WORKBOOK 11.3: UN SECURITY FORCE OPERATION POLICIES

Purpose: To provide information about types of policies and a sample policy

Part 1: Policies in a Standard Operating Procedures Manual

Policies and procedures should be documented in a standard operating procedures manual to provide direction and help ensure consistency in performance.

Types of Policies to Include in the Manual

The following are types of policies that should be included in the manual:

- **Description of the facility site**, to include general functions, number of personnel at the facility, employees, contractors, and visitors
- **Floor plan of the facility**, which identifies:
  - Critical areas
  - Security countermeasure locations
  - Emergency evacuation routes
- **Description and application of access controls for the facility**, such as card access with additional personal identification numbers for critical areas for specified personnel, including the procedure for granting visitor access as well as escort responsibilities
- **Security force responsibilities** that include a detailed outline of procedures for performing their assigned functions, for example:
  - Conducting patrol activities
  - Maintaining assigned posts
  - Dealing with the public
  - Reporting unusual occurrences

Organizations that possess a security force should have a wide range of policies and subsequent procedures for security force activities.

Other Examples of Policies and Procedures

- Pre-employment procedures to ensure the selected candidate meets the background investigation check
- Pre-employment medical examination to ensure the candidate meets the required medical standards
- Attendance and graduation from an accredited security force training center
- Qualification standards to include firearms, physical fitness, written examinations, and continued performance appraisals of work performed
- Special skill training such as tactical team training and hostage negotiations
- Legal requirements education to ensure compliance with statutory law
- Security education and operations covering classified and sensitive information
- Training on response to and reporting of incidents of security concern and the protection of critical infrastructure

- Weaponless self-defense training
- Intermediate force weapons training
- Knowledge of communications methods and procedures
- Vehicle operations knowledge, including safety and routine and emergency operation
- Knowledge of post and patrol operations requirements, including site-specific plans
- Knowledge of post and general orders, policies and procedures
- Awareness of the types of, and potential deployment of, weapons of mass destruction
- Donning and use of assigned personal protective equipment such as gas masks and protective clothing

Part 2: Sample: UN Security Force Operation Policies

The following content represents excerpts from the United Nations World Bank Group policies and procedures.

Security Risk Management

Security risk management shall be an integral part of the World Bank Group (Bank Group) activities, enabling operations and enhancing the safety, security, and wellbeing of personnel, dependents, and other assets. It starts with a rigorous threat and risk assessment, leading to the selection and application of logical security measures and the implementation of mitigating measures to reduce the overall risk to an acceptable level. This approach not only applies to the physical security of the Bank Group Country Office, but is also applicable to all activities at the country level, as well as, specific activities such as procuring armored vehicles, letting a guard contract, tracking the movement of visiting missions and hosting conferences and meetings.

How does this work in practical terms?

A common example would be guards at Bank Group offices. The need for persons to guard a World Bank Office location should be identified through a security risk assessment. The appropriate response to mitigate [treat] the threat may include engaging the services of guards to protect the facility. The analysis should also identify the number of guards required, the number and location of guard posts, and their specific tasks. Using this approach, which is based on modern security risk management practices, will produce an appropriate result of treating the risk and also provide solid substantiation for the necessary expenditures for security requirements. The rest of this guide must be read bearing this approach in mind as it provides the foundation for all security risk activities and procedures applied by the World Bank Group office.

Principles of Risk Mitigation

- Threats have the potential or possibility to cause harm. A threat only translates into a risk to the Bank Group (in a particular location) if the Bank Group (personnel and premises) is vulnerable to it, expressed in terms of the

likelihood of the event occurring and the potential impact or consequences for the Bank Group if it does occur.
- Hazards refer to harmful natural or man-made accidental events, while threats refer to deliberate human causes.
- Risks are defined as the combination of the impact and the likelihood for harm, loss, or damage to the Bank Group from the exposure to threats.
- Security Risk Management is an analytical procedure that assist in assessing the operational (program) context of the Bank Group; and identifies the risk level of undesirable events that may affect the Bank Group personnel, assets and operations; providing guidance on the implementation of cost effective solutions in the form of specific prevention and mitigating strategies and measures with the aim of lowering the risk levels for the Bank Group by reducing the impact and likelihood of an undesirable event to an acceptable level.

