel. During these periods, key staff would be relocated to this standby facility located outside the area affected by the disturbance. This standby facility would normally be located in a nearby country or State.

42. **Supporting technologies**. Data replication technologies are used to synchronize data between the primary and secondary facilities on a regular basis. Replication refers to the use of software and hardware resources to synchronize data.

43. **Illustrative example**. The United Nations Interim Administration Mission in Kosovo (UNMIK) has established an in-theatre, off-site facility in Skopje. In the event of widespread civil unrest in Priština, where the mission headquarters is located, key staff will be relocated to Skopje and will be able to resume critical operations within a short period.

44. In the recent past, the United Nations Operation in Côte d'Ivoire (ONUCI) has had to evacuate staff during various periods of unrest. During these evacuations to declared safe havens in Ghana and the Gambia, mission personnel were isolated from their work owing to a lack of access to critical business information and applications in the absence of an off-site facility. While a limited capacity communications network, entailing primarily voice and facsimile communications, was provided to evacuated personnel, no access to mission data or applications could be provided. The availability of an in-theatre, off-site facility would have ensured that key staff could continue essential operations.

45. A shared facility is the most cost-effective solution for missions located in the same geographical region. Each mission would share the costs associated with the establishment, maintenance and staffing of one off-site data centre. For example, most of the missions in the Middle Eastern region could locate their tier 2 site in Cyprus. The Department of Field Support is actively seeking such cost-saving opportunities.

D. Tier 3: Out-of-theatre, off-site (United Nations Logistics Base at Brindisi, Italy)

46. **Purpose**. Tier 3 calls for the backup of mission data in the United Nations Logistics Base and the provision of ICT infrastructure that will enable a limited number of key personnel to continue operations at the United Nations Logistics Base in the event of an occurrence that requires evacuation of all staff from the mission, where no tier 2 facility is available or where the entire theatre of operations is compromised.

47. The United Nations Logistics Base serves as the hub for all common ICT services and as a data repository for the critical data of field missions. It is peace operations' designated out-of-theatre, off-site standby facility for mission staff in the

event of an out-of-theatre evacuation. The United Nations Logistics Base facilitates business continuity by providing access to telecommunications provided both commercially and by the United Nations, enterprise applications and mission data and information systems. Access would be granted to e-mail, Internet, corporate data files and centralized applications hosted in the United Nations Logistics Base such as the Mercury procurement system and the Galileo inventory management system. On arrival in the United Nations Logistics Base, evacuated personnel would be provided with immediate access to ICT resources and could continue critical operations. In addition, all electronic transactions that had been processed in the United Nations Logistics Base would be immediately available to personnel upon resumption of duties in their duty station.

48. **Supporting technologies**. Replication technologies, similar in this regard to the tier 2 methodology, are used to transfer files and databases to out-of-theatre servers in the United Nations Logistics Base. The data are then used for offline backup protection, disaster recovery and data mining. These replication and file transfer technologies move multiple files efficiently, irrespective of their size. They also have the ability to transmit only parts of a file that have been changed, thereby reducing transmission time and bandwidth utilization, and thus increasing efficiency in the various communications links. Whenever possible, data transfers are scheduled to take place during nights and weekends when satellite links are less utilized. In a multi-tiered configuration, the latest and/or most critical files and databases are stored in real-time, fast-access storage platforms, while older and less critical files are stored utilizing more cost-effective and economically viable storage systems.

49. **Illustrative example**. During the second Gulf war in 2003, a number of personnel were evacuated to the United Nations Logistics Base from the United Nations Iraq-Kuwait Observation Mission (UNIKOM). These personnel were provided access to ICT resources and were able to continue limited operations, as access to critical data was available through centralized applications. Mission data from UNIKOM distributed systems were also available as they transported the data using storage devices, a process that would not be required today as all mission data are backed up in the United Nations Logistics Base.

50. The three-tier strategy outlined above will provide missions with the capacity to continue limited operations in cases of localized or regional disruptions. A comprehensive list of all field missions and their current disaster recovery and business continuity arrangements is contained in annex III. However, given increased dependence of the Department of Field Support and the Secretariat on the central communications hub in the United Nations Logistics Base, the Department of Field Support is currently seeking a secondary active communications facility that will provide fail-over in case of a disruption to the ICT infrastructure of the United Nations Logistics Base. Section VI below examines the necessity of having a secondary active communications facility and provides an update on the steps that have been taken to date towards sourcing the facility.

VI. The secondary active communications facility

A. Identification of need

51. The Information Technology Services Division and the Department of Field Support have identified the need for a secondary active communications facility that will be used to complement the United Nations Logistics Base and to host Secretariat enterprise system solutions as part of the three-tiered global disaster recovery and business continuity framework.

52. The development of a centralized hub for telecommunications, centralized applications, a central data repository and a global help desk in the United Nations Logistics Base satisfies an important and ever-increasing requirement for efficient and cost-effective ICT services for United Nations peace operations. In the current operational environment, it would be impossible to start new United Nations peace operations without the ICT centralized support services offered through the United Nations Logistics Base, such as the Internet, the provision of essential corporate information systems, long-distance calling, e-mail, voice over Internet Protocol, web mail, application support and a global help desk.

53. Limiting Department of Field Support operations to a single site, although benefiting from economies of scale and gained efficiencies, presents an enormous risk of compromising missions' core functions owing to the dependence on a single point for ICT operations. While all field missions avail themselves of backup and disaster recovery services from the United Nations Logistics Base, the telecommunications hub and centralized applications (Galileo, Mercury, etc.) hosted there do not have a remote backup facility. Thus, the entire Department of Peacekeeping Operations/Department of Field Support ICT network relies on a telecommunications hub that has no "alternative" in case of a major outage. An outage in Brindisi would have a catastrophic impact on all field missions' global operations: field missions would lose much of their voice communications, in particular inter-mission communications and international telephone access; all missions would lose access to the Intranet and e-mail; most missions would lose access to the Internet; and access to essential centralized information systems would be unavailable. This vulnerability has been highlighted by the Office of Internal Oversight Services (OIOS) in its recent management audit of the Department of Peacekeeping Operations.

54. A secondary active site with full capabilities must be established to ensure the continuity and integrity of the core functions of the Department of Peacekeeping Operations/Department of Field Support in the event of a catastrophic incident and to provide continuous voice, data and video services in cases of short-term disruptions. The Department of Field Support is currently seeking such a facility, one that will meet its requirements for a secondary active site and will also meet the requirements for hosting the Secretariat systems.

B. Concept of operations

55. The term "secondary active" describes the core approach taken in establishing the facility. Both the primary and secondary sites will be considered "live" operational hubs, as the workload will be distributed to both sites simultaneously.

Neither facility will be on standby, awaiting a disaster, but will be continuously online (that is to say, each site will process approximately 50 per cent of the traffic). In the event of a disaster at one site, the remaining operational site will be required to absorb only 50 per cent. This configuration will ensure that in case of a major outage, only 50 per cent of operations would initially be compromised at any given time. The facilities are often referred to as “active/active” or “hot” sites in this type of configuration. Each facility has the capacity to absorb some or all of the work of the other for an extended period of time, thereby eliminating dependency on the availability and relocation of staff at any single location, and eliminating the risk associated with a single point of failure. The configuration supports maximum geographical separation and assures business continuity through actual use rather than through infrequent testing. Additionally, the utilization of least-cost routing technologies will facilitate usage of the best rates available for field missions’ external telecommunications traffic, thus providing continuous savings for the Organization.

56. It is anticipated that site B will be utilized by all United Nations peace operations, United Nations Headquarters and offices away from Headquarters. As it is scalable, site B provides additional opportunities which could include utilization by United Nations organizations, funds and programmes. The facility will mirror the telecommunication infrastructure currently in place in the United Nations Logistics Base and will present an opportunity for significant improvements in equipment layout, integration and configuration.

