SECTION I : INTERNSHIP REPORT CANTONMENT GENERAL HOSPITAL

2.1 **Introduction**

2.1.1 Delhi Cantonment lies in the south West District region of Delhi. All the four major transport modes are easily accessible to the residents nearby the Cantonment. Other areas nearby include Dwarka, Dhaula Kuan, Tilak Nagar, Vasant Vihar, Nariana, Janakpuri, R K Puram, Shanti Niketan and West End. Delhi airport is approximately 5 Km from the hospital. All trains plying from Delhi towards Rajasthan/ Gujarat stop here and Delhi Cantonment itself is one of the stations. This region is also connected by Delhi Metro and the nearby stations are Janakpuri / Tilak Nagar. DTC busses are also available from major railway stations.[1]

2.1.2 The British established the Delhi Cantonment in the year 1914. Till Feb 1938, the cantonment Board Delhi used to be known as Cantt Authority. The area of the Cantonment is 10,791.88 acres. It has 63974 Households. As per 2011 India census Delhi Cantonment had a population of 116,352. Males constituted 58% (67,703) of the population and females constituted 42%(48,649)[2]. Delhi Cantonment has an average literacy rate of 91.11%, which is above the national average of 79.9%[3]. Male literacy is 94.54% and female literacy is 86.26%. In Delhi Cantonment, 11.36% of the population is under 6 Years of age.[2]

2.1.3 The Delhi Cantonment is a class I cantonment Board. Presently, the Cantonment Act, 2006 and various policy letters and instructions of the ministry of Defense, Government of India issued from time to time, govern the Cantonment. Though the board functions as a local municipal body, yet it is under the administrative control of Directorate General Defense Estates, New Delhi and Principal Director, Defense Estates, Western Command, Chandigarh.[4]

2.1.4 The cantonment Board consists of eight elected members, three nominated Military members, three Ex officio members (Station Commander, Garrison Engineer and Senior Executive Medical Officer), and one representative of District Magistrate.

An officer of Indian Defence Estates Services, which is a central civic service, is posted as the Cantonment Executive Officer (CEO) as well as the member secretary of the board. The board is headed by the president cantonment board (PCB), who is also the station commander and also presides over the meetings of the cantonment board. The station commander of the army is the Ex officio president of the cantonment board. At present Brig B K Rattanpal is the president of the cantonment board.

2.1.5 The term of elected members is five years. The vice president is elected from amongst the elected.

2.2 Organisational Profile

2.2.1 Cantonment board hospitals have been raised in all cantonments of the country to look after the civilian population living in and around the cantonments. These hospitals come under the local cantonment board headed by a chief executive officer (CEO) who is an officer of Indian Defence Estates service cadre of civil services and works under the administrative control of Director General, Defence Estates, Government of India, Ministry of Defence. Shri B. Reddy Sankar Babu, IDES is the present Chief Executive Officer of Delhi Cantonment board.

2.2.2 One of the mandatory functions of the cantonment board is to provide the basic health cover to the civilian population of Delhi cantonment area. The board has been performing this through Cantonment General Hospital located at Sadar Bazar, Delhi Cantonment.

2.2.3 Cantonment General Hospital (CGH) provides the basic health cover to the civilian population of Delhi cantonment area[4]. The hospital made a modest beginning from one of the barracks of the old base hospital building at Sadar Bazar, Delhi Cantonment. The hospital was shifted to its present location in 1963. The hospital is a 100-bedded unit (under extension) at present, providing general medical and primary emergency care services including laboratory, X Ray and delivery services. The permanent staff consisting of a CMO, 12 General Duty doctors, a Dental Surgeon and 35 Doctors on contractual basis manage the hospital. It has a full time dental clinic and part time visiting specialist of dermatology and ophthalmology. It has limited IPD services. It has in its premises a Health post of Delhi Government, which provides Maternal and child health services including Antenatal care and immunization services. It also has DOTS Centre of Delhi Government providing treatment of Tuberculosis. An AYUSH clinic run by Centre Council for Research in Homoeopathy (CCRH) is also functional on daily basis. The hospital carries out Birth and Death Registration, an important function of Delhi Cantonment Board. It is implementing all national health programs including pulse polio program, school health and Tuberculosis control[4].

2.3 **Structure of the Hospital**

Figure 2.1: Cantonment General Hospital

2.3.1 The General hospital is housed in a three-floor building with the following constitution:

(a) **The Basement** has the AC plant, Linen store, Furniture store, Pump house and Generator set.

(b) **Ground Floor** – Has the reception and registration Centre, Emergency, Casualty room, Ortho, Gynecology, Ophthalmology, ENT, Medical, Psychiatric, Skin, Ayurveda and Homeopathic OPDs, Minor OT, Radiology (X Ray and

USG), ECG room, Immunization and injection room, Family Planning and counseling room, Labor room, Physiotherapy room, DOTS Centre, main Pharmacy, Dressing room and plaster room.

(c) **The First Floor** – Has the administrative block, Dental department, Path Lab, Pharmacy store, Ayurveda store, Family ward (18 Beds), and a conference room.

(d) **The second Floor** has the major OT, VIP rooms (06 beds), Private wards (06 beds), Male ward (20 beds) and CSSD.

AMBULANCE
DELHI CANTONMENT BOARD HOSPITAL
Advanced Life Support Ambulance

Figure 2.2: Ambulances

2.3.2 **Ambulances** – The hospital has two mobile dispensaries to cater for distribution of medicines and critical care in remote areas of the cantonment. It has two Basic Support Ambulances and one Advanced Life Support Ambulance.

2.3.3 **Staff**

The hospital is headed by a CMO (In charge) under whom is the following staff: -

(a) **Permanent** – Doctors -13, Nurses Grade B/ ANM - 02, Technicians – 02, Pharmacist -02, Administrative staff -18.

(b) **Contractual** – Doctors -35 (Specialists – 19, Additional GDMO - 11,Senior Resident - 5, Jr Resident -2, Nurses -39, Technicians -21, Pharmacists – 02).

2.3.4 **Departments**

Cantonment General Hospital provides care through the following departments:

(a) General

(b) Orthopedics

(c) Obstetrics & Gynecology

(d) Pediatrics

(e) ENT

(f) Gastro

(g) Surgical

(h) Skin

(i) Ophthalmology

(j) Medicine

(k) Clinical Nutrition

(l) Dentistry

(m) Psychiatry

(n) Cardio

(o) Oncology

(p) Physiotherapy

(q) Ayurveda

(r) Homeopathic

2.3.5 **Outsourced Services**

The hospital has outsourced the following services

(a) Security - 30 persons

(b) Housekeeping and waste disposal - 60 persons

2.4 **Services Provided by Hospital**

(a) Preventive Health Check

(b) Radiology

(c) Path and Lab

(d) Anesthesia

(e) Gen Immunization

(f) Maitri (AIDS)

(g) Care for Senior Citizen

(h) DOT Centre

(i) Kishori Clinic

(j) School Health

2.4.1 <u>Services not catered for in the Hospital</u>

The hospital has not catered for the following services: -

(a) Blood Bank

(b) Mortuary

2.5 <u>Observations/Learning</u>

2.5.1 During the Internship period I was attached with various departments of the hospital. Working in Delhi Government hospital being administered by cantonment board was a pleasant experience. The hospital is being well administered under the present CMO. The major observations and recommendations based on the general analysis of data and observations during the internship period and visits to various departments which can go a long way in improving the hospital is as under: -

(a) **<u>Services Related</u>**

(i) There is already a daily footfall of 850 persons attending various OPDs in the hospital and the trend is that the strength will increase, as quality of services will improve.

(ii) Most of the patients are from middle class, or the lower strata of the society as the hospital is catering to the civil population staying in the cantonment area.

(iii) OPD services are the main stay of the hospital and start early in the morning at 0800h, lunch break is at 1300h, the hospital continues till 1500h.

(iv) A huge rush is there at the registration as well as near the OPD area, which has most of the consultation rooms. There is less rush at Dental, Ayurvedic and Homeopathic OPD area as they in different locations.

(v) There is a common waiting area in the gallery, during the OPD time the patients and their attendants are seen standing in the gallery due to limited seating capacity. There is a requirement to create a bigger waiting area with token number display system to reduce the rush and streamline the OPD system.

(vi) There are some sign boards showing the details of facilities in the hospital, fire prevention measures, hand washing rules, actions to be taken during an earthquake etc. but there is still scope of more sign boards for easy understanding of the patients.

(vii) Registration for OPD is done at the registration counter on two windows where a person has to give his demographic data, which is then fed on the computer at the desk. A yellow slip is physically filled and given to the patient directing him to report to the specific specialist or to a general physician. Once registered the OPD slip is valid till six months. There is a requirement to automate the registration process to reduce the rush as also to ease the data management and billing.

(viii) Once the specialist sees the patient he gives a white chit containing the prescription or an investigation slip if required, this slip can be given at the pharmacy and medicines can be collected. The prescription is also entered in the patients yellow slip for record.

(ix) There is also a requirement to introduce EMR in the hospital.

(x) Most of the prescribed medicines were available in the pharmacy. The pharmacy has an efficient system of storage and accounting of medicine however there is a need to introduce an automated system, which could give real time details of medicines available in the pharmacy to the consultants and assist the pharmacy to monitor the stock and expiry details.

(xii) Emergency casualty services are functional 24 X 7 however the ICU is not yet functional. It would be made functional.

(xiii) The house keeping and security services have been out sourced. There is a high level of cleanliness in the hospital and security staffs both male and female were found to be doing their task efficiently.

(xiv) The Laboratory, Physiotherapy services, Dental, Ayurvedic and Homeopathic clinic were found to be popular and well subscribed.

(b) **Staff Related**

(i) A major portion of the staff were found to be working on contractual basis hence the staff turnover ratio was also found to be very high which effects the efficiency of the hospital. It is strongly recommended to have a 50 – 50 ratio of permanent and contractual staff.

(ii) The hospital has some state of the art medical equipment like Laparoscope, OT table etc but due to lack of the expertise of specialist Surgeons and doctors these equipment has not been used. There is a requirement of carrying out a gap analysis and developing a proper roll on plan for expansion and a coordinated procurement of the equipment and appointment of the staff as per standards of a 100 bedded hospital.

(c) **Miscellaneous Aspects**

(i) **Use of IT**. There is legal requirement of keeping hard copies of the medical document, however, the feasibility of increasing the usage of IT throughout the hospital should be encouraged without compromising on the legal requirement of keeping hard copy of medical documentation.

(ii) **Formation of Quality Circles**. Quality circles should be formed among resident doctors, Nursing Staff, House keeping, etc. so that the experience available amongst the people working on ground is shared amongst themselves for overall benefit of all stake holders.

(iii) **Training**. Increase the pre induction-training period of the new staff and regular structured refresher training for the complete staff.

(iv) **Audit**. Involving of functional staff in audit of all departments as first step in the audit of processes. For that the staff from both medical and non-medical departments can be detailed for carrying out audits on monthly basis. This can help in the self-assessment by the staff and bring in behavioral changes.

(v) **Central Security Room**. There is a need for creating a central security control room with more CCTV cameras installed.

SECTION II: STUDY OF HOSPITAL SECURITY AND ASSOCIATED RISK THREAT AND VULNERABILITY ASSESSMENT AT CANTONMENT GENERAL HOSPITAL, NEW DELHI

3.1 Introduction

3.1.1 Security is a carefully orchestrated balancing act that ensures an open, functional environment of care that effectively protects assets. Typically, a hospital deploys various security measures throughout the facility or campus. These security measures may include policies and procedures, physical security, equipment, security personnel, or some combination of these measures. Security policies and procedures may include a security management plan, workplace violence prevention policy, visitor management policies, and bomb threat procedures. Physical security equipment can include close circuit television systems, alarm systems, access control systems, lighting and perimeter security systems. Security personnel include the proprietary security force, contractual security personnel and other personnel who serve in a protection capacity. Typical physical security measures will depend on the nature of the hospital, however many physical security measures are common across various hospitals for example, closed circuit television is commonly deployed in most hospitals.

3.1.2 Securing the environment of care is a challenging and continual effort there are unique challenges in balancing the open campus environment with the protection needs of the hospital patients, employees, and other assets. No hospital is without security risk and effectively managing risk is crucial to maintaining balance between protection and openness[5].

3.1.3 Hospital security system must effectively mitigate risks. Process consists of the identification of threats and vulnerabilities to the hospital with the end goal of selecting appropriate security measures to reduce identified risks.

3.1.4 By Definition, vulnerability is a weakness or gap in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerabilities are Opportunities[6], Opportunities for losses, Opportunities for rule breaking violations, Opportunities for crime. Vulnerability can be structural, Procedural, electronic, human and other elements which provide opportunity to attack assets[7].

3.1.5 Vulnerability assessment is a system approach used to assess a hospitals security posture and analyse the effectiveness of existing security program. Primary aim of a vulnerability assessment is the security survey which identifies and measures the vulnerabilities at the hospital and determining what opportunities exist to attack by means of checklists that guide the assessment during off site preparations and on site inspections of the facility. Security survey is a fact finding process whereby the assessment team gathers data that reflects who, what, how, when and why of a hospital existing security operations[8]. The basic process of a vulnerability assessment first determines what assets are in need of protection by the facility's security program and then identifies the protection measures already in place to secure those assets and what gaps in protection exist. Assessments identify security weaknesses that can be exploited by an adversary to gain access to the healthcare organisation's assets. Vulnerability assessment's objectives are to maximize life safety, protect assets, and maintain continuity of operations.

3.1.6 Threats are specific events or conditions that seek, obtain, damage or destroy a hospital asset[6]. Historical information is the primary source for a threat assessment however other threats may emerge without a historical context[5]. Threat assessments are more detailed analyses to evaluate the likelihood of adverse events, such as terrorism and crimes that may affect hospital operations; most common form of threat assessment is incident analysis. Broadly speaking, incident analysis is a logical examination of crimes, which have penetrated preventive measures. The frequency of specific crimes, each incident temporal details (day and time), and the risk posed to proper inhabitants.

3.1.7 Risk is the result of threats and vulnerabilities. Without the potential for threat and vulnerability coming together in time and space, risk is undetermined or non-existent. Assessing risk is more of an art than science[6]. The purpose of risk assessment step is to identify risk mitigation strategies, which can be employed to reduce the hospital's risk to an acceptable and manageable level. Mitigating risk involves identifying strategies that can reduce threats and vulnerabilities through the implementation of additional security measures or other means.

3.2 **Need for Study**

3.2.1 There are a multitude of reasons mandating the provision of the proper level of security for the healthcare environment. These reasons include a moral responsibility, legal concerns, complying with accreditation/regulatory requirements, contributing to the provision of quality patient care, maintaining the economic/business foundation of the organization and maintaining sound public, community and staff relations. The joint commission standards and NABH standards require that hospitals identify and manage security risks.

3.2.2 Exact crime statistics for health care institutions are difficult to obtain in India because many crimes go unreported. In USA losses per bed per year estimated to range from $3000 to $3500[9]. Certain industry executives agree that 3% of any operating budget is an accurate measure of crime loss[14]. Kunders et all have estimated that one out of every ten hospitals employees steal habitually[11]. A study over a five year period at West Jersey Hospital in Camden, New Jersey revealed that disorderly conduct was the most common incident, followed by assaults and property damage[12]. Another study at Chicago's 1418-bedded Cook Country hospital found, "Pilferage of hospital property appears to be way of life".

3.2.3 Cantonment General Hospital is a 100-bedded unit (under extension) at present, providing general medical and primary emergency care services. It is one of the premier health services institute. At Cantonment General Hospital, there is a never-ending flow of employees, patients, visitors, salespeople and contractual staff. In the year 2014-15 OPD figures were 2,32,102 whereas in 2015-16 the OPD increased to 3,10,406[4]. A large number of female employees need protection especially during night shift changes. Patients are particularly vulnerable at all times because of their limited Physical capabilities. What makes protection really difficult is that institute remains open twenty four seven for emergency services.

3.2.4 The hospital despite providing the best services is not exempt from violence, pilferage, theft, fraud or other threats. It is imperative for Cantonment General Hospital administration to ensure personal safety of patients and staff to ensure a safe environment ensuring delivery of uninterrupted quality health care. In view of the above study was conducted with the aim to study the hospital security and assess the associated threat, vulnerability and risk at Cantonment General Hospital.