The intent of any mitigating measure should be to achieve one or more of the following:
- Reduce the likelihood of the specified risk from taking place against the Bank Group
- Reduce the vulnerability of the World Bank Group to the specified risk
- Reduce the impact on the World Bank Group if the event occurs

Decision Making

- Country Office managers in each location are ultimately responsible for the safety and security of World Bank Group staff and for reconciling operational objectives with security measures. It is they who have ultimate authority for deciding which measures are appropriate in the local situation and for deciding how they are implemented.
- Country Manager's receive advice and practical support from security specialists, but they may not delegate the accountability for security.

Monitoring and Compliance

- The World Bank Group has a "Duty of Care" for its staff and must take appropriate steps to ensure they are not exposed to unnecessary risk. The term "Due Diligence" in the context of security management, means that managers have taken all reasonable measures – allowing for the situation, available information concerning possible risks, and their own capacity or resources – to avoid exposing staff to unnecessary danger.
- Corporate Security exercises "Due Diligence" by ensuring that policy and procedures to achieve this are issued throughout the World Bank Group security management system and through Global Security (Compliance), by ensuring that the appropriate processes are implemented at the country level.
- Managers shall be able to show that they have exercised due diligence for the safety and security of their personnel. Demonstrating literal compliance with the generic global security standards may not provide sufficient proof of "due diligence", if it can be shown that the specific situation required extraordinary

security measures. It is therefore in the manager's own interest to use the security risk management process, maintaining records of analysis undertaken and resulting decisions.

Business Continuity Management

Business continuity planning is the creation and validation of a practiced plan for how World Bank Group offices will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The objective is to ensure business, which is an ongoing state how operational activities are conducted. In plain language, BCP is working out how to stay in business in the event of disaster. The central elements of Business Continuity Management are: (1) incident management (crisis response and disaster recovery), and (2) business continuity. Incidents may include building fires, earthquakes, pandemics, demonstrations, power cuts, floods, and bomb blasts. The product addressing the latter is a business continuity plan. In the case of the World Bank Group a decision has been made to combine the security plan and business continuity plan into one document; the Emergency Response & Business Continuity Plan. This plan allows for the integration of existing preparedness activities and it ensures that other plans such as security, pandemic influenza inform, support and complement each other.

The Country Office Emergency Response & Business Continuity Plan (the Plan) addresses a Country Office's process for responding to emergencies and business interruptions. Its purpose is to help staff prepare for, respond to, stabilize, and restore operations in the event of an interruption. The Plan does not, and cannot, cover every contingency. It does, however, provide a basic framework and reference for planning and actions. The Plan is a living document and should continually be updated to reflect new and changing conditions.

Security Coordination and Management

Although host governments have the primary responsibility for the security of World Bank staff, their dependents, and property, the World Bank Group (Bank Group) has nonetheless developed a comprehensive program to protect its interests and respond in times of emergency. This is done through prudent operational and physical security measures to protect staff, facilities, and programs, and for individuals to take personal security measures to reduce risk against their persons, families, and possessions.

The Bank Group participates and cooperates within the larger, unified UN security management system and supports the central role of the UN Department of Safety and Security.

The UN is responsible for inter-agency arrangements for the protection of UN organizations and specialized agencies, including the World Bank Group, against hazardous situations which may be beyond the control of the host government. The World Bank Group will generally seek to act in unison with other members of the

UN community; however it reserves the right to act unilaterally in order to protect the well-being of its staff and its corporate assets and reputation. To this end, the Bank Group will implement its own security plans and procedures for operations in Country Offices. The Bank Group Country Manager shall keep the UN Designated Official informed of the Bank Group intentions since the World Bank Group remains part of the UN security management system. Bank Group Country Managers are therefore encouraged to actively participate in the activities of the SMT since they cannot unilaterally decide to withdraw from the system.