57. The secondary facility would also host the computing and data storage equipment capable of operating the Secretariat ICT services that have been deemed critical to supporting business continuity operations. The two sites (the United Nations Logistics Base and site B) will mirror one another in terms of data and could be accessed remotely from the business continuity sites to operate critical software applications of any of the Secretariat duty stations covered by the plan.

C. Facility sourcing process

58. In respect of selecting a suitable facility, the first major consideration would be its location, as the facility requires the visibility of all satellites currently utilized by the United Nations. Long-term contractual arrangements have been established with the satellite providers and it is envisaged that these arrangements will be required for the foreseeable future. This requirement limits possible host countries to those located within the geographical convergence of the footprint of the satellites.

59. It is also critical that site B be located at a safe distance from the current facility in the United Nations Logistics Base so as to ensure that both facilities are not compromised owing to any single event. This requires geographical separation and an independence from the current logistic, power and communications infrastructures in Brindisi. The objective is to minimize the risk that both a primary and a backup site, and their respective labour pools, could be impaired by a single wide-scale regional disruption. For example, a national power outage at one facility would not impact the second facility, as they would not share the same power grid.

60. The Department of Peacekeeping Operations, in December 2005, had initially requested proposals to host site B from the 43 States Members of the United Nations

located within the satellite convergence area. In March 2006, prior to a final selection, the Department of Peacekeeping Operations requested the Internal Management Consulting Section (iMCS) of the Office of Internal Oversight Services (OIOS) to conduct a management review of the solicitation and selection process. The Internal Management Consulting Section concluded that it was unable to validate or endorse the process used by the Department of Peacekeeping Operations, as the review had uncovered several areas where the site selection process needed to be more systematic, consistent and transparent; and it recommended three possible courses of action. After carefully considering the alternatives, the Department of Peacekeeping Operations decided to proceed with the option to disqualify the selection process and start over with a more systematic and reliable method.

61. With the active participation of the Internal Management Consulting Section in the preparatory stages, the Department of Peacekeeping Operations developed a refined process and method of soliciting, reviewing and evaluating proposed sites. In July 2006, the Department of Peacekeeping Operations resubmitted requests to all Member States within the predefined geographical area to submit new proposals to host the site. An information exchange session was conducted with Member States on 25 July 2006.

62. A multidisciplinary working group was established to conduct an assessment of received proposals utilizing selection criteria and a scorecard methodology developed with the Internal Management Consulting Section during the initiation phase of the project. Four Member States, Finland, Romania, Serbia and Spain, submitted proposals. These proposals first had to meet certain prequalification criteria, regarding, for example, location within the convergence area, size, unobstructed view of the satellites and unrestricted access to the site for a minimum of 10 years. A rigorous process of assessment of the proposals that met these criteria was then performed. The scorecard methodology used to evaluate the proposals was based on a weighted scoring method summarized under three major groupings: technical factors, financial analysis, and other operational considerations. Technical factors included site considerations, power, communications infrastructure and safety and security. The financial analysis was based on the cost associated with establishing the facility. Operational considerations included the accessibility to housing, health services, ground transportation and shipping.

63. Based on the predefined assessment criteria, the working group determined that the proposal for a site at Valencia submitted by the Government of Spain was technically compliant, met the geographical, logistic, power and communication separation requirements outlined in paragraphs 58 and 59 above, and offered the most advantageous terms for the Organization. The Department of Field Support is engaging in discussions with representatives of the Government of Spain in order to draft a host country agreement. The total three-year cost to the United Nations peacekeeping operations for establishing the facility, comprising equipment purchases, staffing and operational costs, is estimated at $9,817,450. It is envisaged that costs may be recovered for the usage of the facility by non-Department of Peacekeeping Operations/Department of Field Support entities, when it is fully operational, through standard charge-back mechanisms. In its proposal, the Government of Spain offered to assume all other costs, such as those for all construction related to establishing the facility. It is planned that the facility will be fully operational in 2010, if the project is initiated in the fiscal period 2007-2008.

64. The above estimate of $9,817,450 includes the establishment of one P-5 post required for management of the facility. Given its crucial role in global telecommunications for peacekeeping and the active relationship with the United Nations Logistics Base as outlined in paragraph 55, establishing and managing site B will be a complex undertaking and will require extensive knowledge and managerial expertise. The incumbent will be responsible for all ICT operational, managerial and administrative tasks associated with the set-up and daily operations of the facility, with administrative assistance to be provided by the United Nations Logistics Base. Duties will include: planning and design of the facility's infrastructure in conjunction with the host Government; project management; supervision of staff within the facility; initiating the procurement of required equipment; installation of the equipment upon completion of the structures; day-to-day management of the facility and its resources when established; and liaison with the host Government, the United Nations Logistics Base and United Nations Headquarters.

VII. Timetable for implementation

A. United Nations Headquarters and Offices away from Headquarters

65. The time frame for the development and implementation of the proposed plan is approximately 18-24 months, contingent on procurement, delivery of goods and the availability of the required human resources, as detailed in section VIII below.

66. The project plan is to be implemented concurrently for the United Nations Logistics Base and site B, as soon as it is made available by the Department of Field Support, and will be customized based on the unique requirements of each installation. Twelve months are indicated for the duration of all activities with a contingency of from 6 to 12 months to account for procurement, recruitment and facility readiness for each installation.

67. The implementation plan will include procurement of goods and services and recruitment of human resources; as both these activities will need to be conducted frequently, they have the potential to significantly impact the final implementation.

68. Based on lessons learned and the extensive research of the proposed project, several steps have already been taken to ensure a timely and risk-managed project schedule. These steps include:

- A global Secretariat-wide project management team
- Published expressions of interest and request for proposals
- A single source, systems-contract approach, wherever feasible
- Fully defined technical specifications and standards
- Establishment of the integration and interoperability of components

69. Consultations with industry suggest that the estimate of 18-24 months is very realistic.

B. Department of Field Support: site B

70. As detailed in section V, the Department of Field Support is well advanced in the implementation of disaster recovery and business continuity for field missions. However, as outlined in section VI, a secondary active communications facility is required to eliminate the risk associated with a single point of failure that would exist based on dependence of field operations on the United Nations Logistics Base. It is expected that site B will be fully operational upon completion of the project.

VIII. Financing and managing the project

A. Resource requirements

71. The disaster recovery and business continuity approach, based on cost-benefit analysis, balances operational requirements and cost-efficiency. The approach measured cost sensitivity to Recovery Time Objective/Recovery Point Objective benchmarks of less than 24 hours and greater than 24 hours. The analysis indicated nominal cost differences between 12 hours and 48 hours. However, a Recovery Time Objective/Recovery Point Objective of less than 12 hours was estimated to cost nearly twice the amount in the current proposal based on telecommunication and hardware costs. On the other hand, a Recovery Time Objective/Recovery Point Objective of 72 hours or more was estimated to cost approximately half the amount in the current proposal; however, the resulting detriment to the operations of the Organization was deemed to be significantly costly overall and therefore not acceptable. The present proposal for the implementation of an ICT disaster recovery and business continuity capability commensurate with the operational requirements of the Secretariat has been assessed to be the most cost-effective.

72. Table 1 below summarizes all costs associated with the implementation of disaster recovery and business continuity in the United Nations Logistics Base and site B. These include all capital expenditures as well as projected recurring expenditures including telecommunications costs, maintenance costs and the costs for the human resources deemed necessary to install and operate the proposed infrastructure and the systems designed to support the plan.

73. Project costs proposed to be financed from the regular budget in the biennium 2008-2009 are estimated at $11,249,400 United States dollars. The three-year project cost for peacekeeping is $9,817,400, of which $298,700 is for the period 1 July 2007-30 June 2008 and $9,518,700 for the period 1 July 2008-30 June 2010. The details of these costs are shown in the table below.

