

UNOPS helps its partners in the United Nations system meet the world's needs for building peace, recovering from disaster, and creating sustainable development. UNOPS is known for its ability to implement complex projects in all types of environments around the globe. In an effort to promote organizational excellence, UNOPS seeks highly qualified individuals for the following position:

Vacancy Details

Vacancy Code	VA/2010/NAO/DFS/ISM/03-15
Post Title	ICT Integration and Security Manager
Post Level	P4 (Fixed Term Appointment)
Project Title	Field ICT Support
Org Unit	NAO/DG/UNDFS/ICTD
Duty Station	Brindisi, Italy
Duration	One year
Closing Date	15 March 2010

Background

The United Nations Department of Field Support, Information and Communications Technology Division (UN DFS-ICTD) is charged with the provision of continuous and reliable voice, data and video services to the Department of Peacekeeping Operations and Field Support (DPKO/DFS) missions as well as Special Political Missions (SPMs).

DFS has implemented a range of systems to address the principal requirements of peacekeeping operations and to support and enhance the processes DFS undertakes. ICTD wishes to provide senior management with a strategic reporting capacity delivered through a series of dashboards to support senior management decision making and provide visibility and measurement of tactical and intangible mission activities, including improved visibility of deployments, movements and security. These dashboards will enable the organization to identify and measure key performance indicators and to assess the operations of the organization against them over time

UNOPS has been requested to assist in the implementation of this activity.

Duties and Responsibilities

Under the Supervision of the Chief CITS UNLB (or designee), the incumbent will be responsible for the following duties:

- Provides expert advice and support to the Chief, CITS on all Quality Assurance and Risk Management matters.
- Plan, design, develop and implement effective Information and Communication Technology (ICT) security operational procedures, standards, guidelines, ICT security awareness programme, as well

as other requirement statements needed to support ICT security throughout the Organization.

- Manages the ISO 27001 compliant Information Security Management System for continued and/or increased compliance.
- Participates and provides technical support in security aspects of Information Systems/Information and Communication Technology (IS/ICT) projects and systems and in resolving problems with intrusions, security threats, violations and/or breaches.
- Plans and coordinates security reviews of ICT assets (including computer desktop, server, network, firewall, router and other security appliance) and their configurations to ensure effective security measures are in place in adherence with Organization ICT security standards and industry best practices (ISO 27002).
- Develops ICT security action plans comprised of ICT security programmes to achieve DPKO/DFS ICT security objectives and coordinates their implementation.
- Develops and establishes monitoring procedures and metrics to determine the level of success of implementation of security plans.
- Organizes and participates in the evaluation of emerging ICT security technologies.
- Coordinates the ICT security efforts of all UNLB technical teams to ensure that organization-wide information security efforts are consistent and streamlined, and that duplication of effort is minimized.
- Develops and executes plans for corrective actions to address any ICT security issues associated with the lack of effective security safeguards.
- Provides advice and recommendations on ICT security issues arising from the use, development and implementation of information and communications systems.
- Provides expert ICT security advice to Chief CITS on the management, operation and maintenance of the communications and information systems for providing voice data and video; identify the need for new systems or modifications to existing systems in response to DPKO/DFS filed missions needs.
- Participates in the preparation of ICT systems contingency plans.
- Develops and recommends strategies to address specific security aspects of network connectivity, DRBC resources and related training needs of the CITS or missions.
- Develops and reviews ICT security related specifications, Request for Proposal (RFP), Statement of Work (SOW) and cost proposal for procurement and contractual services.
- Oversees technical evaluations and cost-benefit analyses of bids and proposals; reviews bid responses and evaluation and recommends selection.
- Establishes and maintains strong working relationships with DPKO/DFS and other UN entities involved with ICT security matters, and act as the primary focal point for all information security matters with regard to the UNLB communication hub and Data Centre.
- Keep abreast of ICT security developments in the field of communications and information technology fields, including new products and services, through on-line news services, technical magazines, professional association memberships, industry conferences, special training seminars, and other methods, provide leadership in introducing technological changes.
- Assists with the clarification of individual ICT security responsibility and accountability so that necessary ICT security activities are performed as needed, according to pre-established organizational procedures, policies and standards.
- Integrates ICT security into major UNLB ICT related activities and operations to enable effective management of both ICT security and operational risks.
- Develop and implement incident response procedures.
- Directs analyses of ICT security breaches and incidents to illuminate what happened and how this type of problem can be prevented in the future.
- Plans and coordinates the execution of periodic risk assessments that identify current and future security vulnerabilities, determines the level of acceptable risk; and identifies appropriate security controls to reduce information security risks.

Required Selection Criteria

Competencies and Skills

Professionalism – Strong theoretical background and substantial experience in information technology/information management, particularly in the area of security issues and risk assessment. Strong analytical and problem solving skills. Ability to independently maintain assigned systems and develop innovative approaches to resolve a wide range of issues/problems. Demonstrated ability to manage projects and working towards the achievement of defined deliverables.

Commitment to Continuous Learning – Willingness to keep abreast of new developments in the field of information technology/information management, particularly in the area of ICT Security.

Communications – Excellent communication (spoken and written) skills, including the ability to convey complex technical concepts both orally and in writing, in a clear, concise style.

Planning & Organizing - Ability to organize, plan and implement work assignments, juggle competing demands and work under pressure of frequent and tight deadlines.

Teamwork - Strong interpersonal skills and ability to establish and maintain effective partnerships and working relations with people in a multi-cultural, multi-ethnic environment with sensitivity and respect for diversity. Works collaboratively with colleagues to achieve organizational goals.

Skill Requirements

Advanced University degree (Master's degree or equivalent) in Computer or Information Systems, Mathematics, Statistics or other related field. A first level university degree with a combination of relevant academic qualifications and extensive experience in information technology may be accepted in lieu of advanced university degree.

Minimum of 7 years of progressively responsible professional experience in performing ICT security risk managements and assessment activities and experience in other security domains including operations security and incident management.

Substantial knowledge and understanding of information and communication technologies and related security issues is required.

Must possess a broad based certification such as the Certified Information System Security Professional (CISSP). Certification in ITIL, ISO 9001, CoBIT, CISM, or Audit (e.g. CISA) is highly desirable.

Submission of Applications

Qualified candidates may submit their application, including a letter of interest, complete Curriculum Vitae and an updated United Nations Personal History Form (P.11) English Version, via e-mail to **DFSJobs@unops.org**. Kindly indicate the vacancy number and the post title in the subject line when applying by email.

Additional Considerations

- Applications received after the closing date will not be considered.
- Only those candidates that are short-listed for interviews will be notified.
- Qualified female candidates are strongly encouraged to apply.
- UNOPS reserves the right to appoint a candidate at a level below the advertised level of the post.

For more information on UNOPS, including its core values and competencies, please visit the UNOPS website at www.unops.org.