The General Services Department Security Office (GSDSC) is responsible for issuing security and business continuity policies, monitoring compliance with their requirements, interpreting the policies, and developing implementing procedures and standards. Bank Group Country Offices (CO) and facilities are responsible for implementing the arrangements, supported by Security Specialists Country, Office Security Advisors, Senior Security Specialists (SSS)/Security Specialists Regional (SSR), and finally the General Services Department Global Security. The General Services Department Security Office also represents the Bank Group at the Inter-Agency Security Management Network (IASMN). The IASMN brings together representatives of all partners in the UN security management network to coordinate security practices and policies across the UN system.

Bank Group offices are expected to ensure that security considerations figure as a fundamental element of all their operations at the country level and are not only restricted to the physical security of the office. Security should be incorporated in all Bank Group operations and Country Managers shall ensure that the security plan is implemented fully for its personnel and activities, including security preparedness and contingency planning.

Security Arrangements in Country Offices

Country Office Level

The Country Office managers are responsible for the safety, security, and welfare of World Bank Group staff members under their supervision and their eligible dependents. In addition, they have a responsibility for the protection of all assets, property and information belonging to the Bank Group under their supervision. All persons in the supervisory chain will be held accountable for this responsibility.

Country Office managers are also responsible for ensuring that staff members under their supervision adhere to security policies, rules and regulations.

Resident World Bank Group staff members and visiting missions have the responsibility to abide by security policy, guidelines, directives, plans and procedures of the security management system.

Regional Vice-Presidential Unit Level

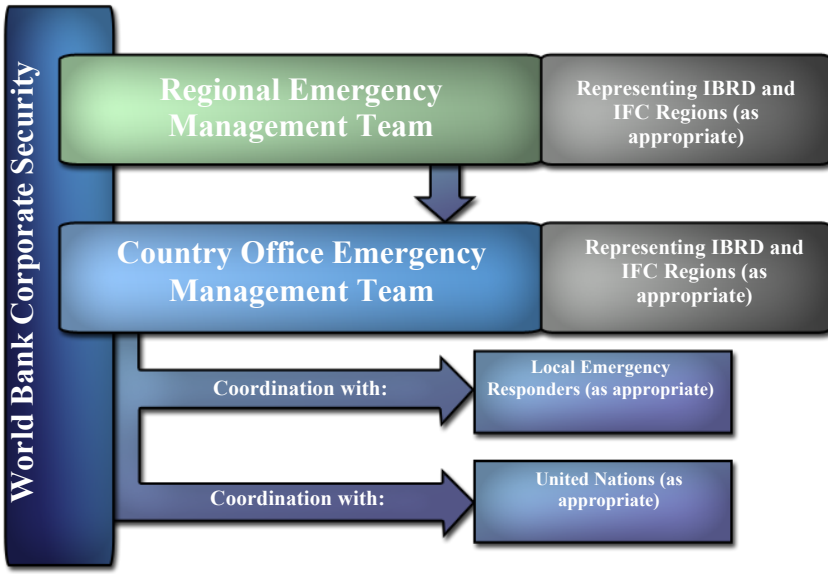
Ultimately the IBRD Regional Vice Presidents or IFC Regional Directors are responsible for ensuring that their respective Country Offices develop and maintain the Emergency Response & Business Continuity Plan. Within the Country Office, the decentralized Country Director /Manager/ Representative is responsible for developing and maintaining the Plan, but may delegate the task for updating the plan.

Management of Country Office Emergencies and Interruptions

The Regional Emergency Management Team (REMT), comprised of the Regional Vice President, the Director of Strategy and Operations, the Chief Administrative Officer, Regional Human Resource Officer, SSS/SSR and Regional Communications Officer (and others as needed), provides high-level strategic guidance and support to Country Offices as they face emergencies and interruptions at the local level.

