OIOS
Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

RISK ASSESSMENT

Department of Safety and Security (DSS)

20 June 2008
Assignment No. [AH2007/500/01]

United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

INTERNAL AUDIT DIVISION · DIVISION DE L'AUDIT INTERNE

OFFICE OF INTERNAL OVERSIGHT SERVICES · BUREAU DES SERVICES DE CONTRÔLE INTERNE

TO: Mr. David Veness, Under-Secretary-General
A: Department of Safety and Security

DATE: 20 June 2008

REFERENCE: IAD: 08-01440

for
FROM: Dagfinn Knutsen, Director
DE: Internal Audit Division, OIOS

SUBJECT: **Assignment No. AH2007/500/01 - Risk Assessment - Department of Safety and Security (DSS)**
OBJET:

1. I am pleased to present OIOS' risk assessment of the Department of Safety and Security (DSS) which was carried out with the assistance of the consulting services of Deloitte Touche Tohmatsu for your information. While we do not require a formal response to this report, you are welcome to discuss any of the issues raised further.

2. OIOS encourages DSS to use the results of this risk assessment to put in place appropriate risk mitigation measures. OIOS will update the risk assessment periodically, based on subsequent audits or additional information obtained.

3. I take this opportunity to thank the management and staff involved in the risk assessment for the assistance and cooperation provided to the project team in connection with this assignment.

cc: Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Maria Gomez Troncoso, Officer-in-Charge, Joint Inspection Unit Secretariat
Mr. Jonathan Childerley, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Programme Officer, OIOS

INTERNAL AUDIT DIVISION

FUNCTION

"The Office shall, in accordance with the relevant provisions of the Financial Regulations and Rules of the United Nations examine, review and appraise the use of financial resources of the United Nations in order to guarantee the implementation of programmes and legislative mandates, ascertain compliance of programme managers with the financial and administrative regulations and rules, as well as with the approved recommendations of external oversight bodies, undertake management audits, reviews and surveys to improve the structure of the Organization and its responsiveness to the requirements of programmes and legislative mandates, and monitor the effectiveness of the systems of internal control of the Organization" (General Assembly Resolution 48/218 B).

CONTACT INFORMATION

DIRECTOR:
Dagfinn Knutsen, Tel: +1.212.963.5650, Fax: +1.212.963.2185,
e-mail: knutsen2@un.org

DEPUTY DIRECTOR:
Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,
e-mail: ndiaye@un.org

CHIEF, NEW YORK AUDIT SERVICE:
William Petersen: Tel: +1.212.963.3705, Fax: +1.212.963.3388,
e-mail: petersenw@un.org

PARTICIPANTS

The OIOS risk assessment team conducted workshops and interviews with the following staff members of Department of Safety and Security, to gain an understanding of existing organizational relationships, risks, controls and process issues.

Table 1: List of participants

Focus Area	Name and Functional Title
Strategic Management and Governance	• Mr. David Veness, Under-Secretary-General • Ms. Diana Russler, Deputy to the Under-Secretary-General
Financial Management Human Resource Management Procurement and Contract Administration Logistics Management Property and Facilities Management	• Ms. Neeta Tolani, Executive Officer • Mr. Jose Fraga, Budget and Finance Officer • Mr. Mario Cianci, Senior Human Resources Officer
Information Technology Management	• Mr. Gerald Ganz, Chief, Field Support Service • Mr. Andre De Hondt, Information Technology Coordinator • Mr. Moussa Ba, Chief, Critical Incident Stress Management Section
Programme and Project Management	• Mr. Mohammed Bani Faris, Director, Division of Headquarters Safety and Security Services • Mr. Gerard Martinez, Director, Division of Regional Operations • Mr. David Bongi, Senior Operations Officer • Mr. Bruno Henn, Chief, Headquarters Safety and Security – New York • Mr. Joseph Martella, First Officer • Mr. Andrew Rigg, Security Coordination Officer • Mr. Prinsloo Barend, Security Coordination Officer • Ms. Corinne Heraud, Officer-in-Charge, Asia and Pacific Section • Mr. Chris Maxfield, Chief, Europe and Americas Section • Mr. Nicolas Morin, Officer-in-Charge, West Africa Section • Mr. Abraham Mathai, Chief, Middle East Section • Mr. John Logan, Chief, Compliance,

Focus Area	Name and Functional Title
	Evaluation and Monitoring Unit • Mr. Richard Floyer-Acland, Chief, Policy, Planning and Coordination Unit • Mr. Igor Mitrokhin, Chief, Threat and Risk Assessment Unit • Mr. William Phillips, Chief, Peacekeeping Operations Support Service

SUMMARY OF RISK RATINGS

The risk assessment identified the following areas as Higher, Moderate and Lower Risk. A summary of the identified risks is shown below. Full details of the identified risks are listed in the attached risk register.

The overall risks have been rated as "higher risk", "moderate risk", or "lower risk" based on OIOS' assessment of the likelihood and impact of the occurrence of events or actions that might adversely affect the Organization's ability to successfully achieve its objectives and execute its strategies, after taking into account the representations made by programme managers concerning actions they have taken to prevent or mitigate the identified risks.

Table 2: Summary of identified risks

Focus Area	Overall Risk
i. Strategic Management and Governance ii. Financial Management iii. Human Resources Management iv. Procurement Management v. Information Technology Management vi. Program and Project Management	**Higher Risk**
i. ii. iii. iv. v.	**Moderate Risk**
i. ii. iii. iv. v.	**Lower Risk**

RISK REGISTER

Risk Assessment of : Department of Safety and Security

1	Focus Area:	Strategic Management and Governance		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
I	**Mandate and Environment**			Likely	High	Higher Risk
	A(i) Lack of clear mandate makes it difficult for the Department of Safety and Security (DSS) to define its strategy, goals and objectives, and resource requirements and to measure its performance and meet the expectations of stakeholders/clients.	DSS communicates with stakeholders/clients at all levels and through different channels such as the General Assembly, the Inter-Agency Security Management Network (IASMN), the High Level Committee on Management (HLCM) and the Chief Executives Board (CEB) to clarify its mandate and what it can deliver given the resources level.	Strategy	Likely	High	Higher Risk
	A(ii) Lack of a Secretary General's Bulletin (SGB) to formally define and communicate the mandate, structure, roles and responsibilities of DSS and its organizational units may lead to confusion, overlaps and clashes among the functions.	DSS is in the process of drafting and revising an SGB on the subject.				
	A(iii) Not being perceived as a neutral organization coupled with more active terrorism activities may expose the United Nations (UN) staff, premises and property to ever-increasing security risks.					