3.3 **Aim and Objectives**

3.3.1 **Aim:** To study the hospital security and assess the associated Risk, Threat and Vulnerability at Cantonment General Hospital, New Delhi.

3.3.2 **Objectives**

(a) To Study the existing security system at Cantonment General Hospital.

(b) To identify likely security threats and vulnerability.

(c) To carryout risk assessment.

(d) To make suitable recommendation, if any.

3.4 **Review of Literature**

3.4.1 The word security has been derived from Latin word *se* meaning without and *cura* meaning care. Webster's New Collegiate Dictionary defines security as "quality or state of being secure, freedom from danger, safety, freedom from fear or anxiety, protection, measures taken to guard against espionage or sabotage, crime attack, escape, an organization or department whose task is security."

3.4.2 The term security or protection for healthcare facilities is often vague. It is in fact a relatively ill-defined concept that can and does take on different connotations in different settings. In the context of protecting healthcare facilities security can be generally defined as a system of safeguards designed to protect the physical property and to achieve relative safety for all people interacting within the organization and environment.

3.4.3 This definition leaves the problem of defining relative safety. What is safe today may not be safe tomorrow. It is difficult to evaluate the environment of a particular facility to determine the relative safety has in fact been achieved and such evaluation are somewhat subjective in nature. The realistic goals for protection, or security, is intended to reduce the probability of detrimental incidents and mitigate incident damage, not necessarily eliminate all such risks. Therefore security is static and can be viewed as a state or condition that fluctuates within a continuum. As environmental and human conditions change so does the status or level of protection. It is this phenomenon that requires organisations to constantly evaluate and re evaluate their system of protection on a continuous basis.

3.4.4 Aspect of Hospital Security

Oliver and Wilson have cited that the nature of hospitals gives rise to the following unique range of problems[13]-

(a) For a large part of the day the public have virtually unrestricted access while visiting patients.

(b) There is a constant legitimate activity throughout the 24 hours using numerous entry points to the buildings.

(c) The nature of some ancillary work is such that it does not attract a high caliber of employees and there are ample opportunities for petty pilferage.

(d) In some jobs, like portage, there is an unquestioned right to be anywhere in the premises.

(e) The premises hold a wide range of targets-drugs, office and technical equipment, clothing, cash, food – everything.

(f) The presence of nurses and their residences attract sexist attacker types.

(g) Casualty receives injured and obstreperous drunks who are increasingly apt to assault staff.

(h) The importance of the prime purpose of the hospital is such that security has limited priority.

3.4.5 **Threats to Hospitals**

Colling has identified that the security related vulnerabilities of healthcare institutions range from simple pilferage to homicide and terrorist attack[10]. Lists of possible risks to which a hospital may be subjected are shown in table 3.1.

Table 3.1: Hospital Security Risks and Vulnerabilities

1.	Assault
2.	Burglary
3.	Bomb Threats/Bombing
4.	Civil Disturbances
5.	Destruction of Property
6.	Drug Abuse
7.	Fire
8.	Gambling
9.	Hostage
10.	Homicides
11.	Identity Thefts
12.	Imposters
13.	Kickbacks/Frauds
14.	Kidnapping/Baby Swapping

15.	Loss of Information
16.	Patient Elopement
17.	Robbery
18.	Strikes
19.	Sexual Assault
20.	Terrorism
21.	Theft

3.4.6 **History of Hospital Security**

(a) The beginning of hospital security can be traced back to 1552 when “ The Order of the Hospital” now known as job descriptions, was implemented at St Bartholomew Hospital in London. The Office of the porter was responsible for beadles or the station guards. Later some hospitals in major cities of United Kingdom employed a security officer known as house detective. In 1950’s and 1960’s the position title was changed to security advisor. During the early 1970 hospital made a concerted effort to create more efficient protection systems. Today the most senior position in hospital security is that chief security officer[15].

(b) During the first half of this century little mention was made of security in the hospitals in USA. The Basic protection activities were performed entirely by maintenance crews as they completed their physical plant duties. As facilities grew in size some hospitals hired a guard to make the rounds. The primary emphasis of the guards round was the fire watch.

(c) After 1950’s as the criminal activities were beginning to be noticed in and around hospitals, the emphasis shifted from fire watch to law enforcement and police officers began to be stationed at the hospital. In 1960’s hospitals became aware that protection of organization was not limited to illegal activities. The need was perceived of a specialized management service touching all departments and functions of healthcare organization. The need was creation of a security department that reported to a administrative level position. During the period 1975 – 1990 management services concept continued to grow. However the definition and day to day functions of security expanded to include safety as well. Many security departments became so involved with safety that they were renamed security and safety.

(d) In the 1990's rapid change began to take shape. The concept of risk management was introduced and security personal was accepted as an important team member in the overall management of the organisation[10]. Managers realized that risks can be never eliminated but it is possible to reduce the likelihood of incident occuring[9]. Presently security is becoming more and more dependent technology at the same time criminals exploit technology to commit their crimes, the extent of which is limited only by technology innovation and offender's imagination. Today a thief can steal without trespassing by using a computer and modem from the comfort of his home[16].

3.4.7 **Hospital Security in India**

(a) There is no documented history of hospital, security in India and the primitive system of 'Chowkidars' manning the entry points continues in most hospitals. However reports of various committees instituted by the government have stated their concern with security in hospitals. The Jain committee report recommended that all costly equipment not in use should be kept locked and an officer be responsible for its custody. It underscored the importance of regular checking of stores to reduce pilferage. The report stressed the need to pay attention to the security aspect, while designing a hospital building[17].

(b) In 1989, the Trained Nurses Association of India highlighted the risk to their personal safety in a memorandum submitted to the High Power Committee on Nursing and Nursing profession. The Association appealed to the Government to study the drawbacks in the personal security system and safeguard nurse's life and honor as women. The memorandum emphasized the danger to the nurses from their employers, fellow workers and social elements and those visiting them for professional work, especially during the night and evening shifts[18].

3.4.8 **Crime Statistics for Health Care**

(a) Exact crime statistics for health care institutions are difficult to obtain in India because many crimes go unreported. In USA losses per bed per year estimated to range from $3000 to $3500[9]. Certain industry executives agree that 3% of any operating budget is an accurate measure of crime loss[14]. Kundars et all have estimated that one out of every ten hospitals employees steal habitually[11]. A study over a five year period at West Jersey Hospital in Camden, New Jersey revealed that disorderly conduct was the most common incident, followed by assaults and property damage[12]. Another study at Chicago's 1418-bedded Cook Country hospital found, "Pilferage of hospital property appears to be way of life".

3.4.9 **International Association for Health Care Security and Safety (IAHSS)**

It was formed in 1968 as International Association for Hospital Security and in 1990 changed to the IAHSS. This Association is the primary resource that designs, shapes and affects the scope of practice in health care security. It was incorporated in the state of Illinois in 1968 as a not for profit, private organization. Hospital security functions as identified by IAHSS are given in Table 3.2.

Table 3.2: Hospital Security Functions As Identified by IAHSS

1	Uniformed Patrols
2	Elevator Operators
3	Information Desk
4	Lost and Found
5	Key Control

6	Identification
7	Finger Printing
8	Education of Employees in safety and fire Protection
9	Accident Reports on Hospital Grounds
10	Manual of Procedures
11	Disaster Procedures
12	Training Security Officers
13	Alarm Systems
14	Maintaining good relations with Official Police
15	Transportation
16	Decreased Patient property

3.4.10 **Principles of Hospital Security**[19]

(a) Roper has described the four cardinal principles (4D), which guide the security program of any facility:

(i) Detect the potential intruder at the entry point as attempt into the facility.

(ii) Deter the intruder so that if he/she does attempt to enter then appropriate security response will be initiated at the earliest possible moment, increasing the chance that the intruder will be caught.

(iii) Delay the intruder so that he/she is apprehended before achieving the objective.

(iv) Deny the intruder any further access to particular target within the facility.

3.4.11 **Law Enforcement and Security**

Some common ground may exist between law enforcement and security however at least 90% of their respective activities are different. Table 3.3 shows the general differences between law enforcement and security. Most important difference is that of “administrative remedy”.

Table 3.3: Comparison Law Enforcement and Security

Law Enforcement	**Security**
Protecting a Society	Protecting an Organisation
Apprehension of Offenders	Prevention of Incidents
Legal Remedies	Administrative Remedies
Tax Supported	Private and Tax Funding
Statute Defined	Organisation Defined
Public Opinion	Return on Investment

3.4.12 **Security Vulnerabilities and Risks** [10]

Health care Organisations have their own set of inherent security in securing a patient care facility. The risk levels may however vary according to the unique operating environment of the organization.

3.4.13 During the process of a security risk assessment it is important to keep in mind the subtle differences between a security audit, security survey, risk assessment and security program review. The audit is rather narrow in focus to determine the validity and operational aspects of a specific element of the security program. The security audit is to determine if a defined element of the security system is operating in the manner intended and producing the end result as expected. In security we most often refer to this term relative to a review of a procedure to determine the degree of compliance with the procedure process and the need to make appropriate changes for identifying the need for training. A security survey is a more random evaluation of the overall program to determine the completeness, acceptance, strengths and weaknesses in the program. The risk assessment is conducted to identify and evaluate security risk by the level of protective measures (safeguards) in place to manage an expectable level of risk. The program review is much the same as the survey, however it will often focus on a specific area of security such as the emergency department, mother infant unit, or change in space design.

3.4.14 The foundation of a healthcare organization protection system is the identification and assessment of the types of threats and degree (Impact) of damage if the threat becomes an actual occurrence. When a threat progresses to actual event organisations viability is diminished in varying degrees depending on the magnitude and seriousness of the resulting damage.

3.4.15 **Structure of Security Risk Assessment**

Checklists and guidelines are only resources that may assist in the review process. A security risk assessment of a healthcare facility need not be overly structured. There are no ready made checklists that fit every organization. Every facility is unique.

3.4.16 **Risk Assessing**

(a) Each of the security risks identified must be assessed in terms of the degree of threat (real, Perceived, and potential) to the organization. In rendering this assessment basic source of information should be utilized. These information sources can be facility and on site survey, checklists, security incidents and crime statistics.

(b) Analyzing risk in terms of real or perceived threat is easily addressed than in terms of potential threat. Environment criminology is the study of the spatial patterns of wrong perceptions and space awareness of the criminal, criminal patterns, target selection and decision to commit a crime. These factors pertain more directly to crime outside the organization, they do relate to varying degrees of internal and other negative acts.[21] Security program safeguards should have some relation to the level of threat.

3.4.17 **Risk Assessments of Security**

The objective of security risk assessment is to identify primary mission and operations, assets of health care organizations (HCO) or healthcare facilities (HCF's), threats to and vulnerabilities of those assets, and develop reasonable risk mitigation strategies to protect assets. Strategic risk assessment process is as shown in Figure 3.1. Security risk Assessments should be conducted on a regular and ongoing basis.

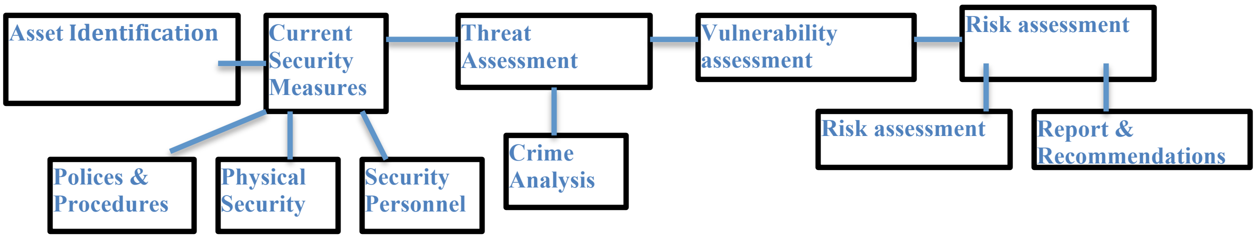

Figure 3.1 : Strategic Risk Assessment Process

3.4.18 **The Components of Security Program**

Security program is made of basically three components shown in figure 3.2

(a) People - Patients, Staff, Visitors

(b) Process - Policies and Procedure, Plans, Training

(c) Technology - Access, Intrusion,Video

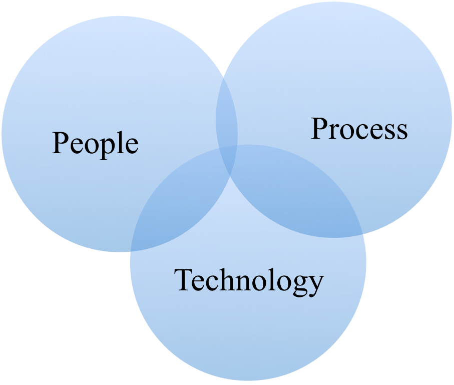

Figure 3.2: Components of a Security Program

3.4.19 **Security Management Plan**

A security management Plan (SMP) is a description of the protection program developed for an organization after evaluating security risks and threats to the organization. An SMP however is a necessary element of managing any healthcare organization.

3.4.20 The security function should not be applied in a manner that it is unduly restrictive in terms of the operational efficiency of providing quality patient care.

The security function cannot be static rather it must continuously evolve to meet the changing needs of times and must remain flexible to cope with the constant changing security risks and vulnerabilities that occur in a patient care enviornment. It must also be constantly evaluated to ensure that the protection function is future organisations objectives and needs.

3.4.21 Security programs must be structured to organisation within the restrictive factors of organisation mission, vision and core values, physical design, community demographics, employee and public, the budget and resource availaibility and the requirements of the facility.

3.4.22 **Fundamental Goals of Security Program:** The fundamental goals of security program are as under which are also depicted in figure 3.3.

(a) Environment – CPTED, Design and Construction Standards

(b) Access – Barriers, locks, Signage

(c) Detection – Surveillance, Patrol, Alarms

(d) Response – Intercom, Security/ Police, Employee, Recording

(e) Security Culture

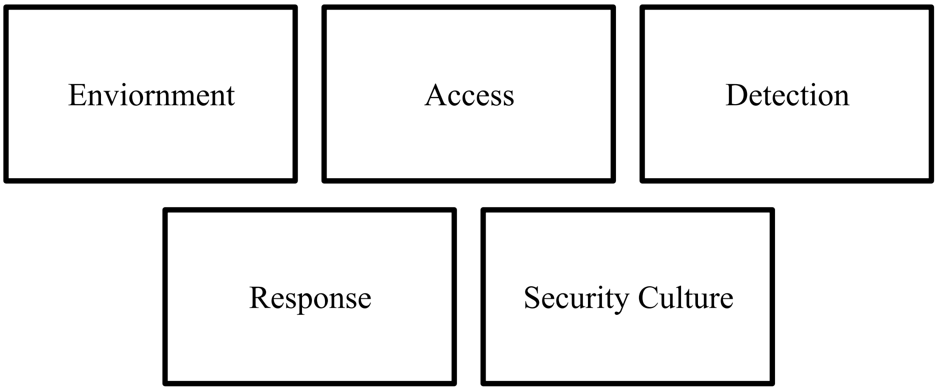

Figure 3.3: Fundamental Goals of Security Program

3.4.23 **Reporting Level and Support**

Security is considered an element of administration. It is required component of security management Plan which clearly specify the position that has the responsibility for security of the organization and has a clearly defined reporting levels for this position. The hierarchical level in the organization to which the security reports reflects the importance that administration pays on security function, and the organization's responsibilities for protecting persons and property.

3.4.24 **Types of Security Force**

(a) Several options are available to healthcare administration for selecting the type of security force to serve their facility. Each of the different models of staffing has its own advantages and disadvantages. The four basic types of security staffing are Proprietary staff (In house), Outsourced staff (contract services), Proprietary security manager or supervisory staff with out sourced security officers and off duty law enforcement personnel.

(i) **Proprietary Staff :** Proprietary staff simply means that that the security department personnel are employees of the organization.

(ii) **Outsourcing:** Since security is not one of its core functions, many hospitals in Europe and majority in US are opting for outsourcing of security management. David Parker has elaborated on the advantages and disadvantages of contract and in house security[22]. These are depicted in Table 3.4.