The Country Office Emergency Management Team (EMT) is responsible for implementing Country Office-specific emergency response and business continuity activities immediately following a business interruption. The team works closely with the REMT, as well as Country Office staff members, to ensure the safety of staff members, limit the impact of business interruptions, and determine the best course of action to continue operations during a business interruption.

Figure 1: Management of County Office Incidents Flow Chart



GSD Corporate Security & Business Continuity will provide advice, guidance and direct support to the REMT and the CO EMT before, during and after a crisis.

For a detailed description of the key security and business continuity roles and responsibilities at all levels refer to the AMS 6 series.

Coordination with the UN Security Management System at the Country Level

The UN system-wide security arrangements are described in detail in the UN Field Security Handbook and summarized here. Each Bank Group office should have a copy of the UN Field Security Handbook, if the UN is present in the country.

The United Nations Department of Safety and Security (UNDSS) was formally established on 1 January 2005 and has since been dedicated to performing the following functions:

- To support and enable the effective conduct of United Nations activities by ensuring a coherent, effective and timely response to all security-related threats and other emergencies;
- To ensure effective risk mitigation through the establishment of a coordinated security threat and risk assessment mechanism within the framework of a common, system-wide methodology;
- To develop high-quality, best-practice security policies, standards and operational procedures across the United Nations system, including the appropriate degree of standardization;
- To support implementation and monitor compliance with those security policies, standards and operational procedures.

In each country or designated area where the United Nations is present, the most senior UN official is normally appointed as the Designated Official (DO) for security. The Designated Official is accountable to the Secretary-General through the Under-Secretary-General for Safety and Security, for the security of personnel throughout the country or designated area. The DO is responsible and accountable for ensuring that the goal of the United Nations security management system is met at the duty station. The DO convenes and chairs a Security Management Team (SMT) to advise on all security-related matters. The SMT includes Country Representatives of all UN organizations, including the Bank Group, plus others with technical expertise, as appropriate. A Chief Security Advisor (CSA) or Security Advisor (SA) assists the DO and the SMT to carry out their security functions.

The principal responsibilities of the DO include:

- Liaising with the host government officials on security matters,
- Forming a Security Management Team (SMT),
- Arranging for a security plan for the country to be prepared,
- Informing the Secretary General (through) UNDSS of all developments which may have a bearing on the safety and security of staff members, and
- Managing, in conjunction with the SMT, crisis situations.

The following services can be expected from the local UNDSS security team:

- Participating in and providing security inputs into operational planning;
- Cooperating on security matters with the Security Focal Point;
- Undertaking security risk assessments for all locations in the country where personnel of the organizations of the United Nations system and their

recognized dependents are present and facilitating the implementation of recommended mitigating measures;
- Preparing, maintaining and updating the overall country-specific security plan, contingency plans and security listings of personnel of the organizations of the United Nations system and their recognized dependents;
- Ensuring that plans for relocation/evacuation to a safe area are current, feasible and implementable;
- Ensuring that an effective and functioning security and emergency communications system is in place;
- Ensuring that all personnel of the organizations of the United Nations system and their recognized dependents receive briefings upon initial arrival, local security training as necessitated by changes in the security environment, and are kept informed of matters affecting their security;
- Maintaining up-to-date instructions for personnel of the organizations of the United Nations system and their eligible dependents on precautions they should take in relation to the implementation of the security plan, including comprehensive listing of emergency supplies they should have on hand and guidance on the behavior during a variety of emergencies, including natural disasters and political crises;
- Reporting all cases in which personnel of the organizations of the United Nations system and/or their recognized dependents have been victims of crime and submitting required reports on such cases;
- Conducting security surveys of residential areas and premises; and
- Advising the DO and the SMT on operational security requirements consistent with the minimum operating security standards.

Security Program Management

For any security program to be effective it should be structured and the activities should be included into the annual work program of the office.