1	Focus Area:	Strategic Management and Governance		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
II	**Organizational Design**			Likely	High	Higher Risk
	B(i) Inadequate authority by the Secretary General to hold the executive heads accountable, may lead to continued segmentation and even breakdown of the United Nations Security Management System, which is led by the United Nations through DSS and participated in by the AFPs. B(ii) Inadequate authority by DSS over the Designated Officials and Security Management Team (SMT), which consists of members from the participating AFPs, may lead to inadequate consideration of reasonable security advice from DSS and potential disfunction of the system. B(iii) Inadequate authority by the Designated Official (DO) over the representatives of the other Agencies, Funds and Programmes (AFPs) , who are members of the Security Management System, may lead to dysfunction of the system.	The Framework for Accountability provides the Secretary General, the Under-Secretary-General (USG) of DSS, the Designated Officials (DO) and the (Chief) Security Advisers (CSA) a certain degree of authority but is of limited use to discharge their repsonsibilities.	Governance	Likely	High	Higher Risk

1	Focus Area:	Strategic Management and Governance		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	B(iv) Inadequate authority by the (Chief) Security Adviser (CSA) over the security officers of the other AFPs, as well as Secretariat departments such as Department of Peacekeeping Operations (DPKO) and Department of Field Support (DFS), who are members of the Security Cell, may lead to dysfunction of the system. B(v) The dual reporting lines of the Security Advisers to both the Designated Officials and DSS may compromise their capacity as an independent security professional.	The Framework for Accountability and other security policies and procedures are supposed to be followed by all the security professionals of the participating entities. The 250 international security professionals administered by the United Nations Development Program (UNDP) are all recruited using standard job descriptions issued by DSS, interviewed by DSS officials, and controlled by DSS in terms of providing daily operational/technical guidance, promotion, mobility, etc. DSS also contributes to the performance appraisals by giving balancing comments to ensure that the security advisers are doing their job.	Governance	Likely	Medium	Higher Risk

1	Focus Area:	Strategic Management and Governance		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	B(vi) Lack of clarity on the roles and responsibilities and reporting lines of some critical security officials weakens chain of command and leads to organizational clashes. B(vii) Potential overlap of functions between DSS and other Secretariat entities may lead to waste of resources and organizational tensions.	DHSSS is redrafting the document "Lines of Reporting, Responsibilities and Administrative Arrangements for Security and Safety Services at offices away from Headquarters and Regional Commissions" to clarify the responsibilities and reporting lines. DSS is coordinating with other departments such as OHRM and UN Medical Services to draw the lines of responsibilities for similar functions. DSS plans to consolidate existing resources tasked with crisis management into a single Crisis Management Unit. Following a recent audit by OIOS, DSS has agreed to re-evaluate its internal structure and rationalize it.	Governance	Likely	Medium	Higher Risk
	E(i) Lack of a unified policy on disciplinary action for non-compliance with security policies and procedures or consistent enforcement of such a policy after it is promulgated, weakens accountability in the whole UN security management system. E(ii) The conflicting roles of the DOs as both a program manager and an officer in charge of security may result in security being relegated to secondary importance and expose staff to excessive risks.	Following an audit of DSS by OIOS, DSS plans to initiate the development of a policy on disciplinary action for non-compliance with security policies and procedures. DSS launched customized induction programs and refreshment training programs to ensure that security is given adequate priority by the DOs.	Operational	Likely	Medium	Higher Risk

1	Focus Area:	Strategic Management and Governance		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
III	**Organizational Culture**			Possible	High	Higher Risk
	A(i) Lack of safety and security awareness by the security officials and staff in general results in disregard of DSS personnel and their advice and non-compliance with security policies and procedures, exposing UN staff and property to security risks that could be otherwise mitigated.	DSS has designed training programmess targeted at different audiences to boost safety and security awareness.	Strategy	Possible	High	Higher Risk
	A(ii) Failure to achieve the right balance between program delivery and security management may either prevent UN programs from achieving their mandates or expose UN staff, premises and property to excessive security risks.	Some AFPs, for example, the World Health Organization (WHO), try to achieve the right balance by factoring security costs into the program budget, i.e., a certain percentage of the program budget should be allocated to security.				
	A(iii) Inadequate attention to safety compared to security may expose UN staff, premises and property to excessive safety risks.	DSS has initiated safe driving and fire safety programs, although such programmes are a lower priority than security.				
	A(iv) Lack of a client/field-focus by DSS Management may lead to inadequate support or priority given to the field security to cope with the risks there.					
	B(i) Lack of a one-UN mindset by vested interests coupled with a residual silo structure of DSS may lead to difficulties in integrating the UN security management system and hence potential overlaps and loopholes continue to exist in the system.	The setup of DSS and the functioning of the whole UN security management system under the Framework for Accountability partially mitigate the risk. And DSS is constantly trying to further integrate the system through communication, collaboration with other stakeholders and is developing policies and procedures to be used by the whole system.	Governance	Possible	Medium	Moderate Risk
	E(i) Security decisions/advices may be overruled due to political reasons, given the political environment UN is facing.		Operational	Possible	High	Higher Risk

1	Focus Area:	Strategic Management and Governance		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
IV	Governance (IASMN)			Likely	High	Higher Risk
	B(i) Lack of clarity over the membership status of the IASMN, the governing body of the UN security management system as authorized by the High Level Committee on Management, may lead to non-cooperation by critical members and ultimately continued fragmentation of the security management system. B(ii) Lack of clarity over the scope of authority of the IASMN may lead to resistance to and non-compliance with the policies promulgated by it and approved by the HLCM/CEM. B(iii) Inability of the IASMN to fairly and adequately reflect the needs of each of its members in its policy-review and decision-making process may lead to non-cooperation or resistance by some of its members, weakening the whole system and exposing UN staff to excessive security risks.	IASMN is in a transitional stage to become the governing body for Safety and Security Service (SSS), an organizational unit of DSS that provides safety and security services to the UN system at Headquarters, duty stations and regional commissions.	Governance	Likely	High	Higher Risk
	E(i) Lack of effectiveness and efficiency in the decision-making process of IASMN may result in policies not being developed, reviewed and promulgated in a timely manner.	As a partial mitigating measure, the Steering Group of IASMN, consisting of 10 major members and chaired by DSS, can review the policy documents and provide their comments and inputs in lieu of the whole IASMN.	Operational	Possible	High	Higher Risk
V	Policies and Procedures			Possible	Medium	Moderate Risk
	A(i) Lack of an overarching security policy to integrate the UN security management system contributes to resistance to and non-compliance with current security policies and procedures.	DSS has started to revise the original Field Security Handbook by changing its name and its content to focus on generic security guidelines/principles applicable and enforceable at all locations.	Strategy	Possible	Medium	Moderate Risk
	E(i) Lack of a clear policy structure may lead to confusion by the users of the security policies and potential non-compliance.	DSS is revising the policies so that policies will be separated from operating procedures.	Operational	Possible	Medium	Moderate Risk