Table 1
Costs associated with the implementation of disaster recovery and business continuity in the United Nations Logistics Base at Brindisi, Italy, and at site B
(United States dollars)

		Peacekeeping budget	
Object of expenditure	*Regular budget (2008-2009 estimate before recosting)*	*1 July 2007-30 June 2008*	*1 July 2008-30 June 2010*
Posts	395 400	96 500	2 453 000
Other staff costs	115 000		511 500
Travel of staff	66 000	64 000	112 000
Contractual services	3 123 800		
General operating expenses	3 674 400	122 600	2 603 800
Furniture and equipment	3 811 000		3 452 700
Staff assessment	63 800	15 600	385 700
Total	**11 249 400**	**298 700**	**9 518 700**

74. The amount requested under the regular budget encompasses the equipment, software and services required to implement replication and disaster recovery capabilities in both the United Nations Logistics Base and site B for the Secretariat and the offices away from Headquarters. It also includes a yearly recurrent amount of $2,338,500 requested in part for the maintenance cost of the equipment but, more importantly, to provide communications infrastructure and links between the offices away from Headquarters and site B serving as disaster recovery site for the most critical applications for offices away from Headquarters. Additional investments may be required by some of the offices away from Headquarters to bring their own systems up to the technical standard needed to operate in such an environment. Capital expenditure will also have to be incurred periodically on additional storage capacity so as to accommodate growth in volume of data to be stored.

75. As outlined in section VI, the three-year cost under the peacekeeping budgets to establish site B is $9,817,450. This includes both post and non-post resources. The resource requirements for the period 1 July 2007-30 June 2008 for peacekeeping amount to $298,700. This includes the establishment of one P-5 post to manage the project and the facility and one General Service post to provide administrative support. Transportation and shipping costs are also included.

76. As indicated in paragraph 20, the implementation of disaster recovery and business continuity across the Secretariat has been uneven at best. While the Department of Peacekeeping Operations is well advanced in the implementation of disaster recovery and business continuity plans necessitated by its operational environment, the Secretariat and the offices away from Headquarters require investment to elevate the technical infrastructure. For that reason, the request for equipment, licences and contractual services is higher for the regular budget and this needs to commence in 2008.

77. The Secretariat and offices away from Headquarters project will be centrally managed by Headquarters under the direction of the Chief Information Technology Officer, who will be supported by the service offices at Headquarters (Information Technology Services Division/Communications and Information Technology Service) and within each respective duty station. To ensure a well-coordinated approach to project management, a small task force made up of staff from within the already existing resources of the Information Technology Services Division and the Communications and Information Technology Service has been established at Headquarters.

78. Headquarters will oversee the central direction, management and coordination functions relating to project management and the activities undertaken by the project management team. Responsibilities carried out by the team will include: promotion of Secretariat-wide disaster recovery and business continuity system design standards; organization of forums, work groups and meetings to ensure a unified approach to the project; coordination and management of single-vendor contracts; facilitation of policy, procedure and guidance directives as determined by the global working group; assuring Secretariat-wide interoperability of relevant technologies; and minimization of redundancy of effort in producing work products such as high-level business cases, requests for proposals, and training materials.

B. Human resources requirements

79. The management and operation of a global operational framework for ICT disaster recovery and business continuity require a small cadre of dedicated staff and contractual services. The establishment of two Senior Disaster Recovery/Business Continuity Officer posts under the regular budget is critical to the achievement of the proposal. The United Nations Logistics Base and site B will need the additional staffing (one P-5 staff member at each location) with specialized skills to deal with the implementation and management of the disaster recovery and business continuity strategy. The services provided will be for the United Nations Secretariat as a whole. In their capacity as global disaster recovery sites, the United Nations Logistics Base and site B will, additionally, require contractual services to support the maintenance of servers that have to run the various mission-critical applications.

80. As outlined in section VI and paragraph 75 above, site B will be fully established over a three-year period. Under the support account for peacekeeping operations, one P-5 staff member and one General Service staff member are required in Phase I of the project. The P-5 staff member will be responsible for the establishment and commissioning of site B, including the planning, implementation, monitoring and evaluation of all site B project activities. The General Service staff member will provide administrative support for the project. The approved posts will be supported within existing resources in the support account for the period ending 30 June 2008 and proposed for inclusion as additional posts in the context of the support account budget for 1 July 2008-30 June 2009. Additional posts will be required for phases II and III to provide management and operational support as the facility is being established as a global ICT hub and will be proposed under future support account budgets.

81. The Department of Field Support requires one P-5 staff member to provide managerial oversight for the disaster recovery and business continuity services in field missions. The incumbent will coordinate all disaster recovery and business continuity activities in field missions from United Nations Headquarters. The incumbent will act as the Department of Field Support disaster recovery and business continuity focal point, provide central direction on the Department of Field Support-disaster recovery and business continuity activities and develop, maintain and implement policies, procedures and systems for the particular needs of disaster recovery and business continuity in field missions. Table 2 below shows the distribution of posts between the regular budget and the peacekeeping budget.

Table 2
Distribution of posts for the United Nations Logistics Base and site B

		Peacekeeping budget		
Category	*Regular budget (2008-2009)*	*July 2007-June 2008 (phase I)*	*July 2008-June 2009 (phase II)*	*July 2009-June 2010 (phase III)*
Professional and higher				
Assistant Secretary-General	—	—	—	—
D-1	—	—	—	—
P-5	2	1	1	1
P-4	—	—	3	4
P-3	—	—	1	1
Subtotal	**2**	**1**	**5**	**6**
General Service and related				
Other level	—	—	—	—
Local level	—	1	5	14
Subtotal	**—**	**1**	**5**	**14**
Field Service (Other level)	—	—	1	2
Subtotal	**—**	**—**	**1**	**2**
Total	**2**	**2**	**11**	**22**

C. Opportunities for return on investment

82. An investment in disaster recovery and business continuity capability is not limited in value to its single purpose, but offers numerous opportunities for significant return on investment. The system is not employed only in instances of response: it is a continuous-use system offering substantial performance and capacity increases for day-to-day operations. With the proposed system in place, the rationale behind providing processing autonomy for the Internal Management Information Section, enterprise resource planning and other enterprise applications to all duty stations and resulting operation of multiple installations begins to

weaken. The consolidation of some resource-intensive administrative activities becomes highly feasible. Such consolidation could generate significant savings to the Organization and, if implemented, will provide impetus for reviewing major administrative functions with significant potential for increased efficiency. Efforts are under way to assess this potential to foster full use of ICT as an enabler of efficiency throughout the Organization so that returns on investments can be realized.

IX. Conclusions and recommendations

A. Regular budget

83. Based on the results of extensive analysis, this report contains a proposal for an implementation commensurate with the demands of the operating requirements of the Organization, while remaining fully cognizant of the ever-present threats to ICT services. The Secretary-General is firmly committed to pursuing this key element of his proposals for secure and reliable mission-critical ICT services supporting the Organization's mission. The implementation of these proposals would give rise to additional activities and resource requirements of $11,185,600 under Section 28D, Office of Central Support Services, of the proposed programme budget for the biennium 2008-2009 (A/62/6 (Sect. 28D)) and $63,800 under section 35, Staff assessment, of the proposed programme budget for the biennium 2008-2009 (A/62/6 (Sect. 35)), to be offset by an equivalent amount under income section 1, Income from staff assessment, of the proposed programme budget for the biennium 2008-2009 (A/62/6 (Income sect. 1)). The proposal would require the establishment of two posts at the P-5 level under the regular budget as well as the major requirements of $3,123,800 for contractual services, $3,674,400 for general operating expenses, and $3,811,000 for equipment, as per paragraph 73.