The office EMT shall meet at regular intervals (in commensurate to the security situation) to review and update security assessments, contingency plans and the practice working in crisis situations. In addition, World Bank Group Country Office managers should attend UN Security Management Team meetings.
Security Focal Points should establish a filing system to maintain records of security documents. The following are some of the documents to have readily available:
- Bank Group Documents
  - Security Risk Assessment and Business Impact Assessment (This is the basis for all contingency planning, including business continuity)
  - Business Continuity and Emergency Response Plan
  - Office evacuation plan
  - Updated staff lists
  - Security related contracts and minutes of meetings with contractors
  - Relevant country maps
  - Safety and Security Registers

- The following are typical registers that should be maintained within the Country Office:
  - Security Awareness Training. Numbers of Staff/Consultants (national and international) employed and how many have participated in security training and briefings. List the kind of training, numbers of personnel attended, date carried out and instructor. A separate list with the names of individuals attending the training should also be kept.
  - Security Exercises. Maintain a record of all security exercises carried out by office such as building evacuation/emergency drills, fire drills and warden drills.
  - Security Instructions. It is very important to register all security instructions that are issued to all staff. Copies of the instruction should be kept in electronic and/or paper format. These instructions should be referenced with a date and number and filled in chronological order. This file will be very important in the case of an investigation.

- UN Security documents
  - UN Security Risk Assessment — this will normally be distributed to members of the Security Management Team (SMT).
  - UN Field Security Handbook (FSH).
  - Country/Area – specific Security Plan.
  - Country/Area – specific MOSS.
  - Country/Area – specific MORSS.
  - Country PEP protocol.

Offices, Premises, & Facilities

All World Bank Group offices shall comply, where feasible, with international building, safety and fire regulations, or applicable laws of the host country as appropriate, including construction to resist earthquakes and other natural hazards. Security risk assessments need to be carried out for each office to identify appropriate access control measures based on the security situation, the size and location of the premises. Premises that are assessed to be at high risk from terrorism are to have:

- Stand-off distance, from the location where a device is likely to be delivered to the building, as estimated/advised by qualified exerts, taking into account the scale of a likely threat, surroundings/approaches, and construction of the building.
- Structural reinforcement and/or blast walls as advised by a qualified expert.
- Shatter resistant film installed on windows.
- Bunkers or reinforced rooms where staff can retreat into when required.
- Surveillance and access control systems.

This Guide, in particular, shall be read in conjunction with the Country Office Physical Security Standards (July 2009) that is posted on the intranet. The following Standards are included in the Country Office Physical Security Standards:

- Standard A — CCTV System

- Standard B — Duress Alarm
- Standard C — Intrusion Alarm
- Standard D — Locks
- Standard E — Metal Grilles
- Standard F — Public Access Controls
- Standard G — Public Address/Emergency Alert System
- Standard H — Safe Haven
- Standard I — Security Doors
- Standard J — Security Lighting
- Standard K — Walls, Fences and Other Barriers

In addition to the specific standards mentioned above the following procedural guidance is provided for Access Control, including Restricted Areas, Identification Cards, Vehicle Parking, and Closed-circuit Television.

Access Control

Because of inherent risks around the world, there is a clear and demonstrated need to develop and implement stringent access control in all Bank Group facilities. Accordingly, Country Offices shall establish procedures to control access to its premises. These procedures shall ensure that only staff members, consultants and contractors have unescorted access to offices and that visitors are screened and access to offices verified before they are allowed to enter. Country Office management is responsible for determining the degree of access for all staff members, consultants and contractors. Where feasible and appropriate there should be separate entrances for staff members and visitors. All buildings and compounds shall have alternate emergency exits and guards should be trained on appropriate surveillance and reconnaissance detection techniques and reporting protocols. The following also need to be considered:

- Electronic Access Control Systems. Country Offices should employ electronic access control systems featuring card readers and ID cards, where possible, which are issued to staff members and temporarily to visiting missions. The access control system should also feature the following: authority to grant access rights, assignment of access rights, audit trail, periodic back-up of data and withdrawal of access rights when staff members resign, transfer or their mission ends. Further, consideration should be given to establishing profiles for staff member access. For instance, some staff members may have full access to the office, while others because of the nature of their duties may have their access restricted to certain hours during the work week.
- Manual Access Control Systems. If an electronic access control system is not in use, stringent key control and attendant procedures should be developed and implemented. This would include a sign in/out logbook for staff members and the changing of lock cylinders if and when a key is lost and access may be or is compromised. Staff members, consultants and contractors shall surrender keys to the office when their employment ends. If they do not, the system must be considered compromised and the lock cylinders changed and new keys issued.

- After Hours Access. To better assure that Bank Group premises and property are afforded optimum security, stringent access control procedures should be in effect. Country Office management determines the hours and days of access, the levels of access and the days and hours considered to be "after hours." Further, the access control procedures should be in writing and all staff members made aware of them. Ideally, entry to the facility should be carried out employing an electronic access control system, which can be managed by restricting the access of card holders to specific days and hours. In addition, intrusion detection alarm system should be in place to complement access control and only those staff members authorized full access to the office should be provided the access code. Where an electronic access control system is not in place, a security guard must control access after office hours, weekends and holidays to permit entry. The guard will maintain a logbook listing the names of staff members who entered the office and the time they departed.
- Visitor Access. Visitors, including vendors, suppliers and maintenance personnel, are welcome at Bank Group offices. The following procedures apply to all visitors:
  - Visitors and vendors shall present a valid photo identification card to the guard or receptionist.
  - The guard or receptionist will enter the name of the visitor, the organization he or she represents, the name of the person(s) they are visiting and the time of arrival and departure.
  - Visitors will be welcomed by reception and escorted in the office by the staff member they are visiting.

The Country Director or Manager may waive all or some of these procedures for persons deemed "well and favorably known," such as senior government officials or diplomats and representatives of international organizations. In addition, dependents of family members may have access during office hours.

Identification Cards

All Bank Group Country Office staff members, contractors, short-term consultants, extended term consultants and extended term temporary employees shall be issued photo identification.

- Issue of World Bank ID Cards. ID cards are issued and managed in accordance with AMS 6.50 World Bank Group Identification Cards that can be found on the World Bank intranet.
- Recording and Mapping of Serial Numbers. The serial numbers of all staff member identification cards that grant access to Bank Group offices shall be recorded.
- Design of Locally Issued ID Cards. Locally designed identification cards should conform as much as possible to those issued by the ID Office in Washington, DC. The ID office in DC can prepare WB card facings which can be affixed to access control cards used in Country Offices.
- Display of ID Cards. All Bank Group staff members, contractors, short-term consultants, extended term consultants and extended term temporary

employees will wear their Bank issued ID cards visibly displayed above the waist while in Bank premises.

- Surrender of ID Cards. Bank Group staff members and other categories of employees shall surrender their Bank issued ID cards when their employment with the Bank ends.
- Lost ID Cards. All employees should report the loss of World Bank issued identification cards to the Security Focal Point. If the card was part of an electronic access control system, it must be dropped from the system within 24 hours of it being reported lost.

Restricted Area Security

In addition to normal access control there are areas or offices in the office where additional measures should be applied to prevent unauthorized access. These areas include Network Control Rooms (NCR) and finance offices.

- Access Rights to Restricted Areas. Country Office management will designate in writing the staff members who may have access to these locations. For example, the Information Specialist and his/her backup are the only staff members who have a regular and recurrent need to have unescorted access to the NCR. If an electronic access control system with audit trail is in use, the staff member managing the system (usually the Information Specialist) will grant access to those persons designated by country management. When access is no longer required, the system will be updated.
- Escort and Supervision of Contractors and Vendors. In the event other persons, including contractors or vendors need access to these locations they shall be escorted by an authorized person.