1	Focus Area:	Strategic Management and Governance		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
VI	**Overall Distribution of Resources**			Possible	High	Higher Risk
	E(i) Lack of a consistent model/methodology to assess and allocate DSS resources across the duty stations and field locations to reflect their relative risk profile may lead to inefficient use of limited resources, i.e., residual risk level may be significantly different across the duty stations and field locations given the resources allocated to each of them.	DSS has agreed to re-assess its structure and resource allocation in response to a recent OIOS audit.	Operational	Possible	High	Higher Risk
VII	**Relationship with Stakeholders**			Likely	High	Higher Risk
	A(i) The required support from the host governments for the protection of UN staff, property and premises, in light of their primary responsibilities in this regard, may not materialize due to lack of effective legal instruments, for instance, robust host government agreements with updated security clauses.	DOs and CSAs in the field are interacting and establishing relationships with the host countries. However, this alone appears to be inadequate.	Strategy	Likely	High	Higher Risk
	B(i) Lack of security focal points from some Secretariat departments prevents active involvement and dialogue with DSS and IASMN on security issues.	The risk is limited because these departments, e.g. the Department of Economic and Social Affairs (DESA), have very limited field presence.	Governance	Possible	Medium	Moderate Risk
	E(i) Lack of general support and cooperation, for instance, sharing of information on security, from Member States at large may expose the UN staff, premises and property to security risks that could be otherwise mitigated.	DSS management is trying to advise and lobby the Member States on this issue through communication through different channels: permanent missions, regional organizations and bilateral relationships at the country level. DSS is trying to leverage all other channels available, i.e., through the Security Council, Policy Committee, CEB and HLCM, etc.	Operational	Possible	High	Higher Risk

Risk Assessment of : Department of Safety and Security

2	Focus Area:	Financial Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
I	Funding			Likely	High	Higher Risk
	D(i) Lack of additional funding from the participating agencies, funds and programs through the cost-sharing mechanism will prohibit DSS from obtaining the necessary resources to strengthen the security system in the field. D(ii) Dependency on extra-budgetary funding for some core programs may result in discontinuity of the programs. D(iii) Dissatisfaction of key clients with the current security management system, which is under DSS leadership, may lead to their refusal to pay their dues, cutbacks in funding, or even complete withdrawal from the system, and hence significantly weaken the system.	As a partial mitigating measure, DSS has to constantly mobilize resources from other countries to crisis zones, leaving other countries vulnerable. The system relies on the continuous negotiation and lobbying efforts to ensure that the AFPs will continue to cooperate and pay their dues on time.	Financial	Possible	High	Higher Risk
	E(i) Lack of operability of the cost-sharing mechanism may prolong the budgeting process and prevent DSS from purchasing necessary security equipment in a timely manner.		Operational	Likely	Medium	Higher Risk

2	Focus Area:	Financial Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
II	**Expenses and Resources Management**			Possible	Medium	**Moderate Risk**
	D(i) Travel and other expenses may not be properly managed resulting in waste of resources or over-expenditure. D(ii) Lack of research on and use of more cost-effective alternatives in delivering admistrative services to DSS personnel in the field may lead to the continous incurrence of higher costs. D(iii) Lack of direct control over DSS funds in the field paid to UNDP, which are pooled together with other UNDP resources, to provide administrative services to DSS personnel, may impact the security operations in the field and add to difficulties in reconciling the accounts.	Expenses are monitored before being incurred and input into IMIS. The Executive Office (EO) trained the whole DSS on travel policy and travel plans are strictly scrutinized. DSS is assessing the possibility of taking over the management and administration service provided by UNDP Copenhagen Office. However due to limited field presence, DSS believes that they will continue to rely on UNDP for administrative service in the field.	Financial	Possible	Medium	**Moderate Risk**
III	**Management of Contract with UNDP**			**Possible**	**Medium**	**Moderate Risk**
	D(i) Inadequate management of the contract with UNDP may lead to financial information not being accurately and timely captured, processed, classified and reported, and services delivered not being in line with the contract.	The Finance Officer in the DSS Executive Office performs monthly reconciliation of accounts payables with UNDP.	Operational	Possible	Medium	**Moderate Risk**

Risk Assessment of : Department of Safety and Security

3	Focus Area:	Human Resource Management		Likely	Medium	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
I	**Recruitment**			Likely	High	Higher Risk
	F(i) Lack of robust recruitment process may result in recruitment of unqualified staff for field locations.	Mitigating controls: scrutiny of resume, panel interview, 3 weeks Security Certification Program (SCP), which is used both as a training program and a screening process, but the effectiveness of SCP is weakened because DSS is recruiting less people now and it is difficult to organize batches of candidates to attend the training.	Human Resources	Likely	High	Higher Risk
	F(ii) Inability to adapt the general UN recruitment process for the needs of DSS to recruit SSS personnel.	SSS has designed more steps to screen candidates, i.e. drug testing, psychological testing and weapon use testing.				
	F(iii) Rendering technical requirements to achieve other recruitment goals such as gender balance and equity in geographical distribution may result in lengthy recruitment process and/or recruitment of staff members who do not have the right level of experience.	All the new security professionals are supposed to receive the same 3-week induction training in Turin.				
	F(iv) Lack of harmonization of contractual conditions despite human resources management reform may impede the redeployment of security personnel between duty stations and compromises staff morale.	DSS anticipates that human resource management reforms will partially resolve the current impediments of redeployment. Following a recent audit by OIOS, DSS plans to further assess the situation and take actions to harmonize the contract conditions.				

3	Focus Area:	Human Resource Management		Likely	Medium	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	F(v) Inconsistent recruitment standards may result in offering same grades to candidates with disparate experience levels, recruitment of underqualified personnel and potential dissatisfaction of staff members. F(vi) Incomplete background checks of security personnel may lead to recruitment of unqualified security personnel and create additonal security risk since security personnel are possibly armed and have unrestricted access. F(vii) Inadequate background checks for personnel employed through 3rd party contractors may expose UN staff and properties to security risks.	Following a recent audit by OIOS, DSS plans to initiate the harmonization of recruitment standards, and will take the lead in proposing a modified package of background checks to the IASMN.	Human Resources	Likely	High	Higher Risk
	D(i) Lack of additional funding from the participating agencies, funds and programs through the cost-sharing mechanism will prohibit DSS from obtaining the necessary resources to strengthen the security system in the field.	As a partial mitigating measure, DSS has to constantly mobilize resources from other countries to crisis zones, leaving other countries vulnerable.	Financial	Possible	High	Higher Risk
II	**Performance and Career Management**			Possible	Medium	Moderate Risk
	F(i) Ineffective performance appraisals may lead to a disconnection between real performance and performance ratings, continuation of sub-standard performance of security personnel, implying that security risks are not adequately detected and mitigated. F(ii) Incomplete career profile of security personnel prevents development and implementation of an effective recruitment strategy and career management of the security personnel.	The performance appraisal of the Security Advisers (SA) are conducted by their first reporting officers, i.e., the DO, using the UNDP PCA system. DSS provides comments as secondary reporting officer to balance the appraisal. DSS is in the process of developing a new profile for security personnel at all levels.	Human Resources	Possible	Medium	Moderate Risk