B. Peacekeeping

84. A secondary active site with full capabilities is required to ensure the continuity and integrity of the core functions of field missions in the event of a catastrophic incident and to provide continuous voice, data and video services in cases of short-term disruptions. The creation of a secondary site at Valencia would enable the Department of Field Support to meet the requirements of continuity in services to missions.

85. The total three-year cost to the United Nations peacekeeping operations for establishing the facility, consisting of equipment purchases, staffing and operational costs, is estimated at $9,817,400. The resource requirements for the period 1 July 2007-30 June 2008 is $298,700 and includes the establishment of one P-5 post and one General Service temporary position, $64,000 for travel of staff and $122,600 for general operating expenses, as detailed in paragraph 73.

86. Approval is needed for one post at the P-5 level under the Department of Field Support to provide managerial oversight for the disaster recovery and business continuity services in field missions, as described in paragraph 81. The position will be supported within existing resources of the support account for the period ending

30 June 2008 and will be proposed for inclusion as an additional post in the proposed budget for the support account for the period 1 July 2008-30 June 2009.

Part two
United Nations Headquarters disaster recovery and business continuity capability

I. Introduction

87. The increase of critical departmental applications with high-availability requirements coupled with the imminent implementation of the capital master plan provides impetus to enhancing current United Nations Headquarters disaster recovery and business continuity capabilities. The present report explains the current condition of the United Nations Headquarters data centres, and the impact of the transition under the capital master plan, and elaborates on a proposal for ensuring the continuity of ICT services for scenarios one and two as detailed in part one, section III. The intended results of the proposal are the design and implementation of a disaster recovery and business continuity infrastructure sufficiently capable of addressing risks and meeting the United Nations Headquarters ICT service demands of the future.

88. The current ICT facilities that provide data centre service include:

- The Secretariat PABX centre: a 2,000 square foot telecommunications facility established in the Secretariat building in the 1980s. This facility provides telephonic services to all Secretariat area buildings.
- The Secretariat data centre: a 5,000 square foot data centre established in the Secretariat building in the 1980s currently providing computing, storage, network and related infrastructure services to all Secretariat buildings.
- The Basement extension: a 1,000 square foot facility established in 2000 to augment the Secretariat data centre as a result of space limitations.
- The Security Command Centre: a 1,000 square foot facility built in 2006 providing computers, storage and network infrastructure for the physical security system.
- The Manhattan Development Corporation 2 (DC2) Secondary Data Centre: a 3,000 square foot facility built in the 1980s to provide disaster recovery and business continuity capability to the Secretariat data centre.

89. The proposal in part two presents an opportunity to improve upon and consolidate these five ICT facilities into two facilities, a North Lawn data centre and a data centre in Long Island City, while providing the necessary additional space needed for actual disaster recovery and business continuity capability. This approach is necessary to mitigate the increased risk exposure for United Nations Headquarters but also offers numerous advantages which, on the basis of cost-benefit analysis and risk assessment, present the most advantageous business case for achieving disaster recovery and business continuity objectives.

90. As indicated in part one, the proposed site B would serve United Nations Headquarters for scenarios three and four and maintain high availability for major

enterprise applications such as enterprise resource planning, customer relationship management and enterprise content management. The proposals of parts one and two of this report are therefore complementary.

II. Risk exposure

91. The initial 3,000 square feet allocated for disaster recovery and business continuity in DC2 are not sufficient to sustain the systems' backup needs for local applications. It also does not allow any leverage for building additional redundancy for the most critical local applications in order to limit business interruptions. Analyses have shown that if the Information Technology Services Division does not improve and expand the area, United Nations Headquarters will not be able to prevent loss of data and increasing downtime may result.

92. In addition, the relocation of data centre facilities currently located in the main Secretariat building under the capital master plan would require the DC2 facility to operate as the primary data centre. This was not its intended use and consequently the facility does not have sufficient capacity to absorb these significantly increased demands. Specifically, the current power and cooling systems are obsolete, there is no emergency power, the space cannot accommodate the required expansion, and the facility does not have a secondary satellite dish. While the facility provided sufficient capacity for the purposes originally intended, its proximity to the Secretariat building and its sharing of power and communications systems do not present the ideal conditions for an enterprise-class disaster recovery and business continuity facility. These risks and the current potential opportunities provide impetus for proposing an alternative strategy aimed at optimizing investment and providing greater value and security to the Organization.

93. Risk exposure emerging from years of growth and the capital master plan project suggest a call for change. Both data centres are located in spaces not intended to accommodate computer room functions and infrastructure. Furthermore, all spare electrical and cooling capacity has been exhausted as a result of expansion since the 1980s designed to meet growing demand. Under current conditions, there is no capacity for growth or scalability to meet future requirements. Moreover, the facilities are showing their age and fallibility along with limited fire suppression capability and poor air flow and cooling, which often result in overheating of critical hardware systems.

94. The current secondary data centre in DC2 has no emergency generator backup, and is located within one city block of the primary data centre in the Secretariat building. These factors render the facility inappropriate as a backup site for mission-critical enterprise applications and for business continuity and disaster recovery purposes. In light of these deficiencies, the Board of Auditors recently noted that the current arrangement was unsustainable through 2008, and recommended relocation of the secondary data centre to a more appropriate site. Clearly, this is a critical problem which the Secretariat must address without delay.

III. Rationale

95. The capital master plan project poses a high risk to the continuity of ICT infrastructure. In the context of this increased risk, information on the establishment of a North Lawn data centre and an alternative data centre facility so as to preserve United Nations Headquarters capability for disaster recovery and business continuity is presented in the following sections. The Secretariat's proposal for addressing these risks offers numerous long-term advantages and presents the Secretariat with a unique opportunity to upgrade and consolidate facilities and with the possibility of establishing multi-agency joint operations.

96. A Long Island City data centre has been proposed to replace the secondary data centre in DC2. The four other facilities will be consolidated in the North Lawn data centre. The Organization is currently considering several sites in Long Island City which could accommodate up to approximately 300 staff and the data centre. The establishment of a location in Long Island City as a replacement for DC2 would enable the Secretariat to take advantage of its geographical, physical, and technical superiority as a disaster recovery and business continuity facility for United Nations Headquarters.

IV. Business case

97. Amid the urgent requirement to increase the size of the United Nations Headquarters secondary data centre and mitigate risks incurred under the capital master plan transition, the Long Island City data centre proposal nevertheless presents a business case with extra benefits that include the consolidation of data centres; access to a lower-rent area along with the freeing up of existing space for United Nations business needs; cooperative arrangements with New York City-based funds and programmes; and improvements to tier 1 disaster recovery and business continuity capability and scalability.

98. **Continuity under the capital master plan**. The transition under the capital master plan will require the relocation of the 19th and 20th floor data centres and staff to a new facility in the current underground North Lawn printing plant building, thus taking advantage of space made available consequent to a reduction in the need to store paper documents, whose number will continue to shrink over the coming years. However, transitions of this nature are always extremely challenging and should not be initiated until an adequate secondary data centre is in place. The Information Technology Services Division proposes to establish a secondary data centre outside of midtown Manhattan as soon as possible, which would thus allow the space on the 11th floor of DC2 to revert to its former use as office space.

99. **Relocation of Information Technology Services Division staff.** There will be a need for additional space for 5 new staff (3 under the regular budget and 2 extrabudgetary) and approximately 36 contractors for whom resources have been proposed under section 28D, Office of Central Support Services, of the proposed programme budget for the biennium 2008-2009 (A/62/6 (Sect. 28D)). These staff and contractors will work on operational matters or major projects within the Information Technology Services Division. Owing in part to unexpected procurement delays but also because of space constraints within the Secretariat complex, the Information Technology Services Division has been unable to move

forward as quickly as anticipated on a number of critical projects. The allocation of additional space would resolve this issue.