Table 3.4: Advantages and Disadvantages of In house & Contract Security

	Advantages	**Disadvantages**
In-house	Loyalty to the hospital	Employees hard to Discipline
	Knowledge of the Hospital	Familiarity can breed lax attitude
	Training overseen by the hospital	Less Flexible
	High Control	High long term costs
Contract	Fixed cost, lower payroll costs	Lowest bidder often selected
	Flexibility can provide additional security officers as needed	Lack of Loyalty
	Always available or Sickness	No vetting of staff possible by the hospital
	Relives the organization of administrative burdens	Lack of knowledge of the hospital environment

(b) Comparison of the use of healthcare Security staff models over 10 Year period is shown in Table 3.5. It should be noted that the Security and IAHSS Healthcare Benchmarking Study results showed that 77% of the 582 Hospitals responding stated that their facilities utilized a proprietary security-staffing model[23].

Table 3.5: Comparing the Use of Healthcare Security Staffing Models

Staffing Model	**1980**	**1990**	**2000**	**2010**
Outsourced/Contract	24%	30%	52%	55%
In House/Proprietary	64%	60%	34%	31%
Combination of Proprietary and Contract	8%	7%	13%	13%

(c) Irrespective of the source of manpower a security guard needs to be physically fit, correctly dressed and equipped. They should be provided at least basic security guards training and possibly follow up program so that they are conversant with the layout and operation of different departments of the hospital. The training would include mock up situations, anticipated threats and prescribed response besides testing for reactions in unfair circumstances[24].

3.4.25 **Authority of Security Officer**

(a) Most healthcare security personnel operate with some authority more than the ordinary citizen.

(b) The authority of officers to act on behalf of the organization should be clearly delineated in organization. Security officers act as agents of the organization who have been engaged to protect, and thus their jurisdiction is within the organization. Jurisdiction, in this regard, is the legal right to exercise authority.

3.4.26 **Staff Strength**

(a) Specialists in the field of hospital security do not prescribe any index. Rather advocate a well trained, Motivated and well equipped security force. The number of security persons required is affected by security hardware application and organization policies. Srinivasan and Chunawala have suggested that the security function in a hospital be vested in a security officer, assisted by one or two assistant security officer, security guards as required depending upon the necessity and policies of organisation[25].

(b) The number and types of security personnel required for efficient security program is fundamental question for any facility. It is not easy as applying a simple formula for example square feet of buildings, campus acreage size, number of beds, number of employees, comparisons to "Like" facilities, or any other profile data. It is specific to an individual facility since the numerous factors that must be considered vary in depth and scope from organization to organization. To arrive at the required number of security personnel, it is necessary first to analyze and understand the security mission, determine the level of the organisation's security risks and vulnerabilities to be managed, review physical safeguards in place, and identify the various services to be rendered. The next step is to design a program that will support the mission, properly manage risks and implement the intended services. Only then can the number of staff required to operate the program be determined.

(c) The hospital staffing norm suggested is one security guard for every 15 hospital beds in every shift[26]. Based on the US healthcare industry trends, Benjamin & Kemppainen have recommended one security officer per 250 bed capacity of the hospital as the minimum standard. The ideal in their opinion would be one security officer per 160 beds, if the financial resources permit[27].

3.4.27 <u>Selecting Security Personnel</u>

The security personnel are among the first people visitors see, so they should be able to create positive feelings about the facility and enhance the perception of safety within the organization. In short, the protection program needs a reliable professional team where the security employees are ambassadors for the organization and the customers they order to provide professional security officers, not just security guards, the healthcare protection program must be comprehensive, effective programs for recruiting, selecting and retaining high quality individuals.

3.4.28 Basic Traits and characteristics necessary for security personnel

(a) **Confidence -** Successful security officers should have the capability to rebound from negative feedback or criticism and have the ability to approach and respond to situations in a self assured and consistent manner.

(b) **Assertiveness -** A security officer must be direct and persuasive when dealing with others, have the ability to influence or direct a self desired outcome.

(c) **Empathy -** In general, an officer demonstrating empathy will be open mined and flexible and should have the ability to identify, understand, and relate to the needs and reactions of other people.

(d) **Helpfulness -** Accommodating, service minded, and team spirited, the healthcare security officer should be internally motivated to help others and work as part of a team.

(e) **Problem Solving –** Dealing with problems and issues that are complex and unique is a frequent requirement of security officer. They need to understand and possess the ability to resolve routine problems.

(f) **Sociability -** The activities and tasks of a health care security officer provides ample opportunity to interact with other people. Security staff should be friendly, outgoing, and possesses the ability to initiate contact with others.

(g) **Thoroughness –** Conscientious, with careful attention to detail, to protect a healing environment requires those individuals who take a personal sense of responsibility for the quality of their work.

3.4.29 **Training :** One of the most critical challenges and of the basic responsibilities of the security administrator is to identify the means for each person in the security department to reach the competency level required to perform the function as per the job description.

3.4.30 **Uniforms**

(a) Security personnel should wear a traditional uniform or a blazer and slacks. The consensus of healthcare security administrators is that security officials should not be outfitted in plainclothes. The uniform should not be designed to represent uniform of any law enforcement agency.

(b) Name plates, Badges, organizational issued identity and recognition pins are commonly found on security uniform. Each serves an important purpose and can be a source of pride for the officer. The style, color, and type of badge are often controlled by local or state regulations.

3.4.31 **Identification Badges**

Healthcare organisations must provide identification to each employee. It is a common practice to provide this identification utilizing a picture badge to be worn by all staff. The rapid use of electronic card access systems in HCFs has resulted in one badge that has multiple uses. The identification card utilized in healthcare provider organizations has several purposes. One purpose is to function as a basic element of access control system and to accomplish an electronic keeping function. Second, it serves the purpose of compliance to JCI standard, which requires that all patients have the right to know who the person is providing direct patient clinical care.

3.4.32 **Identification Badge Program**

There are several key security issues relative to administration of staff identification systems. First, the system provide for expeditious replacement of lost or stolen cards or badges. However, replacement procedures often make it easy for staff to obtain two badges. A major advantage of the electronic card access identification system is that a badge can be immediately deactivated. The most common problem in any employee badge identification system is obtaining compliance of displaying the badge as prescribed. A certain number of employees will always resist, and organisations must be prepared to provide strong administrative support.

3.4.33 **Arming Officers**

(a) At present approximately 12 percent of US, healthcare security officers are armed[28]. The November 2007 IAHSS/GE security survey of 579 US hospitals illustrated that 19% of hospital security departments arm their security officers with full firearms[23]. The correct decision on whether to arm security persons for a given organization requires consideration of many different factors. Among these considerations are personal safety, vulnerability, liability, deterrent value, environmental profile, geographical setting, degree of crime in and around the facility, and quality of personnel.

(b) A firearms policy is mandatory. The policy must be clear, concise, and understood by every officer.

(c) Weapons are often found when metal detectors are used to screen persons entering emergency departments[28]. A study at Henry Ford Medical Centre, Detroit, MI, reported ten percent of people arriving at their emergency department carry weapons to some points in the hospital.[29].

(d) All officers who carry firearms should complete a firearm weapon affidavit.

3.4.34 **Handcuffs**

Security officers may need to use handcuffs for custody and control of persons arrested as required. However, the Centre for healthcare and medical Services (CMS) does not consider the use of handcuffs or other restrictive devices in the healthcare institutes as safe and appropriate [30].

3.4.35 **Use of Force**

The use of force by health care security officers is some times necessary to maintain order and safeguard staff, patients, and visitors in a healthcare environment. The security officer must occasionally use a certain amount of force, from mere pressure and verbal persuasion to physical intervention to overcome resistance and ensure compliance with hospital policy and medical care plans. Every healthcare facility should evolve a use of force policy.

3.4.36 **Requesting for Police**

General policy should prohibit healthcare staff from calling for police service as a representative of the organization. Healthcare organizations with full time security effort a authorized representative should make the call for required police service. Organisations without full time security service, the policy should designate an administrator who will not only approve the routine police service, but also generally initiate the call.

3.4.37 Manning Access Points

If all the people entering and leaving a medical care complex could be properly surveyed and controlled, the protection requirement would be quite high. While relatively free access to hospital could be the norm during the day, there is a need to reduce uncontrolled access during the evening and night hours. A general plan is to lock designated entry points at 16: 30 PM and to lock access points at the termination of designated visiting hours. All facilities should designate specific controlled entrances for late night patients and visitors.

3.4.38 Security Staff Scheduling

There are generally two types of schedules – the monthly schedule, which covers a specific time period in advance, and a working schedule, which is a day-to-day document that reflects the actual officer who filled the shift. The master schedule when properly constructed, can be modified each day to reflect any changes in actual shift and/or post assignment.

3.4.39 Patrolling Activities

Security operations are primarily concerned with force deployment, which includes response to requests for service, fixed- post assignments and general service response to critical incidents.

3.4.40 Basic Patrol Concepts

Patrol can best be examined by the separation of patrols into external and internal.

(a) **External Patrol:** External patrol generally covers the grounds, parking area and streets surrounding the facility buildings. External patrols are intended to protect vehicles and people entering or leaving campus grounds. Officers on external patrol provide perimeter protection. A major responsibility of external patrol is to ensure the integrity of facility access points by frequently checking doors, windows, roof access, and fire escapes to preclude unauthorized use. The basic types of external patrols are foot patrols, bicycle patrols, vehicle patrols, personal transport vehicles, or a combination of each. Regardless of the type of vehicle used for patrol, they should be easily identifiable as security vehicles. To be an effective deterrent, it is not enough that the protection capability is present. It must also be highly visible to the people being protected and to those who might be contemplating a criminal act. Patrols on bikes are friendlier; security officers become approachable and less threatening. The bike patrol support traffic flow, render assistance and further extend the presence and effectiveness of our security force[31]. Using transporters, security staff are also more alert and less fatigued when they have to respond quickly to a situation versus running or pedaling on a traditional bicycle.

(b) **Internal Patrol:** Effective preventive patrol is the backbone of a deterrent program. Patrol is not just walking down the corridor or through an area it requires being alert and checking and observing with all five senses.

3.4.41 **Purpose of Records**

Records provide a memory system, permit the exchange of information, fulfill administrative needs, assist in the verification of the activity, direct operational procedures and general planning processes.

(a) **Memory System:** The need to retrieve information contained in a report occur within hours, days, or even years after it was completed.

(b) **Operational Policy and Procedures:** Security operations require policies and procedures to execute the proper delivery of emergency and routine security service actions. A goal of security operations is to achieve professional and consistent actions by all the security staff in the discharge of their daily responsibilities.

3.4.42 **Format of Report:** The style/format of security reports depends on individual preference, but it must be designed in a manner that assists the report writer in preparing a complete report in an efficient manner. The main consideration is simplicity.

3.4.43 **Daily Activity Report**

As a basic rule, all field officers should be required to complete a report of their activities during their tour of duty. Examples of entries in daily activity report include assistance to motorists, the reasons for not accomplishing schedule rounds. unplanned or unscheduled activities such as escorts or the name of a person not permitted entry to a closed area.

3.4.44 **Security Incident Report**

The basic record found in all security operations is the security incident report (SIR). This report should not be confused with the unusual incident report (UIR) that is commonly utilized for clinical staff to report medication errors, patient falls, and other clinically related situations. These two types of incident reports (SIR and UIR) should be maintained separately and combined into single multiuse form. The SIR, in aggregate, is the primary source of data, which identify past security incidents or situations occurring at a facility or within a hospital system. The most common method of presenting this information is via statistical reporting of the number of incidents, by incident category, for a specific time period in a spreadsheet format.

3.4.45 **Records Retention**

The absence of a document retention policy could lead to an accusation of destroying evidence if a particular document cannot be located. This is commonly known as spoliation of evidence and could constitute an obstruction of justice criminal offence[32]. Guidelines for record retention varies from organization to organization however common practice should be as shown in Table 3.6[10].

Table 3.6: Guidelines for Record Retention

Security incident report	5 years
Monthly or annual activity reports	5 years
Annual security evaluation reports	5 years
Parking violation/reminder notices	1 year
Security condition reports	6 months
Security officer daily activity reports	3 months

3.4.46 **Patient Care**

(a) The nurse assigned to a patient is responsible for his total care, which includes the safety of the patient. Nurses however, receive support from the security system in protecting the patient just as they receive support from other disciplines administering medical care.

(b) The basic protection for inpatients comes from the hospital unit staff, which consists of nursing personnel, unit clerks, entry persons, and ancillary staff. It is extremely rare that security personnel routinely interact with patients on a proactive basis.

(c) Nursing staff must be acutely aware of who enters the hospital and for what purpose; especially during after hour periods. Just as the security role becomes more custodial during the night hospital nursing assumes a more custodial role for the patients safety of course, nursing staff have a responsibility during operational periods to challenge strangers on the unit or in patient room at any time.

(d) A common medical record form used in many hospitals is the LAMA form. It is normally used for patients who, after admission, decide they do not want to stay in the hospital. If unit personnel cannot persuade these patients that it is in their best interest to remain, the patients are asked to sign the form stating that they acknowledge that they are leaving AMA. Patients can refuse to sign the form and should be allowed to leave.

(e) LAMA is different from elopement or patient wandering and is determined by the patient's decision to leave the facility having been informed of and appreciating the risks of leaving without complete treatment.

3.4.47 **Patient Risk Groups**

Certain patient risk groups require specific attention relative to security. These basic groups are identified by patient type and include the combative patient, VIP patient, forensic patient, the wandering patient, the infectious patient, behavioral health patients, patients with autism, and the infant/pediatric patient.

(a) **The Combative Patient**

(i) Security personnel assist with combative patients most often in four areas of the facility: the emergency department, the intensive care units (ICUs), the mental health areas, and the general nursing unit and medical clinics.

(ii) The emergency department requires frequent security assistance, especially in facilities that treat many drug overdose patients, patients with injuries due to shooting or stabbing incidents, and patients with mental health or alcohol/drug impairments. Waiting areas of the ICU are a common location for family members and visitors of the patient to express great emotion.

(iii) Elopement is always a concern when treating the mental health patients. It is reported that 3- 15% of all patients admitted to mental health units elope each year. Certain sources suggest that there are identifiable characteristics of the patient who is prone to elope. Such sources indicate that these patients are generally male and usually verbalize a desire to leave prior to elopement. Often they have eloped on prior occasions and have schizophrenia or a mood disorder[33].

(b) **The VIP Patient**

(i) The VIP patient is any patient who poses special security problems and may require certain security precautions to be taken. For celebrities and high profile politicians, strict visitor control procedures may be required. In some cases their own security personnel accompany these patients. The hospital's protection service thus has little responsibility for the patient's security. This is especially true when a government figure is involved. Special telephones, quarters for protection personnel, special visitor passes, and the like may require considerations.

(ii) The same type of security safeguards and procedures are utilized for each type of VIP. However the degree of the security precautions and activity will vary with the specific patient status. In general the security precautions and safeguards could include the following actions:

(ia) Notify appropriate organization personnel including top Management, of patient identity and circumstances requiring increased VIP security measures.

(ib) Notify public safety agencies if deemed appropriate and coordinate efforts with these agencies.

(ic) Assign a patient room that is away from elevators and stairwells or exits.

(id) If security officers, bodyguards, or forensic staff will be utilized assign a patient room at the far end of a corridor. If this type of personnel is not utilized assign the patient a room close to the nursing station where good surveillance of the room can be maintained.

(ie) Remove the patient name from the patient information system, Front desk, and census reports, substituting an assumed name for the actual patient.

(if) Maintain the patient's chart in the patient's room.

(ig) Brief the nursing unit staff of general information and specific action items required of medical care staff.

(ih) Determine if any visitors will be allowed.

(ij) Obtain name and telephone number of person(s) co-coordinating security for the VIP who can be contacted as questions arise or if there is an emergency. This contact person may be a family member.

(ik) Utilize security officer briefing procedures to communicate information to all security personnel.

(c) **The Wandering Patient**

(i) Wandering patients are a security concern presented certain types of dementia patients, most frequently those with Alzheimer's disease.

(ii) A patient movement control system utilizing electronics is a fairly common safeguard for suspected wandering patients. The patient wears a tag that contains a radio frequency circuit, which communicates with a detection sensor usually installed in the exit door or elevator openings.

(d) **MLC/ Forensic cases**

(i) The forensic patient may either be brought to the health care facility for emergency or outpatient treatment or for a post hospitalization as an inpatient. In all the cases, the forensic patient must be viewed as a potential threat to the facility. Most health organizations do not have holding cells or other security places commonly found in the jail or corrections facility.