Risk Assessment of : Department of Safety and Security

4	Focus Area:	Procurement and Contract Administration		Likely	Medium	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
I	**Procurement**			Likely	Medium	Higher Risk
	E(i) Procurement may be managed in a fragmented manner leading to loss of economy of scale, poor standardization and difficulty in managing the assets procured. E(ii) Lack of a policy to clearly define the roles and responsibilities regarding the technical verification and inspection of security equipment and associated vendors by DSS may lead to purchase of defective equipment. E(iii) Lack of capability by DSS to perform technical verification of the vendors/equipment may lead to purchase of defective equipment. E(iv) Lengthy procurement process may compromise DSS operations and expose UN staff, premises and property to security risks that could be otherwise mitigated. E(v) Failure to maintain confidentiality of travel information by the external vendor(s) may lead to leak of confidential information and expose traveling staff to security risks.	Currently there is a centralized procurement center in Dubai for DSS equipment used in field locations. Procurement for SSS in New York and offices away from HQ is managed locally. The general contract conditions contain a confidentiality clause.	Operational	Likely	Medium	Higher Risk

Risk Assessment of : Department of Safety and Security

6	Focus Area:	Information Technology Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
I	**Information Management**			Likely	High	Higher Risk
	A(i) Information and Communication Technology (ICT) management decisions may not follow the department's strategic goals and direction due to insufficient funding.		Strategy	Possible	High	Higher Risk
	B(i) Inadequate support for the ICT infrastructure and applications may lead to failure of alternative decision-making processes.		Governance	Possible	High	Higher Risk
	D(i) Inadequate funding of the ICT strategy may lead to DSS's mission not being supported by its ICT resources.		Financial	Possible	High	Higher Risk
	E(i) Lack of a common understanding of DSS's ICT priorities may lead to conflicts about allocation of resources and priorities.		Operational	Possible	Medium	Moderate Risk
	F(i) Inadequate resources for IT exposes DSS to the risk of: a) ICT services not supported adequately. b) Inability to provide 24/7 assistance to field office locations.	The Information Management Coordinator, the only dedicated IT staff member, is supported by two external contractors for the management of departmental databases.	Human Resources	Likely	High	Higher Risk
	G(i) Inadequate support for the ICT infrastructure and applications exposes DSS to the following potential risks: a) Inability to recover data and applications in a manner which meets the Organization's needs. b) Inability to maintain consistent data. c) Inability to ensure adequate solutions for the protection, business continuity, and disaster recovery of all critical data.		Information Resources	Possible	High	Higher Risk

Risk Assessment of : Department of Safety and Security

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
I	**Regional Desks**			Likely	Medium	Higher Risk
	B(i) Lack of commensurate authority by the regional desks may prevent them from fulfilling their expected accountability and responsibilities, which are not clearly defined in the Framework for Accountability.		Governance	Possible	Medium	Moderate Risk
	E(i) Lack of direct control over DSS personnel in the field, who report to the DOs as their first reporting officer and are holding UNDP contracts for administrative convenience, weakens the whole chain of command and accountability.	The 250 international security professionals administered by the United Nations Development Program (UNDP) are all recruited using standard job descriptions issued by DSS, interviewed by DSS officials, and controlled by DSS in terms of providing daily operational/technical guidance, promotion, mobility, etc. DSS also contributes to the performance appraisals by giving balancing comments to ensure that the security advisers are doing their job.	Operational	Likely	Medium	Higher Risk
	E(ii) The regional desks and other DSS units may be unable to provide timely guidance and support to the field security operations because of the long distance to most of the field locations and time differences.	As partial mitigating measures, advanced technology is used to facilitate communications, and the communication center is operating on a 24X7 basis.				

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	F(i) Lack of field experience may compromise credibility of HQ desks officers and prevent them from providing proper advice and support to the field security officers. F(ii) Heavy administrative burden on the Security Advisers may result in their inability to focus on regular security duties, impacting the security operations in the field. F(iii) Inability to attract and retain security personnel with UN field security experiece compromises the authority and operations of the regional desks.	Each new desk officer is supposed to go through the 3-week Security Certification Program (SCP) held in Turin as the field security advisers do. However, this is not consistently delivered. As a mitigating control, DSS is researching the possibility of assigning two or three personnel to take over that burden.	Human Resources	Likely	Medium	Higher Risk

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
II	Security Management in the Field Locations			Possible	High	Higher Risk
	B(i) Lack of adequate skills/knowledge by the officials with security responsibilities and lack of awareness of their safety and security responsibilities weakens the security management system in the field locations. B(ii) Inadequate coordination on security management among all the entities present in the same location, who are members of the UN security management system, may expose UN staff, premises and property to excessive security risks that could be otherwise mitigated.	DSS has rolled out training programs to these key players, but the coverage is not ideal due to a number of reasons (Refer to HR Section). DSS also believes that careful selection of the DOs will serve as a partial mitigating control. 1) The Framework for Accountability approved by the General Assembly provides responsibilities of each key player. 2) All the security professionals from each entity are supposed to follow the common set of policies and procedures enacted by DSS and endorsed by the IASMN. 3) In large missions, a security cell is also in place, under the leadership of the CSA, coordinating on safety and security issues. 4) The SMT meets on regular basis with active attendance from the members and meeting minutes are kept for most of the field locations.	Governance	Possible	High	Higher Risk

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	E(i) Ineffective security threat and risk assessment may compromise the quality and relevance of the security plan developed on the basis of the risk assessement, and hence of the security arrangements put in place.	1) Risk assessments are reviewed by SMT and DO. 2) Risk assessments are reviewed by the desk officers under the Regional Desks. 3) Training (involving the Threat and Risk Assessment Unit), not just training of the SAs, but also the DOs and SMT members.	Operational	Possible	High	Higher Risk
	E(ii) Lack of an effective warden system, which serves as the last mile in the UN security management system in the field, exposes staff and dependents to hightened risks in crises.	Wardens are appointed and training is provided to them in many locations.				
	E(iii) UN personnel may go to locations which are not security-cleared or which have movement restrictions, exposing them to safety and security risks.	Security clearance procedures are in place to monitor the movement of staff members and regulate their movements, in line with the prevailing situation.				
	E(iv) Placing increased reliance on local staff for critical tasks without providing adequate security coverage to them may expose both the local staff and international staff to undue risks.					
	G(i) Lack of effective and fully functional channels and equipment to timely communicate security information may expose staff to hightened risks in crises.	Generally, field security personnel and vehicles are equipped with communication equipment such as radio systems in the field locations, but they are not always tested regularly to ensure the functioning of the radio communication systems and the capability of the staff to use them.	Information Resources	Possible	High	Higher Risk
	G(ii) Lack of updated staff and dependents information may expose staff and dependents to hightened risks in crises because the staff may not be able to be contacted.	An integrated system to track the movements of staff and dependents is used at some locations but not consistently.				