Where a manual access control system is in place, strict key control should be exercised and the staff members authorized access to the office should enter their names and the dates and times of access in a logbook. Only staff members authorized to access to the office may retain the key after office hours.

Vehicle Parking

Country Offices that have parking facilities they control will establish procedures to manage access. Country Offices in multi-tenant office buildings should lobby building management to develop and implement vehicle access control procedures.

- Categories of vehicles. Only Bank Group owned vehicles and those owned by staff members, consultants and contractors will be allowed to park and access shall be controlled by a guard or a card access system. If a guard is controlling access to the parking area, the vehicles of vendors and suppliers, who have been previously approved for frequent access, may be allowed to enter and park for brief periods of time. Taxis may not enter Bank Group parking areas or lots.
- Vehicle Access Procedures. In the absence of a card access system, the guard controlling access should be provided a list of the staff members, consultants and contractors authorized to park. For visitors, vendors and suppliers, the guard should maintain a logbook with the name of the driver, other occupants,

the make and model of the vehicle, the license plate number and the arrival/departure times.

- Vehicle Search Procedures. The level of vehicle search procedures depends on two conditions; (1) the threat level and (2) the degree of control of access the Bank Group offices have. In facilities occupied solely by the Bank Group, screening procedures can range from a full search of the vehicle employing mirrors for the underside and a visual inspection of the interior, the engine compartment and the trunk to allowing access to vehicles operated by Bank Group staff members without the benefit of any search. The vehicles of important visitors may be allowed access to the facility's parking lot.

In multi-tenanted facilities, Country Office management should encourage building management and other tenants to institute some vehicle access control and parking restrictions.

Closed-Circuit Television

Closed-circuit television (CCTV) will be employed to enhance security, especially at entrances to buildings and offices, in common areas and the perimeters of standalone facilities.

Cameras should not be positioned overtly or surreptitiously to detect or prevent crimes unless their use in this manner has been approved by headquarters. During the installation of the CCTV, it is essential for the Security Focal Point to be trained on how to use and maintain the CCTV and how to record and store footage. The procurement specialist will insert the obligation of this training and in the TDR for vendors. Where possible it may be better to rely on a local vendor to maintain all security systems, including CCTVs.

When a CCTV system is not operating as it should, the Country Office may be vulnerable, incident response may be delayed, and liability may be incurred. Camera maintenance shall be considered before system implementation. Having adequate spare parts or a service agreement with a vendor or service integrator is advisable.

- Administration. The Security Focal Point and/or his alternate will be responsible for overseeing the operation and maintenance of all CCTV units.
- Use, Storage, and Archiving of Tapes. If the CCTV units are equipped to record images, the tapes or other medium will be retained for a period of 30 days and stored in a secure container, such as a locked file cabinet in the Network Control Room. After the 30-day period, the recording medium may be reused.

Closed-Circuit Television Procedures Example:

- Security officer will sign a site log which contains Officer Name, Time and Date, Signature
- CCTV system must be reviewed each day by playing back 15 seconds of recording for each camera to ensure camera is:
  - Functioning
  - Play back is clear

  - Camera is properly positioned
- Deficiencies will be noted and reported to site supervisor

Provision and Management of Security Guards

Security guards are an essential and valuable component of most security programs and the need is identified through the security risk assessment process. Within the Bank Group, this component may be provided through the following means:

- Provision of security guards through a professional security contractor;
- Provision of security guards through the landlord under the building lease agreement.
- In special circumstances, other means of provisions of guards may be agreed between the Country Director/Manager, the Regional Office of the CAO, GSDSC and GSDPR.

In line with the overall responsibility of Country Office security, the Country Director/Country Manager is ultimately responsible for the management of the security guards / security contractor for the Country Office. The responsibility for overseeing the day-to-day performance of the security guards / security contractor may be delegated to the Security Focal Point or other Country Office senior staff.

This responsibility would include meeting at least quarterly with the Contractor's Representative / Contractor's Security Manager to discuss the Contractor's guard performance. This responsibility will be reflected in the Statement of Work (SOW) of the Contract.