(ii) Confusion and conflict can take place when caring to forensic patient. It is important that the prisoner remain in custody of the correctional officer at all times. Medical caretaker should never ask to remove restraints unless medically required. Sometimes handcuffs, belly chains, and shackles must be removed for MRI imaging procedures, X – rays at the restraining or other procedures that may genuinely be in compatible to standard police restraints. Managing unrestrained prisoners in any environment is inherently dangerous and should not be tolerated.

3.4.48 **Patient Property**

(a) A highly visible and troublesome security problem is missing patient property. The impact of property loss on a sick patient and the negative public relations that result indicates a concern far more important than the value of property involved.

(b) When patients are admitted, the person who signs the admissions form should be required to initial a statement that the hospital is not responsible for personal property not in its possession or control. The patient should be advised to surrender for safe keeping any keys, credit cards, jewelry, watches, and money over a established limit.

3.4.49 **Visitors**

(a) Areas of the hospital that present special visitor control considerations are the medical/surgical patients units, pediatric units, obstetrical units, behavioral health units, ICUs, the medical treatment area of the emergency department, and isolation units.

(b) People who are stopped by the security and questioned concerning their business can often become annoyed or hostile regardless of the approach or intent of the security officer.

(c) Most hospitals define specific hours for visiting patients. Specialized units, such as the ICU, are often more restrictive, limiting the number of visitors, placing minimum age restrictions for the visitor with a predetermined maximum length for an individual visit.

(d) A visitor control plan used during regular visits should be considered as the minimal protection for the patient only as a screening procedure at best.

3.4.50 **Elements of Crime**

There are three basic elements necessary for a crime to occur, a criminal with a desire and ability to commit a crime and a victim who provides an opportunity for the crime. Healthcare facilities, by their very nature, can afford ample opportunities for crime. Involvement and participation of employees in security awareness activities can be one of the most cost effective components of the healthcare protection program. Employees can do a great deal to reduce the opportunity for crime in the hospital. This requires that staff be given clear direction and sufficient training and education. Security training should begin with the first day of employment and continue through to the end of the individual's service to the organization.

3.4.51 **Physical Security Safeguards**

(a) The basic definition of physical security applies as well to non electronic and electronic physical security measures.

(b) **Barriers:** Barriers are one of the oldest forms of physical security. These are either man made or natural. Common manmade barriers currently being used in healthcare security programs:

(i) **Locks and Keys:** Locking devices of all kinds are a primary element in virtually all security systems. Electronic locking systems are rapidly replacing the traditional lock and key systems for many areas of a facility.

(ii) **Marking Property:** Conspicuously marking organizational property is a cost effective means of reducing property loss. Asset number tags, although important, do not deter theft to any extent and can generally be easily removed. Marking hospital property serves the following purposes, it identifies the ownership of the property in case of theft, it assists with management accountability controls (inventory), it provides a visible sign that the property being removed is hospital property and it serves as a deterrent to theft.

(iii) **Fencing:** Surface parking areas are prime locations for fencing. The basic premise behind fencing parking areas is criminals do not want to engage in their criminal acts where the means of escape is limited. On the other hand it may limit the victim escape route. General experience however demonstrates that properly fenced areas are considerably safer than unfenced areas.

(iv) **Lighting :** Security professionals generally agree that exterior lightning is one of the basic and cost effective components of protection program. Exterior lighting serves two distinct purpose, safety and security. Safety lighting provides the means for persons to navigate the exterior, avoiding slips, falls, and environmental obstacles. Security lighting, on the other hand, is designed to discourage criminal activity and to provide light for surveillance purpose.

3.4.52 Technology in Security

Since the vulnerable assets of the hospital are spread at different locations and availability of manpower is limited, it is not possible to manually protect an asset round the clock. The services of the security personnel need to be strengthened by technical support. There are many technologies that assist healthcare security staff in preventing crime. The key electronic security systems most frequently grated into the healthcare protection program are in detection, access control, and video surveillance. The application of technology in hospital security system can broadly be divided into two categories detection (Closed Circuit Television (CCTV) Intrusion Detection System) and denial (Access Control System).

3.4.53 Security Control Room /Central Security Station

The efficient operation of a protection system requires there be a center, or hub of operations. One of the basic functions of the central security post is to handle security communications. To maintain a high level of protection, each employee must report problems and suspicious activity to security. The easier it is to contact security, the more the employees will be motivated to participate in prompt reporting of incidents or requests for service. The station monitors security, fire, and critical electrical/ mechanical building functions, and also serves as the operational center for a variety of security and management services.

3.4.54 Alarms

A basic component of most electronic security programs is an alarm system. Alarm systems have many fire detection and warning applications however, use of security alarms in the healthcare environment continues to increase. It should be properly planned, installed, and used. The alarm system is a very cost effective component of the proactive security system.

3.4.55 **Electronic Access Control Systems**

Today's electronic access control programs can protect "itself from itself" by requiring double or triple authentication for access to those areas that require the highest levels of restricted access, such as the pharmacy, narcotic dispensaries, and IT server rooms. Multi application functionality (access control, time and attendance) enhances security through encryption and mutual authentication.

3.4.56 **Access Control System**

(a) Access control system identifies and permit only authorized persons to enter a protected area. Any one of the two principally different systems can be used.

(i) **Digital keypad system**. These system permits access when keyboard is punched in correct sequence.

(ii) **Card Reader System**. Access is controlled by digital card through the card reader. The card is encoded with necessary data for admission. The card reader admits card with pre-determined data is presented. Proximity can be used in place of simple cards, where instead of inserting the card in the slot, the badge is passed near the reader. Variation of card reader system, called dual discrimination is being used to protect movable valuable assets and prevent infant/child abduction in many Western hospitals.[35]

(b) **Video Door Phones**

Video door phones display an image of the visitor shot real time on the phone's monitor and a built-in microphone speaker on the unit to let the staff member communicate with visitors. Authorized visitors can then be granted entry with push of a single button. The system can help prevent accidental and/or unauthorized entry to susceptible and prohibited areas.

(c) **Closed Circuit / Television Video Surveillance**

(i) The three objectives of a CCTV system are to deter potential crime, improve staff and patient safety, and record evidence that could help identify and prosecute criminals. Mt Vermon hospital in Middlesex, England has reported a sharp drop in crime post installation of CCTV system[36].

(ii) Digital video recorders (DVRs) and CCTV cameras have made significant advances in features and functions, taking advantage of fast computer processes and high- density storage media to digitize, compress, and record video from analog cameras.

(iii) DVRs and Network Video recorders (NVRs) have many advantages over older analog recording technology. Streaming video can be continuously recorded and discarded in cycles of days, weeks, or months if no security incidents occur. If an incident does occur, disk indexing and time stamping make it simple to find video from given date and time.

(iv) Dev has observed that CCTV can be usefully employed in different hospital areas like lobbies, emergency entries, cashboxes, generator rooms, basement, OPD waiting area, reception, VIP section entry, entry to operation theatres, intensive care units, records room and wards[37].

(d) **Biometrics -** Lost identification cards are no longer feared as biometrics or personal identification codes can be required to accompany the card to gain access. Latest technologies include finger print reader and eye/iris signature readers.

(e) **IP Cameras:** Increasingly, electronic security systems are analog to digital, Internet protocol (IP) based equipment transport information that facility staff needs to manage threats. IP based cameras are now more widely accepted and quickly becoming the standard in healthcare industry IP based CCTV systems, camera images are now available anywhere the data network is available, unlike analog system which generally require coaxial cable at each viewing location. Besides providing a digital platform, IP cameras analytics that can be programmed into the camera, frequency network bandwidth and improving storage and processing capabilities.[38].

3.4.57 **Infant Protection Systems**

(a) Infant abduction prevention is a top concern for hospital administrators, and security of infants is certainly a priority, both for safety and public relations reasons. "Infant Tagging," as it is often called, is a high tech infant protection program designed to prevent baby abductions from infant care units, nurseries, and found more and more frequently in pediatric units. Typically, a small round button like tag attached to a band is placed around an infant's ankle or wrist soon after birth. Each tag is actually a miniature RF device that works in conjunction with the access control system and automatic door locks.

(b) Hospitals are increasingly integrating electronic infant security systems with access control and CCTV cameras integrated system can also link infant handling to card holders, activate CCTV cameras, and lock stairways.

3.4.58 **Metal Screening**

There are some areas in healthcare environments that need metal screening. The most likely application in a healthcare setting is the emergency department. Of particular importance to medical facilities is electromagnetic interference (EMI) caused by the metal detectors. Pace makers, defibrillators, nerve stimulators, and other medical devices may be inactivated or reprogrammed by this phenomenon. Instances of this happening have been extremely rare; however studies conducted by the German Heart Institute in Munich, Germany indicate that EMI is not as likely to occur as common wisdom would lead us to believe.[39] All unstable and ambulance transported patients deemed "at risk" should be scanned using a hand held wand once it is medically safe to do so.

3.4.59 **Emergency Call Boxes**

Emergency phones, call boxes, phone towers, or mounted emergency phones are all names used to describe emergency phone system designed to connect a potential victim of crime or someone in need of service with security. They communicate intercom style speakerphone equipped with one, two, or safety buttons[40].

3.4.60 **Crime Prevention through Environmental Design**. The basic concept of crime control through environmental design (CPTED) is that crime can be prevented or mitigated by design of the internal and external environment of a facility to increase crime deterrence and the likelihood of apprehension of criminals. The three basic strategies of CPTED are natural access, continuous surveillance, and territorial reinforcement. Utilization of the strategies produces a proactive, unobtrusive perception by visitors, staff, and patients[30].

3.4.61 **Managing Healthcare Conflict and Violence**

(a) Work place violence can affect or involve employees, visitors, contractors, and other employees.

(b) Violence threatens the safety of staff, patients, and visitors in hospitals and healthcare organisations of all sizes and settings. It demoralizes healthcare professionals, especially nurses, who are most often the victims of violence, and costs hospitals untold millions in lost time, employee turnover, reputation for quality care, and additional security measures[41].

(c) More than one in 10 NHS workers in United Kingdom (12%) reported experiencing physical violence from patients or their relatives in a 2008 survey[41]. A report from Statistics Canada found that patients had physically assaulted 34% of nurses in Canada in 2005. Survey of nearly 19,000 nurses found that more than a quarter reported they had been physically abused by a patient in the previous year.[42] A 2006 Queensland (Australia) Nurses Union survey found that 45% of nurses had experienced some form of violence in their workplace[43].

3.4.62 **Security Sensitive Areas**

There are three major areas of healthcare that normally involve the designation of security sensitive areas, the infant care/birth center, and the section/pharmacy/stores. Other areas in specific healthcare delivery systems may require the organization to declare additional security sensitive areas. These include pediatrics, specialty clinics (such as methadone, detoxification, or research labs, mental health units, and centralized departments.

3.4.63 **The Hospital Pharmacy/Stores**

(a) The security of the hospital pharmacy begins with proper handling, supervision, and training of the pharmacy staff. Personnel hired to work in the pharmacy should be screened thoroughly to establish their integrity. Other employees such as nurses, delivery and even security personnel should be restricted from areas where drugs are stored.

(b) Burglary protection can best be provided by installing physically safeguards, such as protection for windows and ventilation openings, locks, and alarms.

3.4.64 **Logistics and Inventory Management**

(a) **Storage:** Certain areas within the general storeroom should be sectioned off to provide greater protection for particularly vulnerable items, including syringes, blank -credit invoices, and linen.

3.4.65 **Equipment Management**

Equipment should be assigned to a specific department with a periodic inventory is essential. When property is transferred record should be annotated to relieve one department and assigned accountability to the other. Furniture is normally stenciled with hospital's initials or logo. Etching tools are used for instruments and other metal equipment.

3.4.66 Linen Control

The loss of linens in medical facilities of all sizes is generally goes unchecked, healthcare facilities should conduct at least one complete inventory check each year. The discarding of linen should be a controlled practice, and the transformation of discarded linen into rags should be a centralized operation. Rags should be appropriately dyed a specific color and supplied to users to prevent abuse of the reusable linen supply. New linen that has not been put into the system should not be stored in the laundry area. Linen can be ordered from vendors with the hospital's markings.

3.4.67 Cash Management

(a) At the close of the cashier function, or changing of shifts (i.e., cafeteria) , receipts should be taken to the designated central cash management location for accounting and storage.

(b) Persons transporting receipt bags from an operating unit should utilize a locked bag. It is suggested that cash transfers that require the leaving of a building and travelling any distance on grounds be accomplished by two persons. An armored car service is a standard security requirement.

3.4.68 Emergency Preparedness – Management and Planning

(a) **Basic Emergency Planning:** Patient care facilities should perform a hazard vulnerability analysis (HVA) to identify potential emergency events that have the potential to impact the ability to meet a demand for services.

(b) **Fire Safety Programming:** A fire safety program can be viewed as five basic elements – prevention, detection, containment, evacuation, and extinguishment. These elements chronologically define a standard organizational response to a fire threat. Security's role in a fire situation is part of the overall facility fire plan, which includes ensuring that the responding fire department personnel gain access to the facility complex, buildings, and internal areas. This may require unlocking gates or doors, holding elevators, turning on the lights, and even escorting fire personnel to the fire area. Plan includes controlling traffic, including vehicular traffic and people on the perimeter of the fire scene as well as the emergency operations areas, assisting emergency personnel throughout the emergency. Fire plan must include providing fire training and preparing appropriate documentation of the fire incident.

(c) **Bombs and Bomb Threats:** One of the unique features of the bomb threat is the guessing game – Is it real or is it hoax? Where do we check? Is evacuation necessary? These basic questions become the framework of the facility response plan.

(i) **The Bomb Threat Plan:** Basic steps of bomb threat programming can be called as prevention, establishing authority, receiving the threat, searching for the bomb, evacuating the building, terminating the emergency, and documenting the threat.

(ii) **Prevention:** These steps are the same security safeguards that are followed in every day use to protect the organization against security risks. Limited access, access controls, noting suspect people and vehicles, and providing emergency equipment as part of everyday protection system.

(iii) **Establishing Authority:** One of the most important aspects of properly managed bomb threat is to specifically establish organizational authority. Authority and responsibility for handling the initial crisis management designated to a position that is readily available 24 hours a day.

(iv) **Receiving the Threat:** The bomb threat can be received in numerous ways. The most common method is by telephone, and the most common recipient of such information is the operator. Telephone operator and others who are likely to receive these calls should be trained to keep the caller talking as long as possible and to ask key questions, such as where the bomb is, when it will go off, why it was placed, what kind of bomb it is, and other questions that may keep the caller on line. The person who receives the call should make notes or activate a recording device.

(v) **Searching for the Bomb:** The bomb threat information received must be communicated to the designated authority who in turn notifies the appropriate law enforcement authority. In most cases, the law enforcement authority and facility management will decide jointly the type and extent of search required. It is not practical or possible to conduct an all-out search in every case.

(vi) **Evacuating the Building:** The decision to evacuate rests with the facility administrative authority working in cooperation with the public safety agency involved. The evacuation of employees from a given work area presents no serious problems. Any plan for evacuating patients however, must take into consideration the magnitude of the problems involved in moving the helpless and the sick and the medical complications that may result. The level of evacuation is another decision that must be made depending on specific situation. A safe distance for evacuation is generally considered to be a 200-foot radius from the suspected object, including the floors immediately above and below.

(vii) **Terminating the Emergency:** An important part of the organizational reaction to the bomb threat is the decision to end the response. All people notified of the receipt of the threat should also be officially – that the organization is resuming normal operations.

(viii) **Documenting the Threat:** The last step in bomb threat procedure is to document the incident for future reference.

(d) **<u>Terrorism</u>.** A question that continues to be asked is, Are hospitals a likely target for large scale terrorist attack? As one might expect, there are varying answers to the question. Some experts state that the threat to hospitals is very low. Others claim that hospitals are at a high level of risk, as one criterion of the terrorist attack is to create a horrific event. A large scale attack on a large hospital, perhaps even a children's hospital, would no doubt meet the terrorist objective. The general consensus of professional security administrators, however, is that the probability of terrorist attack on a hospital is in the low to low-medium range.[10]

(e) **Strikes and Picketing:** A real test of a facility's protection plan comes when the facility faces strike or picketing situation. A strike occurs when some of the organisation's employees, commonly represented by one or more unions, refuse to work as a protest against a specific grievance or a failure to negotiate a mutually acceptable compromise. Picketing refers to the placement of people around the exterior of the facility for the dual purposes of informing the public of all their problems and curtailing deliveries of supplies and equipment. The primary purpose of Strikes/ Picketing is to allow the dispute in favor of the protestors. The hardships may include disruption of patient care, intimidation of non-striking staff, loss of revenue, damaged or stolen property, negative community reaction toward the facility, and injury to persons.