100. **Strengthening organizational capabilities**. The move of additional Information Technology Services Division staff to Long Island City will strengthen the organizational capabilities needed for the ICT reform and the implementation of enterprise systems. Only end-user support staff and required management would need to stay in the Secretariat building, while all other ICT resources would work together out of the same location. As the Information Technology Services Division is facing many challenging projects, this geographical proximity will help create more synergy, avoid redundancy and improve communication and efficiency. This also offers the possibility to freeing up space in the Secretariat building for other United Nations needs even after the capital master plan project is over, while providing accommodation for staff at less cost than in Manhattan.

V. Opportunity for joint operations

101. The Information Technology Services Division will require a reliable secondary data centre online before the start of the renovation of the Secretariat building. In fact, this is an urgent situation today. It is understood that the United Nations Children's Fund (UNICEF), the United Nations Population Fund (UNFPA), the United Nations Joint Staff Pension Fund and the United Nations Development Programme (UNDP) have similar problems regarding their secondary data centres. The Information Technology Services Division has approached these organizations and all have expressed an interest in exploring the possibility of sharing a consolidated data centre in Long Island City and sharing costs. The Secretariat sees this as a unique opportunity to work with other organizations located in New York and to reduce long-term costs across the United Nations system while increasing efficiency.

102. Recent discussions with UNICEF, UNDP, UNFPA and the United Nations Joint Staff Pension Fund suggest new opportunities for providing a common service data centre. With the approval of the Long Island City facility, the possible cooperative arrangements, which would include a multi-agency joint operation, may be realized.

103. The new data centre in Long Island City is planned to provide space availability of 12,000 square feet. Only half of that space is needed by the Information Technology Services Division for its actual operations; the other half would be made available to the other organizations, with the advantage for all parties of sharing the fit-out and maintenance cost and benefiting from economies of scale. The Information Technology Services Division will also continue to host part of the Department of Peacekeeping Operations/Department of Field Support operations which represent 20 per cent of its actual data centre activities. Since only 6,000 square feet of the new 12,000 square foot data centre will be used for Information Technology Services Division operations, the Department of Peacekeeping Operations/Department of Field Support will be given the equivalent of 1,200 square feet which represents 10 per cent of the physical space of the new data centre. In this regard, 10 per cent of the fit-out, rental and maintenance cost will be covered by the support account.

VI. Cost-benefit analysis

104. The establishment of a Long Island City data centre was assessed on the basis of a comparative cost-benefit analysis that weighed the options of renovating the existing DC2 facility, seeking alternate New York City-based options, and having operations migrate to a Long Island City data centre. The proposed strategy would enable the consolidation of five existing ICT facilities into two (see para. 88). The two facilities would be geographically separate so as to provide independent power and communication grids, and significantly improved environmental controls such as fire suppression, cooling and emergency power. However, it is also important that they be close enough together to allow technical and support personnel to travel between them quickly and efficiently. The benefits to be derived from the selection of Long Island City are numerous and include dual points of entry for communications; a power and communication grid different from that of the Secretariat; reduction of current lease rates to nearly half those of Manhattan; and scalability to expand as storage and service requirements grow.

VII. Human resources requirements

105. The proposed establishment of a Long Island City data centre will require capital investment for fit-out and installation of equipment. This report identifies requirements necessary in order for the site to operate as a disaster recovery and business continuity facility, including hardware, software, services, communications and staff. Resource requirements include dedicated staff to ensure that the implementation proceeds without delay or disruption. The staff requirements include: three temporary migration managers at the P-3 level to be funded from general temporary assistance to manage the migration of both the DC2 data centre to the Long Island City data centre and the S19, S20, 2B91 and C110 data centres to the North Lawn data centre. These migration managers would start working in January 2009 to allow for from five to six months of planning before the start of the migration in May 2009.

VIII. Timetable for implementation

106. The time frame for the development and implementation of the proposed plan is synchronized with the capital master plan schedule and is contingent on the availability of the required human resources discussed in section VII. The anticipated implementation schedule is as follows:

- The latest capital master plan schedule projects construction of the Long Island City data centre to begin in the first quarter of 2008 and to be completed in May 2009, following approval of funding

- After the finalization of the Long Island City data centre construction, from three to six months will be needed for migration from DC2 to Long Island City

- A similar timing will be followed for the North Lawn data centre, with a delay of six months, meaning a starting date in the third quarter of 2008 and the completion of the project at the beginning of 2010

IX. Financing and managing the project

107. The costs for implementing the two data centres can be divided into two categories: (a) construction, fit-out and lease; and (b) equipment, contractual services and human resources.

108. **Construction, fit-out and lease of the data centres.** The construction and fit-out of the North Lawn data centre have been included as part of the capital master plan project; there are no lease costs, as the centre will be on the United Nations campus. The construction, fit-out and lease for a proposed secondary data centre in Long Island City and the accommodation of the 41 additional staff/contractors will require funding from the regular budget. The estimated requirements are based on the market rate and industry averages for rental of potential buildings in Long Island City and the construction costs. The estimated total for the fit-out of both the office space and data centre and the rent for the first two years is $20,879,200, as presented in table 3 below. Ten per cent of the fit-out and rental of the data centre only will be funded by the peacekeeping budget for its portion of the infrastructure managed by the Information Technology Services Division.

Table 3
Cost of construction, fit-out and lease of the Long Island City data centre
(United States dollars)

	Regular budget	*Peacekeeping budget*		
Object of expenditure	*2008-2009 estimate (before recosting)*	*July 2007-June 2008 estimate*	*July 2008-June 2009 estimate*	*Total*
Improvement of premises: data centre construction	15 782 200	350 700[a]	1 402 900	17 535 800
Improvement of premises: office space construction	1 142 500			1 142 500
General operating expenses: data centre	1 382 700	38 400	115 200[b]	1 536 300
General operating expenses: office space	664 600			664 600
Total	**18 972 000**	**389 100**	**1 518 100**	**20 879 200**

[a] It is estimated that in the first six months the main costs will be design fees and therefore only 20 per cent of the peacekeeping contribution to the construction will be required in the period 2007-2008.

[b] Including the peacekeeping share for the period July-December 2009 so that the total costs can be demonstrated for the two-year period 2008-2009.

109. The major cost is the construction of the data centre which is estimated at $1,000 per square feet, or $12 million for the 12,000 square foot data centre. The construction will include raising floors, the power supply and the air conditioning necessary for a data centre. Another major cost will be for the addition of an emergency generator, which will cost $4 million and provide backup electricity in case of an outage to the local supply. Other costs include the office construction, the installation of security systems and access control systems, and design fees.

Recurrent cost for rent and utilities for the data centre will amount to $781,600 on a yearly basis from which 10 per cent, or $78,200, will be funded through the support account.

110. It is noted that, while the costs presented in this report represent the total costs arising from the construction of a 12,000 square foot data centre, it is expected that there will be an element of cost-sharing between the United Nations and other organizations within the United Nations system, as per paragraphs 101-103 above. The net amount expected to be financed from the other organizations for the biennium 2008-2009 will be dependent on the final outcome of the negotiations with them that are currently under way. It is expected that as deliberations continue as regards the proposals of the Secretary-General on disaster recovery and business continuity, additional information will become available.

111. The Secretariat is proposing to share costs on a square-foot basis. Based on the figure for the total square feet reported in paragraph 110 above, estimated cost-sharing percentages on square feet would be the following:

- United Nations Headquarters: 40 per cent
- Department of Peacekeeping Operations/Department of Field Support: 10 per cent
- Other funds and programmes: 50 per cent

112. The capital master plan will be responsible for undertaking the design necessary in order for the swing space to include both the Information Technology Services Division data centre and staff, with costs borne through this proposal.