Procurement and Contract Management of Security Services Contracts

The procurement and contract management of security services provided through a professional security contractor is regulated by AMS 15.10 Corporate Procurement Policies and Procedures. While the actual procurement process will be managed by either the Country Office or GSDPR, the main task for GSDSC, through the Senior Security Specialist network, is the development of the Statement of Work (SOW) – also called the Terms of Reference (TOR) in support of the Country Office. The statement of work should be based on a thorough needs assessment. Table 1: Needs Assessment Factors shows some of the factors to be considered.

Table 1: Needs Assessment Factors

Factor	Examples
Operational tasks the security contractor is expected to accomplish	▪ Physical protection and guarding ▪ Close protection ▪ Rapid response ▪ Investigative services ▪ Risk assessment and analysis
Type of security required	▪ Armed or unarmed ▪ Physical and/or technical security ▪ Static and/or patrol guard services ▪ Registration and access controls

Level of security required	▪ Number of posts ▪ Hours per post
Minimum experience levels required	▪ Operational experience ▪ Management experience ▪ Training and education ▪ Professional skills
Minimum experience levels required	▪ Outdoors or indoors ▪ Duty times/periods ▪ Ground and terrain ▪ Uniformed or civilian clothes
Working days	▪ Number of days per week ▪ Holidays when security required
Equipment requirements from contractor	▪ Surveillance systems ▪ Communication systems ▪ Weapon systems ▪ Other
Public contact	▪ Level of public contact ▪ Type of uniform required ▪ Level of training in public relations
Contract management requirements	▪ Public complaints procedure ▪ Tribunal mechanisms ▪ Disciplinary procedures ▪ Performance monitoring (see below)

It should be recognized that the level of experience and range of services on offer will vary between companies. Care should be taken when conducting needs assessments to avoid the unnecessary exclusion of newer or smaller operators. Bidding documents should also include a request for the following information:

- Certifications of risk indemnity insurance (where relevant)
- Company balance sheets and statement of overall turnover
- Evidence of the contractor's registration, educational and professional qualifications and those of its managerial/operational staff
- A list of principal services provided in the last three years
- Number and work pattern of employees, (full time/part time)
- Work experience of employees, (including management)
- Turnover rate of employees
- Benefits and training offered to employees
- Extent of pre-employment screening for employees/management staff, (where legally permitted)
- References from similar clients in the local area

For security services, since the requirement may be continuous, the current practice of determining the contract value is:

- Competitive procurement process. Establish the contract value, by calculating the accumulative amount of the estimated annual value of the services over a five year period, and
- Non-competitive procurement process. Establish the contract value, by calculating the accumulative amount of the estimated annual value of the services over a three year period.

Security Incident Involving Guards

Serious incidents involving guards should be immediately brought to the attention of Country Office management and the security contractor's management for corrective action. Depending on the seriousness of the incident and the possibility of public disclosure, Country Office management should consider informing senior regional management in Washington and the Security Operations Center.

Security Incident Procedures Example

- Security officer in violation will be escorted to site supervisor's office; weapon will be removed prior to entering supervisor's office
- Once site supervisor has briefed the guard, the guard will be escorted from the site
- The security officer's company ID badge will be confiscated by site supervisor
- Security officer will be removed from both electronic and manual access entry systems
- Each shift supervisor will be advised of incident and suspension and make such information available to their shift guards

Deployment of Guards in Offices and Residences

Guards supplied by a company, which has participated in and been awarded a contract by GSD Procurement, may be used to carry out security duties, such as controlling access and screening personnel and vehicles entering World Bank Country Offices and parking lots. They may also be tasked to perform duties in emergencies, such as a fire or a bomb threat.

Security guards may also be posted at the residences of international staff members provided the UN Minimum Operating Residential Security Standards (MORSS) recommends such coverage. However, Bank policy is for international staff members to personally contract and pay for these services to a security company and be reimbursed.