3.4.69 **Healthcare Violence Management**

There are three specific steps of preparation and prevention that organisations must implement to properly address health care violence. The first step is to provide a reasonable level of security for the overall environment and especially to areas of conflict. This includes an organized security program that has access control plans, proper physical security target enforced security policies and procedures, staff training and empowerment, and an effective critical incident reaction capability. To adequately plan and implement these safety elements, there must be strong commitment from top management and the board of directors to provide a high level of management support.

3.4.70 **Emergency Security Codes**

The use of word, number, or colour codes to annotate emergency condition to facility staff is virtually common in hospitals. All security personnel should be able to identify codes. Uniform codes help in reducing reaction time to a crisis. Common codes are Cardiac arrest (blue), Fire (red), and Infant abduction (pink).

METHODOLOGY

METHODOLOGY

4.1.1 **Study design**: Observational & Retrospective study combined with data analysis with help of validated tools.

4.1.2 **Period of study**: 01 Feb 2017 to 30 Apr 2017.

4.1.3 **Exclusion**: Cyber security, Legal security, Insurance, Disaster, Patient safety aspect, Employee safety and other Cantonment Areas.

4.1.4 **Study setting**: The data for incident analysis was collected and analyzed for Cantonment General hospital, however, the general security survey involved assessment and risk, vulnerability and threat analysis for the entire cantonment.

4.1.5 **Review of literature**: It was done on healthcare security.

4.1.6 **Security Incident reports** for the year 2015 and 2016 were studied and data regarding type and frequency of security related incidents were collected from the records of security officer, supervisor and administrative office.

4.1.7 Based on this historical data of past incidents and review of literature, 14 security related events were selected for this study. These events selected are those that either had a high incidence in the past at Cantonment General hospital or they have the potential to occur in the current environment. Events selected for the study are shown in Table 4.1.

Table 4.1: Security Events Selected for the Study

S. NO.	EVENT
1.	Conflicts/Workplace Violence
2.	Fraud/Imposter
3.	Infant Abduction
4.	Strike
5.	Terrorism/Bomb Threat/Hostage Situation
6.	Theft
7.	Sexual offence
8.	Fire

9.	Absconding
10.	Misbehavior
11.	Suicide/Attempted suicide/General
12.	Hazardous material Exposure/Leak
13.	Traffic management
14.	Animal Nuisance

4.1.8 Incident reports were further used to analyze the following

(a) Examining the annual trend and comparing the number of security incidents in 2015 and 2016.

(b) Location of security incident i.e. OPD/IPD/Emergency/Campus

(c) Originator of security incident report i.e. who originated the security incident report – Patient/Doctor/Staff/Others.

(d) Action initiated by CMO/security In charge i.e. FIR lodged or resolved at security in charge level.

4.1.9 Assessment of selected events was based on New Jersey Hospital Association security readiness assessment tool[46], summary of tool is enclosed as Appendix A. Tool was selected because it is healthcare based security assessment tool and it incorporates JCAHO security requirements. It was developed by team of experts incorporating best practices to improve hospital readiness in responding to security events. The tool incorporates three main components, which assess and score probability, risk and preparedness of security events in an organization. Assessment was done using study of incident reports, checklist, Onsite facility survey, security expert's inputs and informal discussions and interview. The result of these is then stored in the analysis chart as shown in Table 4.2 for the final evaluation as per guidelines of tool.

Table 4.2: New Jersey Hospital Association Security Readiness Assessment Analysis Chart

	PROBABILITY				**RISK**					**PREPAREDNESS**			**TOTAL**
	High	Med	Low	None	High risk , Possible Life threat	Significant Risk, Possible Life threat	Moderate risk, Minor Injury	Minimal risk, Minor injury	No risk, injury	Poor	Fair	Good	
SCORE	**3**	**2**	**1**	**0**	**4**	**3**	**2**	**1**	**0**	**3**	**2**	**1**	
EVENTS													
Conflicts/Workplace													
Fraud/Imposter													
Infant Abduction													
Strike													
Terrorism/ Bomb Threat/Hostage Situation													
Theft													
Sexual offence													
Fire													
Absconding													
Misbehavior													
Suicide/Attempted suicide/General													
Hazardous material Exposure/Leak													
Traffic management													
Animal Nuisance													

4.1.10 Probability of the above identified security events were scored on the 0-3 scale based on historical data of incidents within the institute, with larger score representing the highest probability and lower being the least.

(a) Incidents that never happened (0%)- Probability score = 0 (None)

(b) Incidents that occurred >0% but <33% - Probability score = 1 (Low)

(c) Incidents that occurred >33% but <66% - Probability score = 2 (Medium)

(d) Incidents that occurred >66% but < 100% - Probability score = 3 (High)

4.1.11 Risk of each event is rated on 0-4 scale based on impact the event may have on the services of a healthcare organization, people and assets associated with the organization. Larger scores are awarded to life threatening, highly disruptive events and lower for the least disruption as under as per Table 4.3.

Table 4.3: Risk Scoring criteria

RISK SCORE	CRITERIA
4	High risk with possible life threat
3	Significant risk with possible injury/life threat
2	Moderate risk of minor injury or inconvenience
1	Minimal risk of injury, or inconvenience to patient, staff, visitor
0	No risk of injury or inconvenience

(a) Five experts scored risk score. Expert responded included assistant engineer, supervisor and four external security experts of repute. Scoring was done by experts following security survey of CGH considering the potential death, threat to life and injuries from incident, potential property damage, business impact and loss of reputation and trust as mentioned in the tool. The final risk score was calculated as mean of scores given by above five experts.

4.1.12 Preparedness for each incident was scored on the 11-3 scale based on facility on site survey using a checklist (Appendix B). Larger score indicates poor preparedness and weak resources and lower score indicate good preparedness and strong resources.

(a) Checklist was based on JCAHO security standard requirements as suggested in tool and inputs from other facility security checklists. Checklist has 13 standards with each standard having multiple check points/ questions.

(b) Checklist was filled as per the physical survey of the facilities by the researcher along with the supervisor CGH. Each conformance/ Advantage/ positive was given the value "1" and each non-conformance/ disadvantage/ gap was rated as "0". Thus conformance scores for each standard were obtained.

(c) Preparedness for each event was calculated separately considering standards vital/ essential for preparedness for that particular event as advised by experts, e.g. infant abduction, score of standards like fire, parking was not considered however, score of security staff selection and training, General employee security awareness & training, Standardized security management plan, Access visitor and public, Staff identification and Lighting was considered.

(d) Score of each event was then expressed as a percentage of the best score possible for that particular event. (Conformance/Non conformances)(Appendix C)

(e) The net score obtained for each event was then broken onto a three-point scale, as follows to obtain final preparedness score for each event as per Table 4.4.

Table 4.4: Three point scale to obtain preparedness score

0% to 33% conformance	Score 3	Poor
33% to 66% conformance	Score 2	Fair
66% to 100% conformance	Score 1	Good

4.1.13 Total score for each event was calculated by adding probability risk and preparedness score of each event in individual column. As per tool lower the score better, meaning risk and probability of that particular security situation is low in institute and it is well prepared for the same. For scientific evaluation and logical assessment, the tool places situations that have received scores 4 or above to be top most priority list of healthcare administrators. Administrator will address all situations however he will place more emphasis on those events/situations scoring 6 or above after analysis.

4.1.14 The identified event scores were then placed in descending order of their total score, this helped to prioritize and recommend mitigation and preparedness.

OBSERVATION AND DISCUSSION

5.1 Introduction

5.1.1 Cantonment General Hospital is one of the premier health services institute. At CGH, there is a never-ending flow of employees, patients, visitors, salespeople and contractual staff. In the year 2014-15 OPD figures were 2,32,102 whereas in 2015-16 the OPD increased to 3,10,406. A large number of female employees need protection especially during night shift changes. Patients are particularly vulnerable at all times because of their limited Physical capabilities. What makes protection really difficult is that institute remains open twenty four seven for emergency services. As described in methodology the existing system of security at Cantonment General Hospital was reviewed and following observations were made.

5.2 Organization Of Security Services In Cantonment General Hospital

5.2.1 The Chief Medical Officer is overall responsible for adequate security for protection of staff, stores, equipment's and information in the Hospital. Organizational structure of Security of Cantonment General hospital is as shown in figure 5.1. Security of CGH can be divided into two parts.

(a) **External Security:** The responsibility of security of CGH is overall of the CEO. An Assistant Engineer of Cantonment board carries out the threat assessment and deploys the security personnel at various installations including CGH. This is the external security

(b) **Internal Security:** The internal security is out sourced from private security agency who are contracted on yearly basis. Each floor of CGH has dedicated Security personnel. In addition both the entry gates are also manned 24 x 7. There is a supervisor who is overall in charge of all these security personnel. At present the institute has contract with private agency M/S LC Security Services Pvt Ltd. A total of 30 security personnel are presently employed for security.

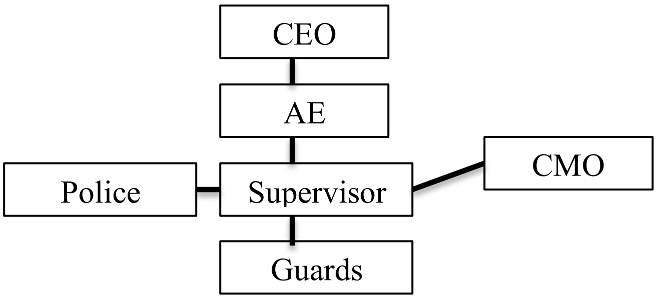

FIGURE 5.1 : Organizational structure of security at CGH

5.2.2 **Perimeter Fencing and Gates**

A 1.5 meters high wall surround the hospital. There are two main gates for entry and exit into and out of the hospital. Main access to the hospital is through gate number 1. All vehicle entry is also through gate number 1. Private security guards 24 X 7 man both the gates. The guards posted at these gates check the vehicles and stores for proper in/out gate pass.

5.2.3 **Security Lighting**

The institute is illuminated externally and internally for security reasons. Externally the luminaries are mounted on six meters high poles about 14-15 meters apart along the road. In addition, there are external lights fitted to the outer wall of the building in various locations. Internally the lighting of various areas is fitted to the roof of the building.

5.2.4 **Internal Security:** The various areas in the institute have different requirements based on their functional role. The patient care areas such as Casualty. Inpatient areas, outpatient area require 24 X 7 vigilance.

5.2.5 **Area of Responsibility**

(a) **Hospital:** The overall security of the hospital service areas is the responsibility of the Assistant engineer (cantonment board), Supervisor and 30 private security guards.

(b) **Fire Brigade:** Delhi Cantt Board maintains Fire Brigade, for the purpose of extinguishing fire and protecting lives and property in case of fire and for rescue purposes with any emergency like building collapse, road traffic accidents, human and animal rescue from a well etc. It is also an emergency support function during any disaster. The role of fire services also includes effective fire prevention, creating awareness on fire safety, and enforcing the inbuilt fire protection arrangement for various types of occupancies. This facility is available 24X7.

5.2.6 **Incident Reporting**

All security related incidents, which occur in the campus, inpatient or outpatient areas are reported by staff or security guard on duty to security supervisor, administrative office and security officer. Complete reporting channel is represented in Figure 5.2.

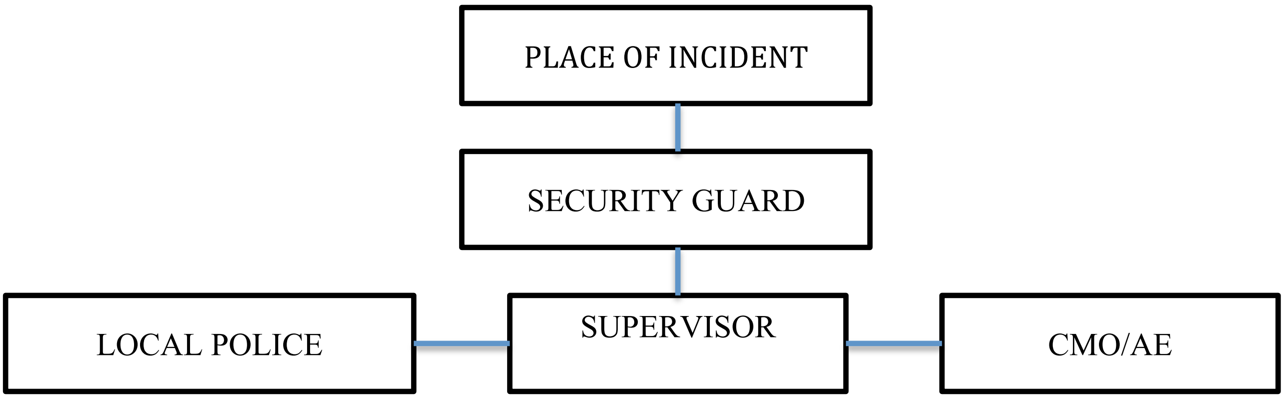

Figure 5.2: Incident Reporting System at CGH

5.3 **OBSERVATIONS**

5.3.1 As described in methodology security incident reports of the year 2015 and 2016 were studied and the data regarding the frequency of security related incidents was collected from the records of security officer, supervisor and Police Post Sadar Bazar. There were no security incidents found documented in records over the years 2015 and 2016. Frequency of each event is as shown in Table 5.1.

Table 5.1: Frequency of Security Incidents

S. NO.	EVENT	Frequency
	X = frequency of occurrence	
1.	Theft	0
2.	Terrorism/Bomb Threat/Hostage Situation	0
3.	Infant Abduction	0
4.	Strike	0
5.	Misbehavior	0
6.	Conflicts/Workplace Violence	0
7.	Fire	0
8.	Hazardous material Exposure/Leak	0
9.	Traffic management	0
10.	Sexual offence	0
11.	Absconding	0
12.	Animal Nuisance	0
13.	Suicide/Attempted suicide/General	0
14.	Fraud/Imposter	0
	TOTAL	0

5.3.2 **Observations**:

(a) It was observed that there were no security incidents reported during the period of study. Minor day to day incidents involving crowd control are effectively handled by the security staff present.

5.3.3 **Security incidents in 2015 and 2016** – Number of security incidents in 2015 and 2016 separately are as under in Table 5.2.

Table 5.2: Number of security incidents in 2015 and 2016

Year	2015	2016	% Inc
No	0	0	0

5.3.4 **Probability Assessment**

As described in methodology probability events were scored on the 0-3 scale based on historical data of incidents within the institute, with larger score representing the highest probability and the lower being the least. Probability scores & Summary of Probability scores are as shown in Table 5.3 and Table 5.4.

Table 5.3: Probability Scores

S no	Event	Frequency	Percentage	High Prob (3)	Med Prob (2)	Low Prob (1)
	X = frequency of occurence			100%>x >66%	66%>x >33%	33%>x >0%
1.	Theft	0	0%			1
2.	Terrorism/Bomb Threat/Hostage Situation	0	0%			1
3.	Infant Abduction	0	0%			1
4.	Strike	0	0%			1
5.	Misbehavior	0	0%			1
6.	Conflicts/Workplace Violence	0	0%			1
7.	Fire	0	0%			1
8.	Hazardous material Exposure/Leak	0	0%			1
9.	Traffic management	0	0%			1
10.	Sexual offence	0	0%			1
11.	Absconding	0	0%			1
12.	Animal Nuisance	0	0%			1
13.	Suicide/Attempted suicide/General	0	0%			1
14.	Fraud/Imposter	0	0%			1
	Total	0				

Table 5.4: Probability Scores Summary

EVENT	PROBABILITY SCORE
Theft	0
Terrorism, Workplace Violence/Conflicts, Misbehavior, Fire, traffic Management, Animal Nuisance and Sexual offence	0
Infant abduction, Strike and Hazardous material	0

5.3.5 **Observations:** All Events although scored zero as there was nil frequency in 2015 and 2016 the implication not being that they can never happen in future but that the probabilities of these situations materializing is extremely low.

5.3.6 Risk Assessment

As described in the methodology risk of each event is scored on 0-4 scale. Risk scoring was done by five experts. The final score for each event was obtained by rounding off the mean to the nearest whole number as shown in Table 5.5. The risk score summary is given in Table 5.6.