113. **Equipment, contractual services and human resources.** Table 4 below summarizes the costs associated with the establishment of the new first (North Lawn) and secondary (Long Island City) data centres. These include all capital expenditures as well as projected recurring expenditures including telecommunications, maintenance costs and the human resources deemed necessary to install and operate the proposed infrastructure and systems so as to support the plan. As 20 per cent of the actual activities are related to the Department of Peacekeeping Operations/Department of Field Support, the same proportion of the cost will be funded by the peacekeeping budget for the acquisition and installation of equipment in both data centres. The total requirements for the equipment, contractual services and human resources needed to establish the two data centres amount to $21,339,300. The requirements for the proposed Long Island City data centre are estimated to be $12,825,200, with $10,260,200 proposed from the regular budget and $2,565,000 proposed from the peacekeeping budget. The requirements for the North Lawn migration from the Secretariat data centre are estimated to be $8,514,100, with $6,811,300 proposed from the regular budget and $1,702,800 proposed from the peacekeeping budget.

Table 4
Costs associated with the establishment of the new first (North Lawn) and secondary (Long Island City) data centres
(United States dollars)

	Long Island City		*North Lawn*		
	Regular budget	*Peacekeeping budget*	*Regular budget*	*Peacekeeping budget*	
Object of expenditure	*2008-2009 estimate (before recosting)*	*July 2008-June 2009 estimate*	*2008-2009 estimate (before recosting)*	*July 2008-June 2009 estimate*	*Total*
Other staff costs	225 100	56 200	112 600	28 100	422 000
Contractual services	1 937 600	484 400	593 600	148 400	3 164 000
General operating expenses	1 816 800	454 200	1 468 800	367 200	4 107 000
Furniture and equipment	6 252 000	1 563 000	4 622 000	1 155 500	13 592 500
Staff assessment	28 700	7 200	14 300	3 600	53 800
Total	**10 260 200**	**2 565 000**	**6 811 300**	**1 702 800**	**21 339 300**

114. A major part of the budget requirements are related to the purchase of new hardware (servers, firewalls, uninterruptible power supply and racks, tape libraries, storage area network and Internet Protocol telephony equipment) to support the data migration. This equipment, referred to as “seed equipment”, needs to be preinstalled to avoid any downtime during the migration and transfer of the existing equipment from the old data centres to the new data centres. Additional funds are requested for the communication infrastructure and contractual services that will need to be built in both Long Island City and the North Lawn to ensure connectivity between the United Nations buildings and the new data centres. Three temporary migration managers are proposed to be funded from general temporary assistance commencing in January 2009.

115. As of year three, there will be annual recurrent costs for maintenance of the hardware and software components, which are estimated at $1,680,400 in annual recurrent expenditure. Twenty per cent of the actual activities of the current data centres are related to the Department of Peacekeeping Operations/Department of Field Support and therefore it is proposed that 20 per cent of the annual recurrent costs ($336,100) be funded by peacekeeping. Capital expenditure will also be incurred periodically on additional storage capacity to accommodate growth in the volume of data to be stored and will be proposed as part of future proposed programme budgets for capital improvements.

X. Conclusions and recommendations

116. Based on the current condition of the data centres and the potential impact of the capital master plan on the continuity of ICT operations, the Secretary-General is committed to establishing an alternative data centre facility to preserve United Nations Headquarters capability during and after this period. The implementation of this proposal would give rise to additional activities and resource requirements of $36,043,500 under the regular budget for the biennium 2008-2009 comprising

$18,972,000 for the construction and lease costs of the proposed Long Island City data centre, $10,260,200 for the equipment needed for the establishment of the Long Island City data centre and $6,811,300 for the equipment for the North Lawn data centre.

117. The Secretary-General believes that it is essential that the Organization proceed with implementation of the business continuity and disaster recovery project without further delay. It is therefore requested that, in the interest both of maintaining the reliability of United Nations Headquarters information services and of implementing the capital master plan, a decision be made to proceed with an ancillary project to lease space and fit out a secondary data centre and office space for incoming staff/contractors/consultants in Long Island City and furthermore to actively pursue the opportunity for the secondary data centre to be shared among multiple organizations, on a cost-sharing basis.

Part III
Summary of resource requirements for disaster recovery and business continuity and request for action to be taken by the General Assembly

I. Summary of resource requirements

118. Table 5 summarizes the resource requirements for parts one and two by site. The total resource requirements under the proposed programme budget for the biennium 2008-2009 are $47,292,900. The resource requirements for the peacekeeping budget are shown for the three financial periods, the last ending June 2010, and total $16,367,000. The entire period covers the three phases necessary for the full implementation of the proposed site B at Valencia and the share of costs for the North Lawn and Long Island City data centres.

Table 5
Summary of resource requirements set out in parts one and two, by site
(United States dollars)

	Regular budget	*Peacekeeping budget*				
Site	*2008-2009 estimate (before recosting)*	*1 July 2007-30 June 2008 (1)*	*1 July 2008-30 June 2009 (2)*	*1 July 2009-30 June 2010 (3)*	*1 July 2007-30 June 2010 (4)=(1)+(2)+(3)*	*Total per site*
Proposed site B: Valencia	11 249 400	298 700	3 917 300	5 601 500	9 817 500	21 066 900
Long Island City: equipment	10 260 200		2 565 000	199 200	2 764 200	13 024 400
North Lawn: equipment	6 811 300		1 702 800	136 900	1 839 700	8 651 000

	Regular budget	*Peacekeeping budget*				
Site	*2008-2009 estimate (before recosting)*	*1 July 2007-30 June 2008 (1)*	*1 July 2008-30 June 2009 (2)*	*1 July 2009-30 June 2010 (3)*	*1 July 2007-30 June 2010 (4)=(1)+(2)+(3)*	*Total per site*
Long Island City: construction and lease costs	18 972 000	389 100	1 518 100	38 400	1 945 600	20 917 600
Total	**47 292 900**	**687 800**	**9 703 200**	**5 976 000**	**16 367 000**	**63 659 900**

II. Action to be taken by the General Assembly: regular budget

119. The General Assembly is requested to approve the additional resource requirements for the biennium 2008-2009 of $30,261,400 under section 28D, Office of Central Support Services, $16,924,700 under section 32, Construction, alteration, improvement and major maintenance, and $106,800 under section 35, Staff assessment, to be offset by an equivalent amount under income section 1, Income from staff assessment.

120. Consequently, an additional provision of $47,186,100 would be required over and above the resources of the proposed programme budget for the biennium 2008-2009. That provision would represent a charge against the contingency fund and, as such, would require appropriations for the biennium 2008-2009 to be approved by the General Assembly at its sixty-second session.

121. The General Assembly is also requested to approve the establishment of two posts at the P-5 level under section 28D, Office of Central Support Services.

III. Action to be taken by the General Assembly: peacekeeping

122. The action to be taken by the General Assembly in connection with the financing of the secondary active communications facility are:

(a) To approve the proposed location at Valencia, Spain, of the secondary active telecommunications facility;

(b) To take note of the intention to meet the additional proposed requirement not exceeding $202,200 to finance the requirements of the secondary active telecommunications facility, to be prorated from within the already approved resources of individual peacekeeping operations for the period from 1 July 2007 to 30 June 2008;

(c) To also take note of the intention to meet the requirement not exceeding $96,500 in general temporary assistance provisions in respect of the P-5 and General Service positions for site B, to be prorated from within the already approved resources of individual peacekeeping operations for the period from 1 July 2007 to 30 June 2008;

(d) To further take note of the intention to meet, from within the already approved resources of the support account for peacekeeping operations for the period from 1 July 2007 to 30 June 2008, the requirement for general temporary assistance provisions in respect of the P-5 position in the Department of Field Support.