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	F(i) Prolonged high vacancy rate in the Security Section at some field locations may lead to inadequate security coverage.	At some locations, a vacancy rate over 20% lasts for an extended period. HR sections in these missions are working actively to fill the gap.	Human Resources	Likely	Medium	Higher Risk

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli- hood	Impact	Overall Risk
III	**Peacekeeping Operations Support Services (POSS)**			Possible	High	Higher Risk
	A(i) Lack of policy basis to ensure coverage of the uniformed personnel in DPKO missions by the UN security system may expose them to excessive security risks that could be otherwise mitigated.	Currently DSS is developing a policy to cover such individual uniformed personnel.	Strategy	Possible	Medium	**Moderate Risk**
	B(i) Inability to maintain a good working relationship with DPKO may lead to breakdown of the critical relationship and prevent POSS from achieving its mandate. B(ii) Inability to maintain good working relationships with the AFPs may lead to inadequate coordination between the participants of the security management system.	1) A Cooperation and Coordination Framework between DPKO (now includes DFS) and DSS was developed. 2) A Standing Committee, consisting of 3 USGs from DPKO, DFS and DSS, meets regularly to discuss critical issues. 3) POSS maintains a good working relationship with DPKO. Apart from the inherent problems of the IASMN, POSS coordinates closely with the AFPs in the integrated missions for security purposes.	Governance	Remote	High	**Moderate Risk**
	F(i) Inadequate training and education of the mission-appointed personnel may lead to security risks not being adequately monitored and mitigated.	The Training Section under the Field Support Service has developed training program for the mission-appointed security personnel and DSS has the capacity to perform the training but due to the cost sharing system this initiative has to be supported by the AFPs. As a temporary solution POSS used 6 staff from DHSSS to provide the training.	Human Resources	Possible	Medium	**Moderate Risk**

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
IV	**Threat and Risk Assessment Unit (TRAU)**			Possible	Medium	**Moderate Risk**
	E(i) The Security Risk Management Model (SRMM) may not be developed properly or updated timely to respond to the changes in the environment, leading to inaccurate risk assessments. E(ii) Lack of adequate validation of the risk assessments to ensure relevance and validity may compromise the realibility of the conclusions and recommendations. E(iii) Recommendations of the Risk Assessments may not be effectively and timely implemented, leading to security risks identified not being properly managed. E(iv) Lack of policies or criteria to prioritize risk assessment requests, given the limited capacity of TRAU, may lead to critical assessments not performed timely or adequately.	This model was recommended by IASMN and endorsed by CEB in 2004 (CEB/2004/6). Member states were broadly consulted on their models during the development process of the model. The model itself contains a mechanism to be reviewed and updated periodically. TRAU has developed internal procedures and mechanisms to ensure vigorous internal validation. Regional Desks and SSS oversee the development of security plans (including operational plans for close protection) based on the risk assessments.	Operational	Possible	Medium	**Moderate Risk**
	F(i) Inadequate coaching of the security advisers who are charged to perform risk assessments for the specific countries could result in low quality of risk assessments in the field and the security plans developed on the basis of such assessments.	1) TRAU works in collaboration with DSS regional desks and security officers deployed to over 150 countries. It is ensured through training that everyone speaks the same language and uses the same methodology. 2) It also invites Security Officers from other duty stations to work with it in New York to bring them up to speed to be able to develop their risk assessments. 3) The Unit provides support to the Regional Desks in the review of the most complex assessments.	Human Resources	Possible	Medium	**Moderate Risk**

7	**Focus Area:**	**Programme and Project Management**		Likely	High	**Higher Risk**
No	**Interview/Review Summary (Description of risk)**	**OIOS Assessment**	**Risk Category**	**Likeli-hood**	**Impact**	**Overall Risk**
	G(i) Lack of reliable and complete information input provided to TRAU to enable valid risk assessments may result in unreliable conclusions and recommendations.	The unit validates the information once it is received. Guidelines and procedures were developed for validating the information.	Information Resources	Possible	Medium	**Moderate Risk**
V	**Headquarters Security and Safety Services (DHSSS)**			Possible	High	**Higher Risk**
	B(i) Inability to manage a sound relationship with key stakeholders, especially the local administration at each duty station and regional commission, could compromise the management and operations of SSS.	DHSSS is revising the Reporting Lines document to partially address the issue.	Governance	Possible	High	**Higher Risk**
	E(i) Lack of divisional policies and procedures may result in operational confusions and difficulties in addressing the safety and security risks.	Currently, DHSSS is coordinating with the Policy Unit and SSS at different locations to fill the gap: recently completed policies such as Firearm related policies and other in-progress polices such as Policy on Conferences and Large Meetings Held away from Headquarters.	Operational	Possible	High	**Higher Risk**
	E(ii) Lack of policy basis for which officials should receive close protection may lead to escalated cost for close protection or leave certain officials exposed to risks.	As a rule of thumb, the SRSGs who are assigned to new missions and executive heads traveling to high-risk locations are protected.				
	E(iii) Inadequate access control to the premises may lead to entry/penetration by terrorists.	DHSSS is implementing an Access Control Project to strengthen access control at the Headquarters and main duty stations and two criminal tribunals.				

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	F(i) Lack of resources to support the Chief of Safety and Security to discharge his/her responsibilities as the Chief Security Adviser (CSA) may compromise his/her work as the Chief of Safety and Security.	As a temporary mitigating measure, DHSSS mobilizes the chiefs to cover each other in crisis situations. For instance, the Chief of SSS in New York was assigned to temporarily replace his counterpart in UNON during the crisis in Kenya while the latter was serving his CSA role.	Human Resources	Possible	High	Higher Risk
	F(ii) Lack of training of security personnel to perform risk assessment for close protection may endanger the traveling officials.	Normally, the TRAU assesses the specific risks associated with the profile of the traveling official and the local security personnel only need to customize that assessment according to the local environment of the destination and develops an Operational Plan based on that.				
VI	**Policy, Planning and Coordination Unit**			Possible	Medium	Moderate Risk
	E(i) Lack of coordination and cooperation with other actors in the United Nations Security Management System to identify policy gaps and develop policies in a systematic and expeditious way.	The Policy, Planning and Coordination Unit coordinates with all other main actors in the United Nations security management system, including DSS divisions, units and sections, Agencies, Funds and Programs, and IASMN, to identify the policy gaps, prioritize policy development initiatives, and set up the taskforce to develop the policies.	Operational	Possible	Medium	**Moderate Risk**

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
VII	**Compliance, Evaluation and Monitoring Unit**			Possible	Medium	**Moderate Risk**
	E(i) Lack of a consistent methodology to identify and select locations/missions to visit for a compliance assessment by considering the need/risk level may lead to suboptimal use of limited resources and high-risk areas not being visited.	The Compliance Unit relies on the Division of Regional Operations (DRO) for input on which locations to visit. The Regional Desks are constantly monitoring the developments in the field and they visit field locations to do inspections as well.	Operational	Possible	Medium	**Moderate Risk**
	E(ii) Check list or assessment programs may not be developed in a way to ensure adequate coverage and depth.	Protocols were developed on a basis for all applicable security policies and procedures, and was validated with DRO. The assessment was not purely interview-based and verifications were performed.				
	E(iii) The results may not be communicated effectively to the right audience and do not receive the adequate attention, resulting in inadequate attention to and action on findings and recommendations.	Compliance report is issued to the desk officers of DRO, security advisers in the field and senior management of DSS.				
	E(iv) Recommendations of the compliance assessment reports are not implemented timely and effectively, leading to loopholes and weaknesses in the security management system not properly addressed.	Desk Officers from DRO oversee the development of action plans and implementation.				
	E(v) Implementation of recommendations may not be adequately monitored and followed-up, resulting in loopholes and weaknesses in the security management system not properly addressed.	Currently the Unit is relying on the Desk Officiers to follow up on the implementation of the recommendations. Meanwhile, DSS is designing a software to track the implementation status of the recommendations. It is developing a tool for self assessment as well.				