Table 5.5: Risk Scores

S no	Event	Expert1	Expert2	Expert3	Expert4	Expert5	Mean	Final Score
1.	Theft	4	2	2	2	2	2.4	2
2.	Terrorism/Bomb Threat/Hostage Situation	3	4	4	3	4	3.6	4
3.	Infant Abduction	2	3	2	3	2	2.4	2
4.	Strike	2	3	3	2	4	2.8	3
5.	Misbehavior	4	3	4	4	2	3.4	3
6.	Conflicts/Workplace Violence	4	3	4	4	2	3.4	3
7.	Fire	3	4	3	4	4	3.6	4
8.	Hazardous material Exposure/Leak	1	2	3	3	2	2.2	2
9.	Traffic management	4	1	2	2	1	2.0	2
10.	Sexual offence	3	3	3	3	2	2.8	3
11.	Absconding	1	2	2	1	2	1.6	2
12.	Animal Nuisance	2	3	2	1	2	2.0	2
13.	Suicide/Attempted suicide/General	2	1	1	2	2	1.6	2
14	Fraud/Imposter	2	1	1	2	2	1.6	2

Table 5.6: Risk Scores Summary

EVENT	RISK SCORE
Terrorism and Fire	4
Strike, Conflict, Misbehavior and Sexual offence	3
Infant abduction, Theft, Fraud, Animal Nuisance, Suicide, Hazardous material and Traffic management	2

5.3.7 **Observations**

(a) Terrorism and fire were found to have highest risk with risk score of 4 implying that these events are highly disruptive and have life threatening and disabling consequences.

(b) Strike, conflict, misbehavior, sexual offence are rated as high risk events with score of 3 meaning they carry significant risk and possible life threat. This situation could affect business, interruption or disruption of services, loss of reputation and trust, financial impact, disruption of work, equipment or facility damage and delay of critical supplies.

(c) The low risk score of 0, 1 was not attributed to any of the events implying that all selected events carry substantial risk and can interfere with smooth functioning of healthcare operation.

5.3.8 **PREPAREDNESS ASSESSMENT**

Standard specific preparedness: Conformance to preparedness standards is as shown in Table 5.7.

Table 5.7: Standard Specific Preparedness

S. No	Standard	Conformance score	Percentage
1.	Security staff selection and training	10/14	71.43%
2.	Standardized security management plan	17/25	68%
3.	General employee security training	9/13	69.23%
4.	Staff identification	14/15	93.33%
5.	Access visitor and public	26/40	65%
6.	Technology application	10/17	58.82%
7.	Parking and transportation	8/9	88.89%
8.	Misc administrative safeguards	51/81	62.96%
9.	Perimeter security	23/38	82.14%
10.	Lighting	14/21	66.67%
11.	Lock and Key	13/27	48.15%
12.	Emergency plan	½	50%
13.	Fire safety	18/41	43.90%
		214/343	62.39%

5.3.9 **Observations:**

(a) Preparedness for fire and lock and key standards is weak. Therefore overall security posture may be improved by focusing on process change and resource allocation towards them.

(b) The overall preparedness comes out to be 62.39%, suggesting a 37.61% scope fro improvement, which may be addressed by recommendations given at the end of the study.

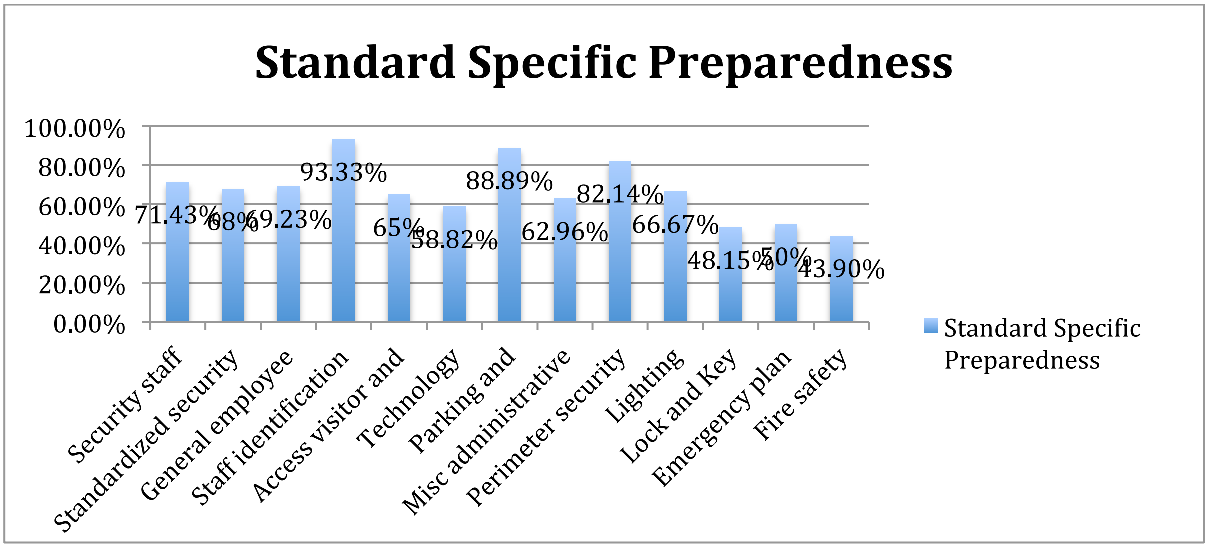

Figure 5.3: Graph Standard specific preparedness

5.3.10 **Preparedness Event Specific:** Preparedness for event considering standards vital/essential for preparedness for a particular event is as shown in Table 5.8.

Table 5.8: Event specific preparedness score

S no	Event	Score obtained	Total Con + Non Con	Percentage	Preparedness score
1.	Theft	96	151	63.57%	2
2.	Terrorism/Bomb Threat/Hostage Situation	47	71	66.19%	2
3.	Infant Abduction	94	128	73.43%	1
4.	Strike	78	120	65%	2
5.	Misbehavior	36	52	69.23%	1
6.	Conflicts/Workplace Violence	113	163	69.23%	1
7.	Fire	31	58	53.44%	2
8.	Hazardous material Exposure/Leak	47	61	77.04%	1
9.	Traffic management	65	86	75.58%	1
10.	Sexual offence	76	113	67.25%	1
11.	Absconding	95	128	74.21%	1

12.	Animal Nuisance	86	130	68.15%	1
13.	Suicide/Attempted suicide/General	67	94	71.27%	1
14.	Fraud/Imposter	35	52	67.30%	1

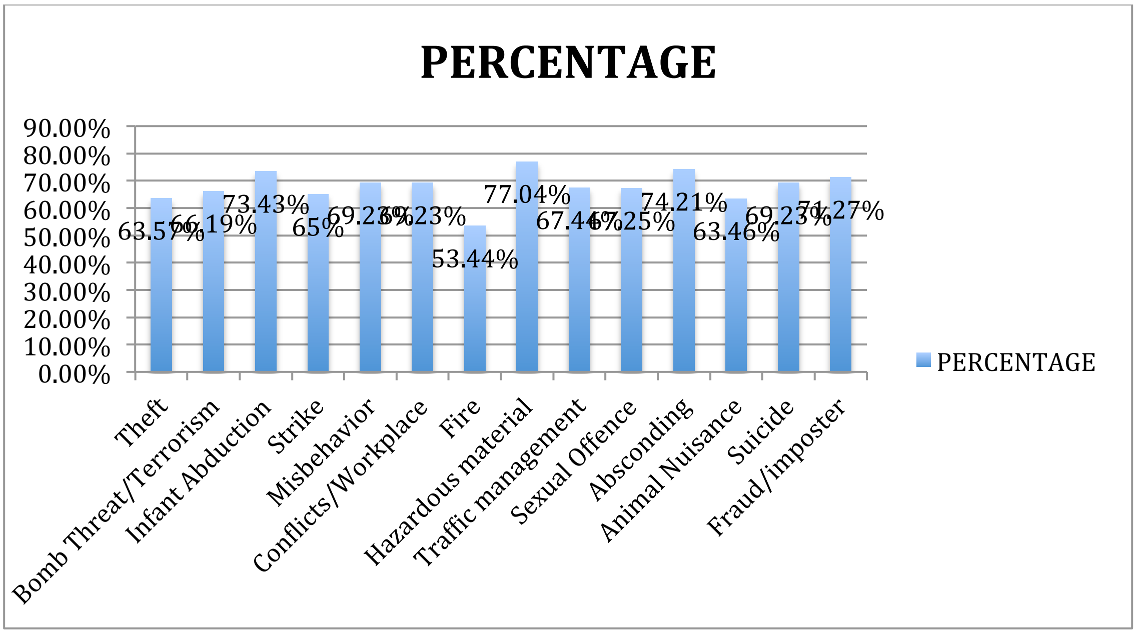

Figure 5.4: Graph Event Specific Preparedness

5.3.11 **Observations:**

(a) It is observed that fire, theft, terrorism and strike are among lowest in terms of preparedness; therefore these are thrust areas, which need to be strengthened for security preparedness as shown in table 5.9.

Table 5.9: Thrust Areas for Improvement in Security Preparedness

Fire	Preparedness 53.44%
Theft	Preparedness 63.57%
Terrorism	Preparedness 66.19%
Strike	Preparedness 65%

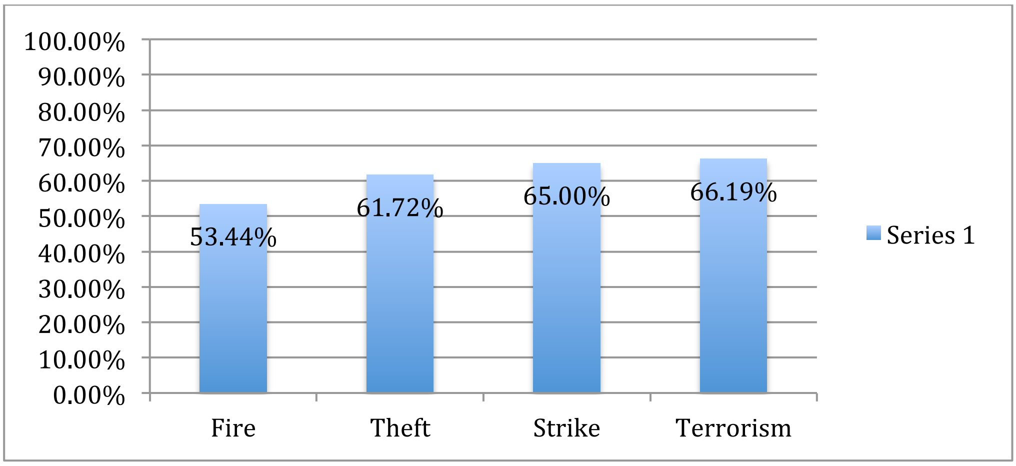

Figure 5.5: Graph Thrust Areas for improvement

5.3.12 **TOTAL SCORE**

Total scores for each event as scored by adding scores of probability, risk and preparedness are as under. Summary of the scores is as shown in Table 5.10 and total score is as shown in Table 5.11.

Table 5.10: Summary Total Scores

Event	PROBABILITY	RISK	PREPAREDNESS	Total
Theft	0	2	2	4
Terrorism/Bomb Threat/Hostage Situation	0	4	2	6
Infant Abduction	0	2	1	3
Strike	0	3	2	5
Misbehavior	0	3	1	4
Conflicts/Workplace Violence	0	3	1	4
Fire	0	4	2	6
Hazardous material Exposure /Leak	0	2	1	3
Traffic management	0	2	1	3
Sexual offence	0	3	1	4
Absconding	0	2	1	3
Animal Nuisance	0	2	1	3
Suicide/Attempted suicide/General	0	2	1	3
Fraud/Imposter	0	2	1	3

Table 5.11: Total Scores

EVENTS	**PROBABILITY**				**RISK**					**PREPAREDNESS**			**TOTAL**
	High	Med	Low	None	High risk, Possible Life threat	Significant Risk, Possible Life threat	Moderate risk, Minor Injury	Minimal risk, Minor injury	No risk,injury	Poor	Fair	Good	
SCORE	**3**	**2**	**1**	**0**	**4**	**3**	**2**	**1**	**0**	**3**	**2**	**1**	
Theft				0			2				2		4
Terrorism/ Bomb Threat/Ho				0	4						2		6
Infant				0			2					1	3
Strike				0		3					2		5
Misbehavior				0		3						1	4
Conflicts/ Workplace Violence				0		3						1	4
Fire				0	4						2		6
Hazardous material Exposure/ Leak				0			2					1	3
Traffic				0			2				2		4
Sexual offence				0		3						1	4
Absconding				0			2					1	3
Animal Nuisance				0			2					1	3
Suicide/Attempted suicide/General				0			2					1	3

5.3.13 **Observations:**

(a) It is observed that terrorism and fire scored highest total scores of 6. As per guidelines of tool, lower the score the better, signifying that risk and probability of that particular security situation is low in the institute and it is well prepared for the same. Therefore high score of 6 for these events signifies an urgent need for attention. The administration needs to place greater emphasis on these situations scoring 6 or above.

(b) Strike (Score 5) should be next in priority in terms of resource allocation and process change after terrorism and fire.

(c) Theft, workplace violence/conflicts, misbehavior, traffic management and sexual offence (Score 4) should be next in priority in terms of resource allocation and process change after terrorism, fire and Strike.

(c) Animal nuisance, infant abduction, hazardous material, suicide and fraud (score < 4) show satisfactory security response.

5.3.14 **Final Evaluation:** Studied events listed in decreasing order of their total scores are as shown in Table 5.12.

Table 5.12: Events in descending order of total scores

Event	Total score	Priority for mitigation, preparedness, resource allocation and process change
Terrorism, Fire, Strike, Theft, workplace violence/ conflicts, misbehavior, traffic management and sexual offence	> 4	Priority I
Animal nuisance, infant abduction, hazardous material, suicide and fraud	< 4	Priority II

5.3.15 **Observation:**

(a) The study involved 14 events for assessment of threat, vulnerability and risk at Cantonment General Hospital. These events were terrorism, strike, workplace violence, misbehavior, conflicts, traffic management, sexual offence, animal nuisance, Infant abduction, hazardous material, suicide, fire and fraud.

(b) The study revealed that Terrorism, Fire, Strike, Theft, workplace violence/ conflicts, misbehavior, traffic management and sexual offence are the security risk requiring immediate attention and priority in terms of planning, policy, decision making, resource allocation and process change at CGH.

(c) Remaining events i.e. Animal nuisance, infant abduction, hazardous material, suicide and fraud require attention on subsequent priority. Institute must address all risk to improve its security posture however should place more emphasis towards preparedness of terrorism, fire and strike.

5.4 **Findings**

(a) No security incidents were found documented as per the records over the years 2015 and 2016.

(b) Probability of all events are therefore low (Probability score zero).

(c) Terrorism and fire have highest risk (Risk score 4). Implying that these events are highly disruptive and have life threatening and disabling consequences.

(d) The low risk score of 0, 1 was not attributed to any of the events implying that all selected events carry at least moderate risk.

(e) Preparedness for fire and lock & key is lowest among standard specific preparedness.

(f) The overall preparedness is 62.39%, suggesting a 37.61% scope for improvement.

(g) Preparedness for fire, theft, terrorism and strike is lowest among event specific preparedness.

(h) Terrorism and fire (Total score 6), need urgent attention towards them on immediate priority.

(i) Strike (Total score 5) is next in priority in terms of resource allocation and process change after terrorism and fire.

(j) Theft, workplace violence/conflicts, misbehavior, traffic management and sexual offence (Score 4) should be next in priority in terms of resource allocation and process change after terrorism, fire and Strike

(k) Terrorism, Fire, Strike, Theft, workplace violence/ conflicts, misbehavior, traffic management and sexual offence (Total score ≥ 4) are the security risk requiring immediate attention and priority in terms of planning, policy, decision making, resource allocation and process change.

5.5 **Recommendations**

This study of "Hospital Security and Associated Risk, Threat and Vulnerability Assessment at Cantonment General Hospital" revealed that terrorism, and fire are the security risk requiring immediate attention and priority in terms of planning, policy, decision-making, resource allocation and process change. CGH has a well-organized security system in place; however preparedness level can be further improved. The following recommendations are offered for these critical events:

(a) **Terrorism/Bomb Threat**: Hospitals, just like other public places, are vulnerable to terrorist acts. CGH being an important hospital located in cantonment makes it a soft target vulnerable to terrorist attack. Capacity to safely neutralize bomb/terrorist threat is one of the most critical factors towards security efficiency of the institute.