123. The actions to be taken by the General Assembly in connection with the peacekeeping operations share of the Long Island City and North Lawn data centres are:

(a) To take note of the negotiations currently under way with the United Nations organizations, funds and programmes in respect of the cost-sharing arrangement including that portion of the proposed peacekeeping support account budget for the period from 1 July 2008 to 30 June 2009;

(b) To also take note of the additional requirement not exceeding $389,100 towards the share of the design and rental costs of the North Lawn and Long Island City data centres to be prorated from within the already approved resources of individual peacekeeping operations for the period from 1 July 2007 to 30 June 2008.

Annex I

Disaster recovery and business continuity deficiencies and proposed remedies, by duty station

Economic Commission for Africa (ECA)

1. The Economic Commission for Africa (ECA) ICT service constituency comprises 900 user accounts on average per year, including subregional offices. An estimated 2,000,000 hits by public users accessing the ECA website are registered monthly, including substantive data repositories and publications. The headquarters duty station (Addis Ababa) is in the process of acquiring additional storage area network, mainly for e-mail storage. There is also a construction project that, when finalized, will provide for a second data centre for scenarios one and two.

2. Site B under this proposal will include protection measures for enterprise applications such as the Integrated Management Information System (IMIS), e-mail, Lotus Notes workflow applications (120 databases), CTS and Chase Insight (treasury), the geographic information system (GIS), the Virtual Library System, statistical databases, correspondence tracking databases, the procurement application, and file servers. Site B under this proposal has the capacity to include protection measures for the ECA main website (www.uneca.org), and substantive data repositories such as geoinformation systems, the ECA Science and Technology Network (Estnet), document tracking systems, statistical databases and “experts” databases.

Economic Commission for Latin America and the Caribbean (ECLAC)

3. The Economic Commission for Latin America and the Caribbean (ECLAC) ICT service constituency comprises 1,000 user accounts on average per year, including subregional offices. An estimated 500,000 public users access the ECLAC website monthly, including substantive data repositories and publications. The duty station does not have a storage area network and therefore does not adequately cover disaster recovery and business continuity requirements.

4. Site B of this proposal will include protection measures for enterprise applications such as IMIS, e-mail, CTS (treasury), Reality (procurement), ECLAC reporting, ProTrack (project management), mission reporting, and file servers. Site B under this proposal has the capacity to include protection measures for the ECLAC main website (www.cepal.org), and substantive data repositories such as Base de Estadísticas e Indicadores Sociales (BADEINSO), Banco de Datos Encuestas de Hogares (BADEHOG), Bases de Datos Estadísticos (BADESTAT), Base de Estadísticos e Indicadores del Medio Ambiente (BADEIMA), and Indicadores de Desarrollo Sostenible (BADESALC); correspondence tracking (SAS); hardware, software and supply inventory; help desk ticketing; and WebBoard.

Economic and Social Commission for Asia and the Pacific (ESCAP)

5. The Economic and Social Commission for Asia and the Pacific (ESCAP) ICT service constituency comprises 1,000 user accounts on average per year, including subregional offices. An estimated 1,140,000 public users access the ESCAP website monthly, including substantive data repositories and publications. The duty station has a storage area network and therefore the investment is leveraged in the budget requirement.

6. Site B of this proposal will include protection measures for enterprise applications such as IMIS, e-mail, Intranet and various administrative databases and file servers. Site B under this proposal has the capacity to include protection measures for the ESCAP main website (www.unescap.org), which is hosted by an external service provider.

Economic and Social Commission for Western Asia (ESCWA)

7. The Economic and Social Commission for Western Asia (ESCWA) ICT service constituency comprises 450 user accounts on average per year, including subregional offices. An estimated 500,000 public users access the ESCWA website monthly, including substantive data repositories and publications. The duty station is in the process of establishing a new data centre and therefore the investment is leveraged in the budget requirement.

8. Site B of this proposal will include protection measures for enterprise applications such as IMIS, e-mail, the IMIS Treasury Subsystem (ITS), the IMIS Reporting System (IRS), the Consultants Registry Subsystem (CRS) and file servers. Site B under this proposal has the capacity to include protection measures for the ESCWA main website (www.escwa.org), and substantive data repositories such as substantive websites and affiliated databases, the e-Technical Corporation (e-TC), the Top Management Information System (TMIS), the Social Statistics Information System (SSIS) and the Population Policies Information System (PPIS).

International Court of Justice

9. The International Court of Justice ICT service constituency comprises 100 user accounts on average per year. An estimated 60,000 public users (2 million hits) access the International Court of Justice website per month, including substantive data repositories and publications. The duty station does not have a storage area network and therefore does not adequately cover disaster recovery and business continuity requirements.

10. Site B of this proposal will include protection measures for enterprise applications such as AccPac Accounting (General Ledger Journal entry), OfficeNet Extra, ZyImage document management, e-mail and file servers. Site B under this proposal has the capacity to include protection measures for the International Court of Justice main website (www.icj-cij.org) as well as substantive legal, linguistic, library and distribution data repositories included in the document management system.

International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991

11. The International Tribunal for the Former Yugoslavia ICT service constituency comprises 1,414 user accounts (808 in Chambers and Registry, 406 in the Office of the Prosecutor and 200 in Defence Counsels) on average per year, including subregional offices. An estimated 100,000 public users access the public website, including substantive data repositories and publications, on a monthly basis. The duty station has a storage area network and the investment is therefore leveraged in the budget requirement.

12. Site B of this proposal will include protection measures for enterprise applications such as Progen (payroll), Onesource (purchasing), the attendance and leave system, VWS (travel support), TRIM (document management), TRIBUNET, SSIS (security incident management), travel automation systems, MIF (evidence registration), OTP (intranet news), SUN (accounting system), TRS (translation request system), WMS (witness management system), e-mail, and file servers. Site B under this proposal has the capacity to include protection measures for the International Tribunal for the Former Yugoslavia main website (www.icty.org) and substantive data repositories.

International Criminal Tribunal for the Prosecution of Persons Responsible for Genocide and Other Serious Violations of International Humanitarian Law Committed in the Territory of Rwanda and Rwandan Citizens Responsible for Genocide and Other Such Violations Committed in the Territory of Neighbouring States between 1 January and 31 December 1994

13. The International Criminal Tribunal for Rwanda ICT service constituency comprises 1,200 user accounts on average per year, including the Arusha and Kigali offices. An indeterminate but significant number of public users access the International Criminal Tribunal for Rwanda website, including substantive data repositories and publications. The duty station does not have a storage area network and therefore does not adequately cover disaster recovery and business continuity requirements.

14. Site B of this proposal will include protection measures for enterprise applications such as IMIS, FACS, Sun Systems Financial, TRIM (document management), Etransport, Zylab (payroll), e-mail and file servers. Site B under this proposal has the capacity to include protection measures for the International Criminal Tribunal main website (www.ictr.org) as well as substantive data repositories.

United Nations Headquarters (New York)

15. The United Nations Headquarters ICT service constituency comprises 7,500 user accounts on average per year, spanning users in 18 annex buildings. An estimated 1 million public users access daily the Headquarters websites, including

substantive data repositories and publications. The Extranet and Intranet sites are accessed worldwide with an average of 250,000 visits daily. An existing disaster recovery and business continuity capability is in operation at the Secretariat building and DC2 data centres.

16. The proposal for Headquarters is two-faceted, including local protection measures, and capacity-building aimed at allowing it to assume its role as a disaster recovery and business continuity facility Secretariat-wide (see part two of this proposal). In the second phase, site B of this proposal will include protection measures for enterprise applications such as IMIS, e-mail, OPICS and SWIFT (treasury), Reality (procurement), disbursement interfaces (ACH and EFT payment systems), human resources vital records, and file servers. Site B under this proposal has the capacity to include protection measures for the United Nations main website (www.un.org) and substantive data repositories.