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
VIII	**Training and Development Section**			Likely	Low	Moderate Risk
	E(i) Inadequate monitoring of the effectiveness of training delivered to the security personnel by training units other than the Training and Development Section may lead to ineffective training not being identified and addressed.		Operational	Likely	Low	Moderate Risk
IX	**Standard Access Control Project (PAC)**			Likely	High	Higher Risk
	B(i) Inadequate consultation may be conducted with stakeholders at different duty stations during the planning stage which leads to inadequate buy-in and cooperation of stakeholders.	According to the Secretary-General's report A/61/566 (titled Strengthened and Unified Security Management for the United Nations: Standardized Access Control), during 2005, DSS, through a team of experts, undertook a comprehensive assessment of the security position at each of the eight main locations of the Secretariat and the two Tribunals. However, OIOS was apprised of information that contradicts this assertion.	Governance	Possible	Medium	Moderate Risk

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	A(i) Lack of clarity on the Headquarters Minimum Operating Security Standards (H-MOSS), which are being revised and consolidated, may result in: 1) goals of the project not being properly defined and open to interpretation; 2) difficulties in measuring achievement of the project; 3) signficant investments being shifted to the 2nd phase of the project.	According to the Secretary-General's report A/61/566, an independent assessment was conducted of the technical soundness and cost-effectiveness of the proposed access control system. The assessment reviewed the proposals with regard to the objectives of the H-MOSS and concluded that the proposed security improvements were fully compliant with those standards. However, OIOS was apprised of information that contradicts this conclusion.	Strategy	Likely	High	Higher Risk
	A(ii) Inadequate assessment may be performed to identify the gap between the current security level and the Headquarters Minimum Operating Security Standards (HMOSS) at each duty station which would result in: 1) full account was not taken of lessons/best practices at other duty stations; 2) key weaknesses in terms of access control were not covered; 3) inadequate consideration and utilization of the investments made through previous projects to improve security; 4) inconsistent levels of compliance with the HMOSS when the first phase is completed.	According to the Secretary-General's report A/61/566, during 2005, DSS, through a team of experts, undertook a comprehensive assessment of the security position at each of the eight main locations of the Secretariat and the two Tribunals and it was concluded that there was no redundant or overly elaborate projects in excess of requirements, as determined by local conditions. However, OIOS' assessment has identified contradictory information from some duty stations.				

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	D(i) Budgeting and cost-benefit analysis for the project may not be performed in a systematic and sufficient manner, resulting in inefficient and ineffective utilization of resources.		Financial	Likely	High	Higher Risk
	D(ii) Inadequate consideration of key elements of cost when budget was done may lead to compromised functionality of the systems when the first phase is completed and hence escalation of costs in the second phase.	The current budget does not include the cost for additional personnel to operate the systems and cost of maintenance. The latter can be covered by warranty in the initial period. The maintenance cost will be budgeted in the second phase and that has been communicated to the Fifth Committee.				

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	E(i) Inadequate support may be provided to the local project teams at different duty stations in terms of technical advice, security standards, system design and procurement, leading to delay in implementation or sub-standard implementation.	Although it has been mentioned in the Secretary General's report A/61/566 that "DSS would provide local managers with technical advice on a case-by-case basis and propose appropriate security standards to them, thereby avoiding unnecessary delays in the implementation of projects already under way", the support provided was not sufficient based on representation of the local duty stations.	Operational	Possible	High	Higher Risk
	E(ii) Poor project implementation, including management of procurement activities, could result in significant delays and cost overruns.	Basic project management structure and milestones have been set up. Progress is monitored. However, delays in implementation have been reported.				
	E(iii) Lack of policies to ensure operability of the access control systems, procedural controls to complement the systems and appropriate protection of confidential information, may lead to undetected perimeter intrusion and improper use/leak of confidential information.	The report of the Secretary-General on an information and communications technology strategy (A/57/620) and the Secretary-General's bulletin on the use of information and communications technology resources and data (ST/SGB/2004/15) make specific provisions for the security of the system and the safeguarding of sensitive information.				

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
	G(i) Inability of the access control system to be expanded and upgraded in the future to reflect the evolving threats and risks facing the duty stations may result in need for re-investment. G(ii) Lack of ability to be integrated and compatible with other UN projects/systems will result in compromised functionality of the access control system and waste of resources due to repetitive investment.	According to the Secretary-General's report A/61/566, the flexibility of the core system allows for system expansion as the need arises where additional layers of protection may be identified as being necessary and the appropriate security hardware installed cost-effectively. Future security enhancements can therefore be implemented incrementally. According to the Secretary-General's report A/61/566 and the PACT, this issue has been fully considered and managed: DSS coordinates with the Department of Management to ensure that the access control project will be in line with overall United Nations Information Technology Strategy. Integration with that evolving strategy in connection with reform initiatives will also be taken into consideration throughout the life cycle of the project.	Information Resources	Possible	Medium	Moderate Risk

7	Focus Area:	Programme and Project Management		Likely	High	Higher Risk
No	Interview/Review Summary (Description of risk)	OIOS Assessment	Risk Category	Likeli-hood	Impact	Overall Risk
X	**Minimum Operating Security Standards and Minimum Operating Resident Security Standards (MOSS and MORSS)**			Likely	High	Higher Risk
	C(i) Lack of clarity regarding the applicability of H-MOSS, MOSS and MORSS may result in difficulties in implementing the standards and non-compliance with them.	The IASMN has made a decision in May 2006 that the issue should be addressed by integrating the MOSS documents into one comprehensive DSS MOSS and DSS is in a process of revising and consolidating the standards.	Compliance	Likely	High	Higher Risk
	E(i) Office or resident buildings used by the UN may not be adequately vetted from a security perspective to ensure they comply with the minimum safety and security standards before they are occupied.		Operational	Likely	High	Higher Risk
XI	**Security Plans**			Likely	High	Higher Risk
	E(i) Lack of current, country-specific and well-tested security plans may increase the security exposure of United Nations operations and staff.	In general, country security plans exist and are being updated, and also reviewed by the desk officers based at Headquarters. Rehearsal of the plans are conducted at some locations.	Operational	Possible	High	Higher Risk
XII	**Crisis Management**			Possible	High	Higher Risk
	E(i) Lack of a clearly-defined strategy, policies and procedures, and resources to manage crises, may expose the UN to prolonged crises and incur more losses that could have been avoided.	DSS is trying to set up the proposed security management unit by consolidating all existing resources.	Operational	Possible	High	Higher Risk

Focus Areas

Focus areas are the key standard processes that are typically found in United Nations operations. These are categories established by the risk assessment framework to facilitate understanding and communicating common processes or functions within the Organization (common language). They are based on a categorization of objectives, using a hierarchy that begins with high-level objectives and then cascades down to objectives relevant to organizational units, functions, or business processes. The IAD risk assessment framework has identified eleven focus areas as follows:

1 Strategic Management and Governance
2 Financial Management
3 Human Resources Management
4 Procurement and Contract Administration
5 Logistics Management
6 Information Technology Management
7 Programme and Project Management
8 Conference and Documents Management
9 Property and Facilities Management
10 Safety and Security
11 Other areas (for areas not included in 1 to 10)

Each focus area may be broken down into sub-focus areas. Examples of sub-focus areas are listed below.