(i) At CGH, bomb threat cannot be adequately identified and diffused due to lack of awareness and training among the security staff. CGH should have a documented bomb threat plan clearly earmarking responsibilities for prevention, carrying out search operations, evacuation and termination of the threat. Staff must be made security conscious and trained to approach a bomb threat in a systematic fashion.

(ii) CGH has selective installation of CCTV; however their numbers do not commensurate with the size and logistics of CGH. Adequate deployment of technology in the form of X ray scanners, digital video recorders, door frame metal detectors and hand held metal detectors at all entry points needs to be done on priority basis.

(iii) At present CGH has no written security management plan. Institute does not conduct annual security assessments to identify its security vulnerabilities. Annual risk Assessment must be conducted and institute must use the expertise of agencies such as Delhi Police, CISF and NSG to formulate own security systems and processes.

(b) **Theft:** CGH is loaded with consumable goods one could use around the home. Those goods include toner and paper for home computer, food products, medications, medical equipment, linen etc. Access to institute is quite porous. Following steps are recommended to deter thefts:

(i) Access control policy with strict ID control and use of biometrics/palm/thumb scans which restrict unauthorized access. The institute must ensure a list of contractual staff working in facility and keep it updated at all times.

(ii) Installation of closed circuit TV system at the facility and use of a central monitoring station on 24 x 7 basis. The institute must maintain restricted access at odd hours, ensure a manned perimeter barrier and fencing which is under surveillance at all times.

(iii) Central key register with strict lock and key control for ensuring safety of property and provision of adequate number of lockers for staff and patients.

(c) **Fire:** Although no fire incident have taken place, all fire fighting equipment are not inspected regularly, fire hose valves at many hose stations are not tested and water pressure in the riser on all floors needs to be sufficient to handle both sprinkler and hoses. Disaster/emergency plan of institute has not been practiced for long.

(i) It is recommended that institute must adhere to the fire safety rules and conduct annual fire audits. Institute must ensure training of staff to rescue and evacuate. Regular fire mock drills should be conducted and serviceability of equipment should be ensured.

5.6 **Conclusion**

5.6.1 Healthcare Security is a unique challenge. In hospital there are so many people milling around patients, staff, vendors, physicians and visitors. It is extremely difficult to maintain easy access at the same time attempting to impose sensible level of security.

5.6.2 Hospitals house inventory of consumable items like food, medical supplies, linen and drugs. Thousands of meals and prescriptions are served every day. Drugs are susceptible to internal pilferage and theft.

5.6.3 This all adds up to a need for different approaches to security. Hospital managers base their security decisions on keeping legal aspects, costs and reputation of the facility. But critical assets of a hospital its people, property, information and reputation must be protected with good security.

5.6.4 Security is everyone's business and not that of administration alone. Effective security programs must include the proper mixture of employee participation, the judicious use of physical security equipment and technology and security personnel.

Security is a situational discipline. One size does not fit all. Security programs must be customized to the individualized needs of each hospital and no two-security programs are, or should be, the same. Unlike other programs, security programs do not lend themselves to universal solutions.

5.6.5 Cantonment General Hospital is an important Hospital situated in the cantonment and has its own risks, threats and vulnerabilities. Hospital must "anticipate and prevent". There are no quick fixes. It is apparent from the study that security risk requiring utmost priority, prompt attention and resource allocation are terrorism, fire and theft.

REFERENCES

1. Https:// en.wikipedia.org/wiki/delhi_cantonment.

2. www.censusindia.gov.in

3. https://en.wikipedia.org/wiki/lieracy_in_india.

4. www.cbdelhi.in

5. Karim H Vellani, Strategic healthcare security: Risk assessment in environment of care.

6. Robert E. Owles, Jr and Karim H Vellani, CPP,CSC, Vulnerability and Risk Assessment in Environment of care.

7. Vellani, Karim H(2006).Strategic Security management:A Risk Assessment Guide for decision makers. Woburn; Butterworth - heimann.

8. Sennewald, Charles A. (2003). Effective Security Management. 4th Edition. Woburn; Butterworth - heinemann.

9. Risk Mangement in NHS. NHS management Executive. Department of health (England) 1993.

10. Colling RL, Hospital Security, Stoneham, MA; Butterworth – heimann; 4th edn, 1992.

11. Kunders GD, Gopinath S, KatakamA. Hospitals: Planning, Design and Management New Delhi Tata McGraw – Hill Publishing Company; 1998

12. Sarnese PM. A Tale of Two Hospitals Security management. March 1996;35

13. Olive E, Wilson J. Security Manual. Alder shot. Hampshire : Gower Publishing Company Limited; 1998.

14. Crime in Services industries. Washington DC. Department of Commerce (US); 1977:66

15. Themmapa Diwakar, Study of hospital security, AIIMS, 2008.

16. Toffer A . The third wave. New York; Morrow, 1980.

17. Report of committee on hospitals New Delhi: Ministry of Health & Family welfare, Government of India; 1968.

18. Report of High Power Committee on Nursing and Nursing Profession. New Delhi. Ministry of Health & Family welfare, Government of India; 1976.

19. Roper CA. Physical Security and The inspection process. Stoneham, MA; Butterworth – Heinemann; 1997

20. Annual meeting held in New York. (1968, September). International Association for hospital security newsletter, 1(1).

21. Kennedy, D. B. (1989). Case your space. Security Management. 47(April).

22. Parker J. Sourcing Security. Hospital development; July/august 1995: 26-27.

23. Weonik, R. (2008, January 21). Securing our hospitals; GE security and IAHSS healthcare benchmarking study.

24. Wyclie JG. In: Fennelly LJ, editor. Effective Physical Security. Stoneham, MA; Butterworth; 1992.

25. Srinivasant, Chunawala SA. Management Principles and Practice. Bombay; Himalaya Publishing House; 1983.

26. Dr S K Gupta. Hospital Staffing Norms, Journal of Academy of Hospital Administration, Vol I, Jan 1989, P-33-35

27. Benjamin RC, Kemppainen RC. Hospital Administrator's Desk Book. Englewood Cliffs NJ; Prentic – e Hall Inc; 1983.

28. Potter, A. N. (2006). Considerations when arming hospital security officers. Retrieved march 31, 2017, from http://www.iahss.org/ref- materials/Potter - Paper/contents.htm. Pg 8.

29. Thompson, B. 92005, March 3). Hospital security and personnel safety concerns. Presented at Henry Ford Medical Center.

30. Crowe, T. D. (2000). Crime prevention through environmental design.

Woburn, MA; Butterworth- Heinemann National Crime Prevention Institute, P. 36.

31. April 30, Kent Hospital. (2006, October 23). Kent adds new security bicycle patrol. Retrieved from http://www .Kenthospital. org/ body.cfm? d=84 &action =detail&ref=81.

32. Bates, N.D. (1995). The power of paperwork. Security management.

33. Latts, W. E. (1998). Psychiatric patients: Promises liability and predicting patient elopement. Journal of Healthcare Protection Management. 14(2), 75.

34. Acess + Control + Security = Constructive Security (editorial). Security Controls march 97; 22-27.

35. Cotag International Protecting Patients. Htpp;// www. Cotag.com. retrieved Feb 2017.

36. Sunter Katy. GCTV; From Patient Treatment to Patient Protection Health Estate Journal Februrary1996; 6-7.

37. Dev H. Integration of Technology in Security Management. Proceedings of the 1st National Seminar Cum – Training Programme on Security, Fire safety and Crisis Management in Hospitals/Healthcare institutions; 1996.

38. Scaglione, B. (2007). Digital security technology simplified. Journal for healthcare Protection Management, 23(20).

39. Jimenez, A. (November/December 2006). Metal detection worth its mettle. Campus Safety Magazine.

40. Colombo, A. (2006 May/June). Call box basics and beyond. Campus Safety Magazine. Retrieved April 22. 2010 from http:// www.campussafetymagzine.com/ articles /articleID.

41. The USDA Handbook on Workplace Violence Prevention and Response. (1998, December). The U. S. Department of Agriculture. Retrieved Apr 19, 2017 from http:// www.usda.gov/news/pubs/violence/wpv.htm.

42. Retrieved Mar 17, 2017 from http://newsvote.bbc.co.uk/mpapps /pagetools /print/news.bbc. Marston, C. (2008, April 13). Violence part of life for NHS staff. BBC News.co.uk/1/hi/health/7337389.stm.

43. Mulholland, A. Nurses say they are fed up with workplace violence. CTV.ca News. From http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20090416.

44. Ironside, R. (2008, Decembeer 22). Fed-up Queensland nurses turning to prostitution. The Courier-mail from http://www. News.com.au /story/ 0,27574, 24831036 -1248,00.html

45. Security Assessments for Healthcare Facilities http://www.security source on line.com/50/security-assessments-for-healthcare-facilities.

46. NJHA Security readiness assessment tool. Sighted Feb 2017. Available from www.gnyha.org/321/file.aspx.

Appendix A

New Jersey Hospital Association Security Readiness Assessment Tool

Procedure: Fill out all the columns on analysis chart.

Type of security Incident/event

1. In the first column, list all the security incidents/situations that could affect hospital. Historical data is indicative. These events selected can be those that either had a high incidence in the past or they have the potential to occur in the current environment.

Probability

2. Rate the likely hood of each incident occurrence on the scale of 0 – 3 with the larger number being the highest probability and lower being least. This is a subjective determination. Historical data, incident report study, frequency will be indicative.

Assess Risk and Loss by Considering

3. Risk of each event is rated on 0 – 4 scale based on impact that event may have on the services of a healthcare organization, people and assets associated with the organization. Larger risk score may be awarded to life threating, highly disruptive events and lower for the least disruption as under. Score risk considering the following.

(a) **Human Impact**. Assess the potential deaths, likelihood of threat to life and injuries from the incident, using the same scale.

(b) **Property Impact**. Consider potential property damage from the incident, including costs of repairs, using scale.

(c) **Business Impact**. Analyse how the situation could affect business, interruption or disruption of services, loss of reputation and trust, financial impact, employees being unable to work, equipment or facility damage, patients being unable to come to the facility, any delay of critical supplies.

Preparedness

4. Examine internal and external resources and their ability to respond to the security need, score preparedness based on facility on site survey using the scale 1 – 3 with the larger number indicating poor preparedness and weak resources and lower scale indicating good preparedness and strong resources. Preparedness includes the training of hospital staff and existing resources, drill outcomes, policy and procedures.

Total

5. When the form is completed, total score for each situation can be calculated by adding probability, risk and preparedness score of each in individual columns. The lower the score, the better i.e. risk and probability of that particular security situation is low and preparedness is good.

6. The comparisons among different incident scenarios should be used to determine planning and resource priorities.

Identified Vulnerabilities

7. The identified events can then be placed in descending order of their total score, which will help to prioritize during review and planning of hospital security. Recommendations for mitigation and preparedness activities are made to relevant departments. The focus of planning should be on situation of higher priority or score. Administrator will address all situations however will place more emphasis on those scoring six or above after analysis.

Risk Assessment

8. The risk assessment is used to evaluate the impact of the environment of care ability of the organization to perform clinical and business activities. The impact may include disruption of normal functions or injury to patients, visitors and staff.

Procedure

(a) The evaluator completes the form by identifying the risk related to the environment and the activities conducted in the area. Each risk is scored using the 0 – 4 rating scale included in the form.

(b) To determine the appropriate score for each identified risk, the reviewer will consider information obtained through a physical tour of the facility, review of annual incident statistics, review of the past minutes, checklist, questionnaire.

Risk Scoring Key

SCORING	CRITERIA
4	High risk area with possible life threatening or disabling consequences, as well some history of associated incidents with serious injury
3	High or Significant risk area with possible life threatening or disabling consequences and no history of associated incidents with serious injury
2	Moderate risk of minor injury or inconvenience to patient, staff, visitor
1	Minimal risk of minor injury, or inconvenience to patient, staff, visitor
0	Virtually no risk of injury or inconvenience to anyone

Appendix B

PREPAREDNESS CHECKLISTS

S. No	STANDARD	Yes/No	Score Conformance = 1 Non Conformance =0
I. Security Staff Selection and Training			
1.	Is guard service employed		
2.	Have written instruction been issued to guards as to their duties and assignments		
3.	24 x 7 guards secure the facility		
4.	Are duty register/ duty card used		
5.	Are duty cards reviewed daily		
6.	Are activity reports maintained by guard for each shift		
7.	Absent reports initiated		
8.	Do guards have keys of gate/ building		
9.	Are guards armed		
10.	Communication system is used by all guards		
11.	Are guards trained in CPR and passed physical fitness test		
12.	Do guards know how to use latest security devices, CCTV etc		
13.	If security is provided by a contract service, have the following issues been addressed? Pre – employment screening including criminal background check		
14.	Have appropriate staffing levels been determined		
II. Standardized Security Management Plan			
1.	Are there written security policy and procedures		
2.	Is there procedure for search screen operation fro entry to facility		
3.	Is there policy for firearm to be carried into the facility by law enforcement officer		
4.	Are security officer armed in facility		
5	Are security personnel Equipped		
6.	Are procedure for emergency evacuation exist in facility		
7.	Do you have standardized security policies and procedures		
8.	Has your facility reviewed and determined compliance with security standards		
9.	Do you conduct an assessment of your security vulnerabilities on annual basis		
10.	Have you developed a security management plan		
11.	Have you obtained a copy of your country's Emergency & Disaster management plan from the		

	country office of disaster management		
12.	Do you have procedures for infant security		
13.	Do you have policy on controlled and dangerous drugs		
14.	Do you have polices to manage court ordered document		
15.	Have you developed standard forms and checklist of steps to ensure all necessary steps are taken foe hospital security		
16.	Are all openings in perimeter wall properly secured and guarded		
17.	Are public areas sufficiently lighted to discourage attempts against person/vehicle		
18.	Is guard free from extra duties so that they are free to perform their protective duties		
19.	Do guards know how to use security devices, CCTV etc		
20.	Does building have fire safety policy		
21.	Is communication system adequate		
22.	Does cashier window have security features		
23.	Do you have protocols for VIP Admission		
24.	Do you have protocol for media management		
25.	Do you get adequate funds for security department		
III. Gen Employee Security Awareness & Training			
1.	Have you developed a process to ensure all new general staff and volunteers receive training by security staff so that they are on the alert for suspicious behavior & are aware of the policies and procedures that must be implemented fro specific security incidents		
2.	Do you ensure that each dept conducts ongoing awareness training for their staff to update them on the threat levels and terror alert advisories issued by security		
3.	Have you developed a standardized plan for all employees to respond to bomb threat		
4.	Do you hold managers responsible for documenting that staff are trained and are following the facilities security policies and procedures		
5.	Have you developed education and training programs for security staff		
6.	Does training for security staff include a counter terrorism program that encompasses the following issues, threat assessment, national threat levels and weapons of mass destruction awareness training		
7.	Do you have policies governing how security personnel deal with following issues, Weapons,		

	Physical force, searching of patients, staff visitors		
8.	Do you have policies governing how security personnel deal with patients, staff visitors		
9.	Does training include instruction on accommodating law enforcement personnel who are in the premises guarding prisoners or protecting crime scene		
10.	Do you have policies that lay out general orders for security personnel and define their authority		
11.	Do you have a policy regarding fire watch		
12.	Do you have hospital security vehicles		
13.	Do you conduct security personnel scenario based assessment		
IV Staff Identification			
1.	Do you have ability to identify which persons have the authority to be on the premises, either as physicians and staff or as a visitor, vendor, volunteer or business associate		
2.	Do you have an identification card policy that has been approved by the committee and CEO		
3.	Are any guidelines designed to assist in developing standardized policies and procedures regarding access by staff		
4.	Do you have a policy addressing the issuance and reissuance of ID cards for all levels and categories of staff and volunteers		
5.	Do you require staff, including physicians to wear ID at all times while on facility property and to show ID upon entering the facility		
6.	Do identification cards for staff, volunteers and physicians include a photo, the wearer's name, title or credentials and department		
7.	Do ID cards allowing access to sensitive areas have distinguishing features such as color coded background		
8.	Do you have a policy to address consequences for failure to carry/ show ID		
9.	Does your policy hold managers accountable for lack of compliance of their employees and ensuring the imposing of penalties		
10.	Do you have a policy addressed the issuance and termination of identification cards that addresses the following, handling and storage of blank and terminated cards		
11.	Do you limit areas to which certain employees have access		
12.	Do you have policies regarding access to sensitive areas		
13.	Do you give warning for inappropriate access or trespass		