United Nations Logistics Base at Brindisi, Italy

17. The United Nations Logistics Base ICT service constituency comprises 24,500 user accounts on average per year, which include 500 Brindisi users and 24,000 field mission accounts. An estimated 500 daily public users access the United Nations Logistics Base and field mission public websites, including substantive data repositories and publications. An existing disaster recovery and business continuity capability is in operation at the United Nations Logistics Base data centre.

18. The budget requirements for the facility provide expansion for the United Nations Logistics Base to enable it to assume its role as a Secretariat-wide disaster recovery and business continuity facility. The United Nations Logistics Base proposal includes the technical enhancements needed to scale its current operation to meet the requirements indicated for each duty station, as reported in the present annex. The proposal is based on an augmentation of its data link to New York, dedicated staffing, and additional storage capacity scaled for current requirements of 71 terabytes, with the capability to expand storage capacity if needed to meet a five-year projection based on industry standards.

United Nations Office at Geneva

19. The United Nations Office at Geneva ICT service constituency comprises 5,000 user accounts. An indeterminate but significant number of public users access the United Nations Office at Geneva website, including substantive data repositories and publications. The duty station has a storage area network and the investment is therefore leveraged in the budget requirement.

20. Site B of this proposal will include protection measures for enterprise applications such as IMIS, e-mail, CTS (treasury), Reality (procurement), Office Wings, Chase insight, Treasury Investment, HIIS, and file servers. Site B under this proposal has the capacity to include protection measures for the United Nations Office at Geneva/Economic Commission for Europe (ECE) main website (www.unece.org) and substantive data repositories such as statistical databases and publications.

United Nations Office at Nairobi

21. The United Nations Office at Nairobi ICT service constituency comprises 2,500 user accounts on average per year, including the United Nations Environment Programme (UNEP) and the United Nations Human Settlements Programme (UN-Habitat). An estimated 12,000 public users access the United Nations Office at Nairobi website per day, including substantive data repositories and publications. The duty station does not have a storage area network and therefore does not adequately cover disaster recovery and business continuity requirements.

22. Site B of this proposal will include protection measures for enterprise applications such as IMIS, e-mail, the Consolidated Treasury System (CTS), the Inventory System, the Resource Management System, the Medical Insurance Plan, the Project Management System and file servers. Site B under this proposal has the capacity to include protection measures for the United Nations Office at Nairobi main website (www.unon.org) and substantive data repositories such as project archives, GIS and publications.

United Nations Office at Vienna

23. The United Nations Office at Vienna ICT service constituency comprises 2,000 user accounts on average per year. An estimated 750 authenticating public users access the United Nations Office at Vienna website, including substantive data repositories and publications. The duty station has a storage area network and the investment is therefore leveraged in the budget requirement.

24. Site B of this proposal will include protection measures for enterprise applications such as IMIS, e-mail, CTS (Treasury), human resources applications, safety and security applications, finance applications, Profi and PowerBuilder applications and file servers. Site B under this proposal has the capacity to include protection measures for the United Nations Office at Vienna main website (www.unov.org) and substantive data repositories such as IDS, NDS, and PowerBuilder and Lotus Notes office automation applications.

Annex II

Previously funded projects

Duty station	*Integrated projects (indicative, not exhaustive)*
United Nations Headquarters	• Backup site in DC2 building, established for scenarios one and two • Storage area network (SAN) and network attached storage (NAS) for local disaster recovery and business continuity requirements • High-availability storage installed • Use of uninterruptible power supply and power generators • Server-clustering in use • Off-site tape facility
United Nations Logistics Base at Brindisi, Italy	• Backup site to Building 261, established for scenarios one and two • Disaster recovery capability established for peacekeeping and political missions • SAN and NAS • E-mail archiving capability • Business continuity to United Nations Headquarters • Use of uninterruptible power supply and power generators • High-availability storage installed
United Nations Office at Geneva	• Backup facility established for scenarios one and two • Partial SAN and NAS installation completed • High-availability storage installed • Use of uninterruptible power supply and power generators • Server-clustering in use • Off-site tape facility
United Nations Office at Vienna	• Backup facility established • Partial SAN and NAS installation completed • High-availability storage installed • Use of uninterruptible power supply and power generators • Server-clustering in use • Off-site tape facility
United Nations Office at Nairobi	• Backup facility established for scenarios one and two • High-availability storage installed • Partial SAN installation complete • Use of uninterruptible power supply and power generators • Server-clustering in use • Off-site tape facility
Economic Commission for Africa (ECA)	• Construction of a new facility with a new data centre is under way • High-availability storage installed • Partial SAN/NAS installation under way • Use of uninterruptible power supply and power generators • Data backup operations on server level exists • Server-clustering partially in evaluation

Duty station	*Integrated projects (indicative, not exhaustive)*
Economic and Social Commission for Asia and the Pacific (ESCAP)	• Backup facility established for scenarios one and two • High-availability storage installed • Use of uninterruptible power supply and power generators • Server-clustering in use • Off-site tape facility
Economic Commission for Latin America and the Caribbean (ECLAC)	• Backup facility established for scenarios one and two for IMIS and Notes • Planning on its way for SAN • High-availability storage installed • Use of uninterruptible power supply and power generators • Server-clustering in use • Off-site tape facility
Economic and Social Commission for Western Asia (ESCWA)	• New data centre being established to cover scenarios one and two • High-availability storage installed • Use of uninterruptible power supply and power generators • Server-clustering in use • Off-site tape facility
International Tribunal for the Former Yugoslavia	• Disaster recovery and business continuity strategy under implementation • Partial SAN and NAS installation established • High-availability storage installed • Use of uninterruptible power supply and power generators • Server-clustering in use
International Court of Justice	• Backup facility established for scenarios one and two • High-availability storage installed • Use of uninterruptible power supply and power generators • Partial NAS installation completed
International Criminal Tribunal for Rwanda	• Backup facility established for scenarios one and two • High-availability storage installed • Use of uninterruptible power supply and power generators • Server-clustering in use
Peacekeeping missions and political missions	• Twenty-five installations connected to the United Nations Logistics Base for file replication • Data replication systems in production • Use of uninterruptible power supply and power generators

Annex III

Current disaster recovery and business continuity arrangements in field missions

Mission	*Distributed data centre (tier 1)*	*In-theatre, off-site (tier 2)*
MINURSO	Yes	No
MINUSTAH	Yes	Yes (Santo Domingo)
MONUC	Yes	Partially operational in Entebbe
ONUB	Yes	No
ONUCI	Yes	No
UNDOF	Yes	No
UNFICYP	Yes	No
UNIFIL	Yes	Yes (Beirut)
UNMEE	Yes	Yes (Addis Ababa)
UNMIK	Yes	Yes (Skopje)
UNMIL	Yes	No
UNMIS	Yes	Partially operational in Entebbe
UNOMIG	Yes	No
UNMIT	Yes	No

Abbreviations: MINURSO, United Nations Mission for the Referendum in Western Sahara; MINUSTAH, United Nations Stabilization Mission in Haiti; MONUC, United Nations Organization Mission in the Democratic Republic of the Congo; ONUB, United Nations Operation in Burundi; ONUCI, United Nations Operation in Côte d’Ivoire; UNDOF, United Nations Disengagement Observer Force; UNFICYP, United Nations Peacekeeping Force in Cyprus; UNIFIL, United Nations Interim Force in Lebanon; UNMEE, United Nations Mission in Ethiopia and Eritrea; UNMIK, United Nations Interim Administration Mission in Kosovo; UNMIL, United Nations Mission in Liberia; UNMIS, United Nations Mission in the Sudan; UNOMIG, United Nations Observer Mission in Georgia; UNMIT, United Nations Integrated Mission in Timor-Leste.