No.	Focus Areas	Examples of Sub Focus areas relating to principal focus
1	Strategic Management and Governance	Strategic planning and monitoring, Mandate and mission, Organizational structure and functions, Start up planning, Liquidation planning, Risk management, Policies and procedures, Governing/Legislative bodies, High level committees, Top level offices.
2	Financial Management	Accounting and financial reporting, Results-based Budgeting, Cash management, Treasury, Contributions, Fund raising, Payroll
3	Human Resources Management	Recruitment, Training, Conduct and discipline, Entitlements and allowances, Performance appraisal system and Medical Services, Use of short term staff (consultants, gratis personnel etc
4	Procurement and Contract Administration	Procurement planning, Procurement process, Local contracts committee, Administration of major contracts such as for fuel, rations, airfield services, medical supplies etc.
5	Logistics Management	Travel services, Transport operations, Air operations, Movement control, Fleet Management and Maintenance
6	Information Technology Management	Management of ICT infrastructure, software development, Communications services, ICT operations, Business continuity and disaster recovery, IT Security
7	Programme and Project Management	Management of programmes such as Rule of Law, Human Rights, Child Protection, Public Information, Disarmament , Demobilization and Reintegration, Mine action, Protection of Civilians, Military and Civilian Police operations, and Logistics; Management of projects such as technical cooperation and quick impact projects
8	Conference and Documents Management	Records management, Publications, Editorial services, Conference management, Translation and interpretation services, Web sites
9	Property and Facilities Management	Management of office premises and facilities, Contingent-owned equipment, Expendable and non-expendable property, Building Services, Inventory management, Local Property Service Board
10	Safety and Security	Security of UN staff and installations, Contingency planning, Evacuation procedures and drills, Occupational safety
11	Other areas	This is for illustration purposes only and is not a comprehensive audit and is included for any other focus areas not specified in 1-10. This may include general office administration, executive offices and common services etc.

Risk Categories

Risk categories are common concerns or events, grouped together by the type of risk that will result. The seven (7) risks used in OIOS Risk Assessment methodology is as follows:

A. Strategy
B. Governance
C. Compliance
D. Financial
E. Operational
F. Human Resources
G. Information Resources

No.	Risk Category	Description
A	Strategy	Impact on mandate, operations or reputation arising from inadequate strategic planning, adverse business decisions, improper implementation of decisions, a lack of responsiveness to changes to the external environment, or exposure to economic or other considerations that affect the Organization's madates and objectives.
B	Governance	Impact on mandate, operations or reputation as a result of failure to establish appropriate processes and structures to inform, direct, manage and monitor the activities of the Organization toward the achievement of its objectives. Includes attributes such as leadership, tone at the top, and promotion of an ethical culture in the Organization.
C	Compliance	Impact on mandate, operations or reputation from violations or non-conformance with, or inability to comply with laws, rules, regulations, prescribed practices, policies and procedures, or ethical standards.
D	Financial	Impact on mandate, operations or reputation resulting from: failure to obtain sufficient funding, funds being inappropriately used, financial performance being not managed according to expectations, or financial results being inappropriately reported or disclosed.
E	Operational	Impact on mandate, operations or reputation resulting from inadequate, inefficient or failed internal processes that do not allow operations to be carried out economically, efficiently or effectively.
F	Human Resources	Impact on mandate, operations or reputation resulting from a failure to develop and implement appropriate human resources policies, procedures and practices to meet the Organization's needs.
G	Information Resources	Impact on mandate, operations or reputation resulting from failure to establish appropriate information and communication systems and infrastructure so as to efficiently and effectively.

Risk Assessment Ratings

The OIOS Risk Assessment Framework evaluates the likelihood of the risk occurring and the impact it will have if it occurs.

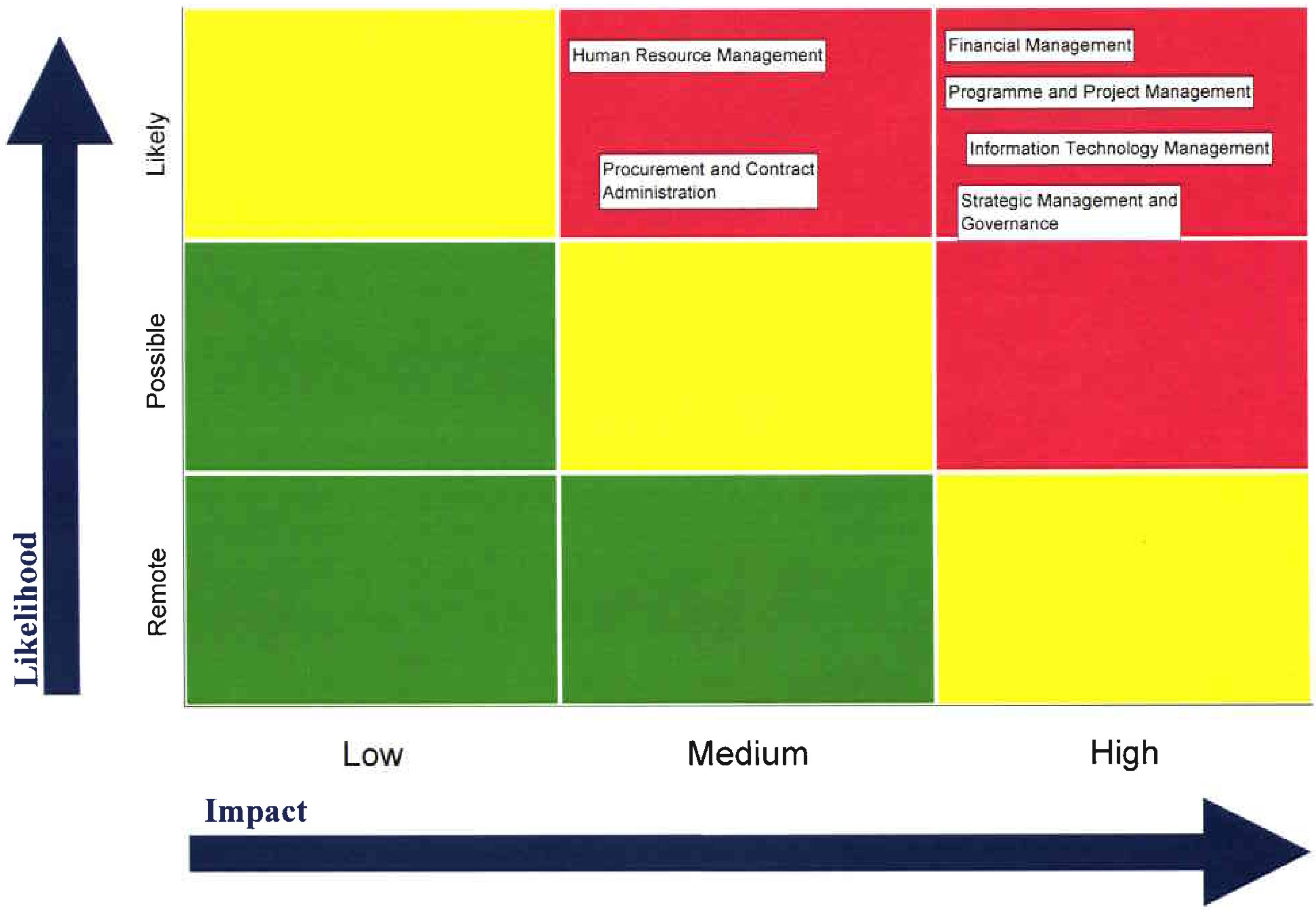
Based on the assessment of the two factors an overall risk rating is derived indicating whether the risk of a focus area is High, Moderate or Low. The ratings used is show below:

Risk Likelihood	
Likely	Conditions within our environment indicate that an event is expected to occur in most circumstances
Possible	Conditions within our enviroment indicate that an event will probably occur in many circumstances
Remote	Conditions within our environment indicate that an event may occur at some time

Risk Impact	
High	Serious impact on operation, reputation, or funding status
Medium	Significant impact on operations, reputation, or funding status
Low	Less significant impact on operations, reputation, or funding status

Overall Risk Combinations Impact and Likelihood	
🟥 Higher Risk	The identified issue represents the following likelihood and impact combinations: • Likely and high • Likely and medium • Possible and high
🟨 Moderate Risk	The identified issue represents the following likelihood and impact combinations • Likely and low • Possible and medium • Remote and high
🟩 Lower Risk	The identified issue represents the following likelihood and impact combinations • Possible and low • Remote and low • Remote and medium

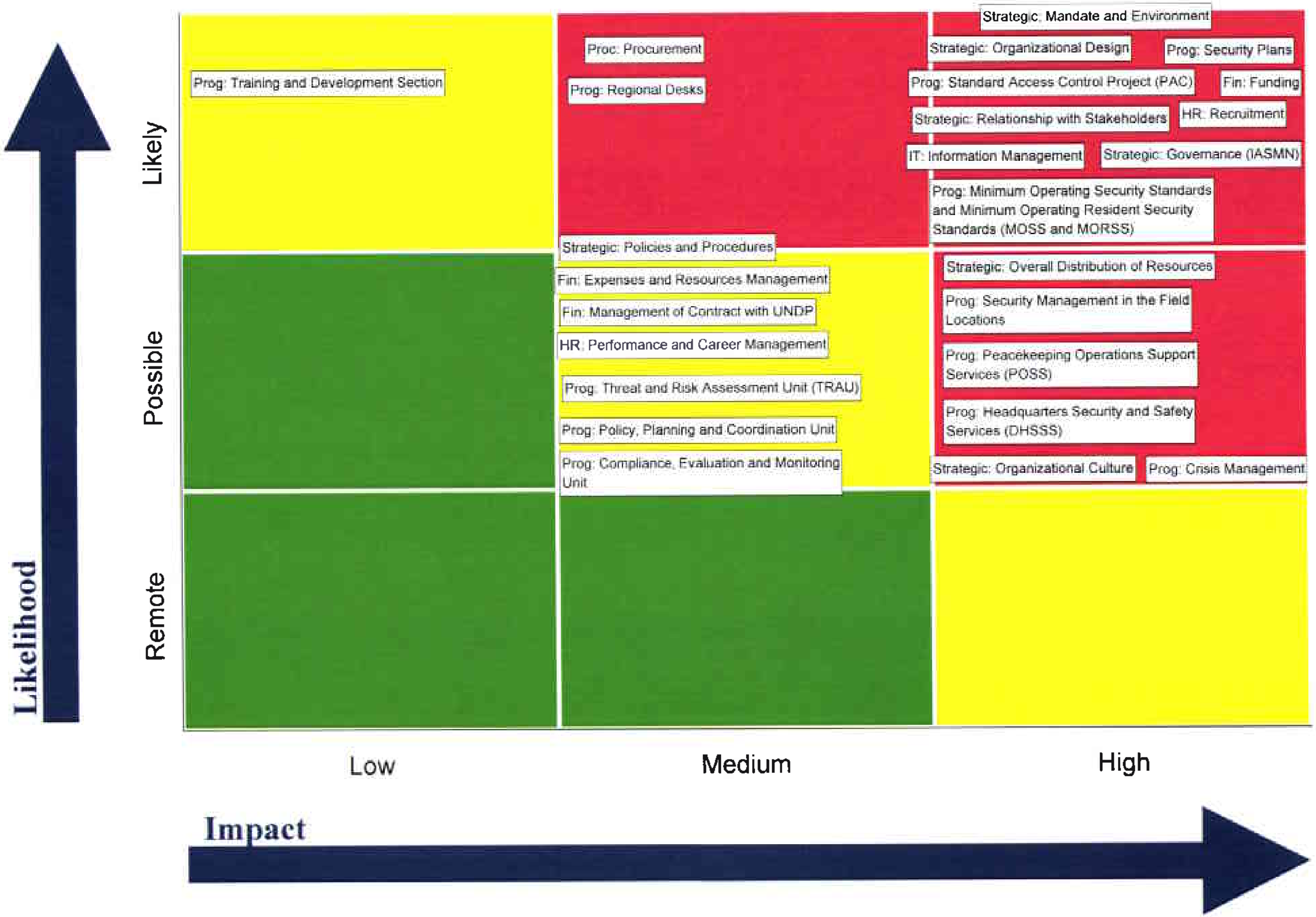
RISK SUMMARY PROFILE (Focus Area)



	Low	Medium	High
Likely	🟨	🟥 Human Resource Management Procurement and Contract Administration	🟥 Financial Management Programme and Project Management Information Technology Management Strategic Management and Governance
Possible	🟩	🟨	🟥
Remote	🟩	🟩	🟨

19/06/2008

RISK SUMMARY PROFILE (Sub Focus Area)



	Low	Medium	High
Likely	Prog: Training and Development Section	Proc: Procurement Prog: Regional Desks Strategic: Policies and Procedures	Strategic: Mandate and Environment Strategic: Organizational Design Prog: Security Plans Prog: Standard Access Control Project (PAC) Fin: Funding Strategic: Relationship with Stakeholders HR: Recruitment IT: Information Management Strategic: Governance (IASMN) Prog: Minimum Operating Security Standards and Minimum Operating Resident Security Standards (MOSS and MORSS)
Possible		Fin: Expenses and Resources Management Fin: Management of Contract with UNDP HR: Performance and Career Management Prog: Threat and Risk Assessment Unit (TRAU) Prog: Policy, Planning and Coordination Unit Prog: Compliance, Evaluation and Monitoring Unit	Strategic: Overall Distribution of Resources Prog: Security Management in the Field Locations Prog: Peacekeeping Operations Support Services (POSS) Prog: Headquarters Security and Safety Services (DHSSS) Strategic: Organizational Culture Prog: Crisis Management
Remote			

19/06/2008