14.	Do you have policy regarding searches of employee packages or lockers		
15.	Do access cards when used have expiry date		
V. Access Visitor and Public			
1.	Are public waiting area routinely searched		
2.	Are rest room routinely searched		
3.	Is any pass system used for waiting areas		
4.	Are direction and floor plan clearly posted in public areas		
5.	Is identification system card or badge used to identify all personnel within facility		
6.	Are there written procedures for the method of identification at the time of entering and leaving controlled areas		
7.	Are all personnel required to wear the security identification badge while on duty		
8.	Do guards at control point compare badges to bearer both at entry and exit		
9.	Are procedures for lost damaged forgotten and posted out badges		
10.	Are badges recorded and controlled by rigid accountability procedures		
11.	Are lost badges replaced by one bearing a different number or one that is otherwise not identical to the one lost		
12.	Are infrequent visitors issued visitor pass		
13.	Are regular visitor provided with special identification		
14.	Are frequent test conducted to determine the adequacy and promptness of response to alarm signal		
15.	Is employee ingress/egress restricted to certain controlled areas		
16.	All access controlled by access device		
17.	Do employees have ID cards		
18.	Do ID badges have picture of employees		
19.	Is ingress/egress control points used fro employee are same as used by visitor, vendor, repairman		
20.	Are ID badges color coded		
21.	Are there guards placed on every entrance		
22.	Are there procedure for returning and accounting temporary passes		
23.	Are there passes for visitors		
24.	Does the pass allow different level of access		
25.	Do you restrict access to sensitive areas and assign access only through special ID		
26.	Do you have policy regarding the handling of individual that are in areas for which they are not authorized		
27.	Do you post sign at entrance to restricted areas		

28.	Do you post sign at emergency department for no entry		
29.	Do you post signs at points of access to instruct certain individual to coordinate their visit with specific department		
30.	Do you evaluate whether to limit use of conference facilities by outside organisations		
31.	Do you have access control policy that has been approved by administration		
32.	Do you limit the number of entry and exit points		
33.	Do you have procedures for addressing searches of suspicious packages and persons		
34.	Do you have a procedure for ensuring the integrity of an electronic access control system access card reader and CCTV in event of power failure		
35.	Do you control access from ambulatory care areas to other areas of hospital		
36.	Have you established a process to rapidly shut down access to the entire facility or specific areas		
37.	Do your emergency management plan and security policies and procedures address building access by media		
38.	Do you policies regarding identification of visitors that addresses consequences for violating access restriction		
39.	Do you require all visitors to sign in and obtain pass		
40.	Do you require outpatient to obtain a pass that is distinct from those fro visitors		
VI. Technology Application			
1.	Is communication system adequate		
2.	Is there more than one communication system used exclusively by security personnel		
3.	Radio frequency in coordination with local facility security/ city police		
4.	Does all telephone go through building switchboard		
5.	Does exchange have any security safeguards		
6.	Can communication be done with outside security agency, if yes which		
7.	Is there CCTV installed in facility		
8.	Do you have policy for use and testing of CCTV, alarm system		
9.	Do you have a video surveillance camera		
10.	Do you a system/machine that produces a visitor/ vendor pass on the spot		
11.	Do you have access control system with locks or cards with computer that produces an audit/record		
12.	Do you have metal detector and policy regarding the same		

13.	Do you have policies regarding key control		
14.	Do you have biometrics/ palm/thumb scans that permit access by authorized person		
15.	Do you biometric check credentials, patient details for relatives in rest room		
16.	Do you limit the number of visitors to patients in emergency and wards		
17.	Do you have central monitoring station		
VII Parking and Transportation			
1.	Is entry and exit from parking area controlled by guard/chain		
2.	Are parking area watched by CCTV		
3.	Are reserved parking facility marked		
4.	Are proper sign posted for parking		
5.	Are parking reserved for staff/VIP		
6.	Have you reviewed transportation routes and parking areas around the hospital to determine whether the routes allow contact with sensitive areas?		
7.	Have you coordinated with local law enforcing authorities to gain understanding of which transportation routes would be used/ blocked during VIP admission		
8.	Do you policy for picking up vehicle from no parking zones		
9.	Do you have policy for transporting staff during emergency		
VIII Miscellaneous Administrative Safeguards			
1.	Some control is used over the use of elevator		
2.	Women guards for female wards		
3.	CCTV camera at all entry/ exit/ parking/ inside hospital including wards with recording and 24 x 7 manning of monitoring room		
4.	HHMD with trained manpower at all entry/exit for screening		
5.	X ray baggage scanner for screening of hand baggage		
6.	Bulk good X ray scanner for screening of bulk items in stores		
7.	Sufficient parking space		
8.	Anti sabotage check of vehicles with inverted mirror by trained guard		
9.	Visual anti sabotage check of premises by trained security guard at least twice		
10.	Centralized alarm system		
11.	Contingency drill for evacuation		
12.	Regular patrolling of hospital		
13.	Visitor management practices		
14.	Security force staffing & utilization		

15.	Security force training		
16.	Signage		
17.	Special measures hazardous material security		
18.	Infant abduction protection system		
19.	Supervision of security staff		
20.	Duty hours/ shifts of security staff		
21.	Uniform of security staff		
22.	Patient records and office information security		
23.	Special measures for computer security		
24.	Traffic control equipment		
25.	Emergency lighting/ backup generators		
26.	Metal/ Explosive/radiation detection		
27.	Contact details/ liaison with local law enforcing		
28.	Assistance to employee and visitor problem		
29.	Maintaining security incident report book		
30.	Panic alarm in emergency		
31.	Staffing of security staff		
32.	Written info to patients regarding safeguarding their valuables		
33.	Sealing locking of stores		
34.	Sealing locking of Pharmacy		
35.	Warning notice in no parking		
36.	Entrances left open to public after hour		
37.	Color coded card for visitor		
38.	Posted speed limits		
39.	Handicapped parking areas		
40.	No parking signage		
41.	Separate entrance and loading area for emergency		
42.	Policy to carry firearm		
43.	Training of security staff to restrain violent individual		
44.	Center dedicated for PR officer		
45.	CPTED		
46.	Written security plan		
47.	Annual risk assessment		
48.	Capability to lock down or limit access		
49.	Facility include security test as part of drills and exercises		
50.	Facility has infant abduction prevention plan		
51.	Facility has capability to monitor movement of persons inside facility		
52.	Arrangements for securing personal property of staff		
53.	Arrangements for securing personal property of patients		
54.	Maintenance of key register		
55.	Maintenance of stamp register		
56.	First in/last out is there a person designated to open up the area		
57.	Are all staff wearing name badges		
58.	What measures exist to safeguard equipment		

59.	Where the equipment inventory is kept and who maintains it		
60.	Measures to ensure record keeping		
61.	Uncontrolled access point into and out of facility		
62.	Employee security awareness		
63.	VIP protocols		
64.	Protocol of hoax/ threat call		
65.	Media management		
66.	Violence in workplace protocol		
67.	Special training for crowd management		
68.	Police control room		
69.	Do you have security officer with assigned responsibility		
70.	Have you conducted security awareness and training program		
71.	Have you developed security incident response and responding procedures		
72.	Do you conduct info system activity review		
73.	Have you conducted vulnerability and risk analysis		
74.	Have you developed media management		
75.	Have you established audit control		
76.	Have you developed policy on workstation use and security		
77.	Have you developed security control room and its SOP		
78.	Do you post signs on exterior and interior of facility informing persons of visiting hours, access to facility		
79.	Do you post sign informing individual that their persons or packages may be searched at facility discretion		
IX Perimeter security			
1.	Does perimeter wall or other type of fencing define the perimeter of facility		
2.	Is type of physical barrier on entry and height of fencing adequate		
3.	Is condition of physical barrier good		
4.	Is perimeter barrier and fencing under surveillance at all times		
5.	Does the building wall, floors or roof form part of perimeter barrier		
6.	If so any door window or other openings on perimeter side		
7.	Are all opening in perimeter wall properly secured and guarded		
8.	Are all gates intact and suitable		
9.	Are openings such as culverts, tunnels, manholes, sewer and utility access, side walks which permit access to facility properly secured		

10.	Are gates or other perimeter entrances which are not in active use frequently inspected by guards or other personnel		
11.	Are gates locked in night		
12.	Are appropriate sign setting forth the provision of entry conspicuously posted on all principal entrances?		
13.	Do guards patrol perimeter area		
14.	Are perimeter protected by intrusion alarm devices		
15.	Is fencing under CCTV monitoring		
16.	Is adequate clear zone on both sides of fence		
17.	Are there any poles near fence which can be used for entry		
18.	Is there any tree/ obstruction in clear zone that obstructs clear view of fence		
19.	Any other opening in fence other than gate which are not protected		
20.	Devices used for access control, CCTV, biometrics		
21.	Do gates need repair		
22.	Do they close without gap		
23.	Are gates equipped with lock and key		
24.	Are alarm device used on gates		
25.	Are these gates used regularly during off hours		
26.	Are any of the gates controlled by card reader		
27.	Guards on gate		
28.	Are hinges and lock hasps securely installed		
29.	Are windows that are not used permanently closed		
30.	Are all accessible windows protected by bars		
31.	If windows can be opened and are locked, are they protected by ordinary lever lock or key locks		
32.	Are there any ladders that should be removed, secured, or blocked		
33.	Are there doors with panic alarm fitted with anti intrusion bars		
34.	Are all unused doors permanently locked		
35.	Are opening to roof securely fastened or locked from inside		
36.	Is internal access to roof controlled		
X Lighting			
1.	Is there provision of perimeter lighting		
2.	Is entire perimeter lighted		
3.	Are lighting all through night		
4.	Are light and wiring inspected regularly		
5.	Lights controlled automatically or manually		
6.	Are control switches inaccessible to unauthorized person		
7.	Are parking areas fully illuminated		
8.	Is exterior of building sufficiently lighted to		

	discourage unlawful entry or placement of explosives against wall		
9.	Are public areas sufficiently lighted to discourage attempts against person/ vehicle		
10.	Is lighting adequate for CCTV surveillance		
11.	Is all lights working		
12.	Are all entry and exit gates well lighted		
13.	Does perimeter lighting also cover building		
14.	If lights burnout do light pattern overlap		
15.	Is someone responsible for turning lights on/off		
16.	Are adequate supplies on hand for maintenance of lighting system		
17.	Are gates exposed or protected by lighting		
18.	Are critical area well lighted		
19.	Is the main power source dependable		
20.	Is there a dependable auxiliary power source		
XI Lock and Key			
1.	Are locks changed		
2.	Are locks adequate		
3.	Are lock no recorded		
4.	Key control, staff is responsible		
5.	Does facility have intrusion alarm system		
6.	Alarm on all main doors		
7.	Is key control system in effect		
8.	Are master keys kept secure		
9.	Is duplication of keys approved by key control officer		
10.	Is no of doors/ entrances used reduced to min necessary		
11.	Are keys signed for		
12.	Are keys deposited for		
13.	Does cashier window have security features		
14.	Is a large amount of cash in office over weekends/overnight		
15.	Is there adequate safe vault		
16.	Is cash room protected by intrusion alarm		
17.	Is escort provided to carry money to bank		
18.	Are safe and vaults existing		
19.	Are they provided with alarm		
20.	Is there designated security officer fro the facility		
21.	Are there procedures fro routine daily inspection of the facility		
22.	Is support agreement with other agency written of informal		
23.	Are periodic fire and evacuation drills held		
24.	Are periodic security conferences held		
25.	Are security plans coordinated with appropriate local, state and national agency		
XII Emergency Plan			

1.	Does facility have emergency plan for bomb threat, fire, earthquake, explosion, natural disaster		
2.	Was after action report drafted stating the deficiency		
XIII Fire Safety			
1.	Does building have fire safety policy		
2.	Is building equipped with fire sprinklers		
3.	Condition of fire fighting equipment good		
4.	Is fire /smoke alarm in place		
5.	Are fire alarms functional		
6.	Are these alarm coded to designate which floor alarm came from		
7.	Are fire exits adequately planned		
8.	Is fire extinguisher strategically located		
9.	Is fire extinguisher regularly inspected		
10.	Is each floor equipped with one or more hose in wall cabinet		
11.	Are those lines connected to those risers that are used for sprinkler system		
12.	Is water pressure in riser on all floors sufficient to handle both sprinkler and hoses		
13.	Is building equipped with fire pumps to keep pressure in these lines high enough to be effective		
14.	Are these pumps manned		
15.	Are fire hose valves at each hose station tested		
16.	Is the fire hose and play pipe tested to ensure that it is rotten/cut/obstructed		
17.	Are there any fire walls dividing floors of the building		
18.	Does building have adequate water supply		
19.	Are fires doors normally open or close		
20.	Is building equipped with fire stairwell		
21.	Are fire stairwell compartmentalized to protect against smoke seepage		
22.	Are fire doors of fire stairwell made of fire resistant or fire proof material		
23.	Does each floor of building form a compartment which would effectively block fire from spreading to other floor		
24.	Are air conditioning and ventilating flues equipped with dampers which would close automatically in case of fire		
25.	Are these dampers regularly maintained and tested		
26.	Are certain elevators set aside for use by fire department		
27.	Are all OS & v valves in the riser in an open position and sealed		
28.	How many public fire hydrants are available within the building		
29.	Is all combustible trash immediately removed or		

	safely stored to avoid fire		
30.	Is all fire fighting equipment inspected regularly		
31.	Is record of inspection maintained		
32.	Does facility comply with local fire codes		
33.	When was facility last inspected by city fire officer		
34.	Does building have fire alarm		
35.	Does building have smoke detectors		
36.	Does building have fire extinguisher		
37.	Does building have sprinkler system		
38.	Do basement have intrusion alarm		
39.	Are basement doors securely fastened or locked when not in use		
40.	Are doors to basement and attic locked when not in use		
41.	Are air conditioning and heating vent opening in public areas secure from tampering		

Appendix C

EVENT SPECIFIC PREPAREDNESS

S NO	Events	Checklist standards applicable	Conformance score	Con and Non con	Percentage
1	Theft	Score of security staff selection & training + staff identification +Access visitor & public+ technology application+ perimeter security + lock & key	96	151	63.57
2	Terrorism/ Bomb Threat/ Hostage Situation	Score of Standardized security management plan+ Security staff selection and training+ Technology application+ General employee security training+ Emergency plan	47	71	66.19
3	Infant Abduction	Score of Standardized security management plan+ Security staff selection and training+ General employee security training+ staff identification+ Access visitor & public+ Lighting	94	128	73.43
4	Strike	Score of Standardized security management plan+ Security staff selection and training+ Misc administrative safeguards	78	120	65
5	Misbehavior	Score of Standardized security management plan+ Security staff selection and training+ General employee security training	36	52	69.23
6	Conflicts/ Workplace Violence	Score of Standardized security management plan+ Security staff selection and training+ General employee security training+ Access visitor & public+ Misc administrative safeguards	113	163	69.23
7	Fire	Score of Emergency plan+ Fire safety	31	58	53.44
8	Hazardous material Exposure/Leak	Score of Standardized security management plan+ Security staff selection and training+ General employee security training+ Emergency plan	47	61	77.04
9	Traffic management	Score of Standardized security management plan+ Security staff selection and training+ Perimeter security+ Parking and transportation	65	86	75.58
10	Sexual offence	Score of Standardized security management plan+ Security staff selection and training+ General employee security training+ Access	76	113	67.25

		visitor & public+ Lighting			
11	Absconding	Score of Standardized security management plan+ Security staff selection and training+ General employee security training+ staff identification+ Access visitor & public+ Lighting	95	128	74.21
12	Animal Nuisance	Security staff selection and training+ Perimeter security	86	130	68.15
13	Suicide/Attempted suicide /General	Score of Standardized security management plan+ Security staff selection and training	67	94	71.27
14	Fraud/Imposter	Score of Standardized security management plan+ Security staff selection and training+ Access visitor & public	35	52	67.30