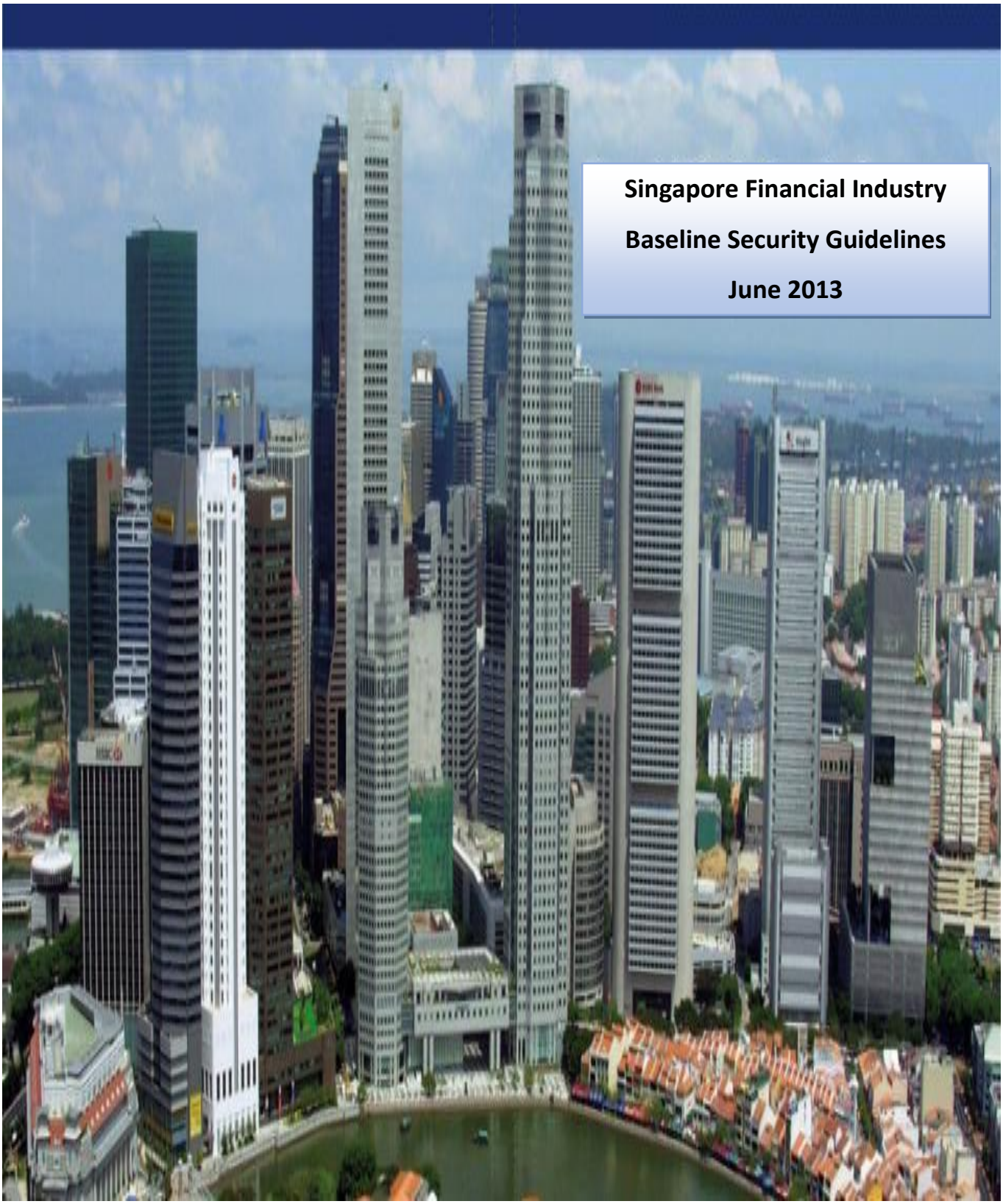

Singapore Financial Industry Baseline Security Guidelines

June 2013

CONTENTS

SCOPE

This document* addresses physical security from five dimensions, namely Intelligence, People, Structures, Systems and Procedures.

- The **Intelligence** dimension refers to the ability to leverage on information sources to identify and assess issues that create risks to the organization so as to facilitate physical security protection against the identified risks.

- The **People** dimension deals with enhancing security personnel and staff capability in maintaining security and protection during peace time and security-related incidents.

- The **Structures** dimension addresses the leveraging of resilient structures to protect assets and infrastructure.

- The **Systems** dimension addresses the use of security protection technology to detect, reduce and mitigate the risk of security violation.

- And, finally, the **Procedures** dimension refers to establishing and formalizing administrative processes to enhance physical security protection and to reduce the impact of a violation.

* Developed by the Financial District Security Programme (FDSP)

1. INTELLIGENCE

Intelligence relates to information gathered by an organization for the purposes of detecting, identifying and assessing issues that create risk to the organization. The provision of timely, accurate and objective intelligence serves to prepare the organization against these risks and helps to guide security decisions and actions in relation to the organization's risk management processes.

1.1 Mitigation

Information is the currency of intelligence. The mitigation phase under the Intelligence dimension deals with activities pertaining to information gathering, analysis and dissemination.

1.1.1 Information Gathering

- Organizations are recommended to tap on a variety of open sources for information. These include (but are not limited to) media sources, commercial vendor reports, and public databases.

- Where relevant, organizations are recommended to participate in national forums and initiatives that provide platforms for information gathering and sharing. Examples include:

    1) The Financial District Security Programme (FDSP) or other security related forums such as the Singapore Police Force's Project Guardian.

    2) The Singapore Police Force (SPF) SMS alert scheme, which provides updates on crime related news.

- Organizations are also recommended to join the relevant industry bodies such as the Sister Banks Group (APAC) or Association of Banks in Singapore so as to establish networks with industry peers

and obtains regular communication on industry-specific security issues.

- Additionally, organizations are encouraged to send their security officers to join professional security associations to establish a network of contacts with local and regional practitioners.

- Where relevant, security officers are also recommended to attend seminars, conferences or talks by local think tanks or institutions to obtain insights from and establish networks with subject matter experts on security-related issues.

1.1.2 Information Analysis

- Following the gathering of information based on the organization's requirements, the information should be analyzed, placed in the relevant context and used to assess the potential physical security implications for the organization.

1.1.3 Dissemination of Intelligence

- Intelligence should be disseminated in a timely manner to the relevant organizational stakeholders to facilitate the initiation of appropriate actions and response by the organization.

- Where appropriate, and subject to organizational policies and guidelines on information sharing, organizations are encouraged to share non-sensitive information and/or intelligence with relevant industry peers.

1.2 Response

The Response phase under this dimension typically involves activities pertaining to the monitoring of developments relevant to the incident as well as the management and dissemination of situational updates to the relevant parties. The organization is recommended to:-

- Perform continuous monitoring of the situation from various sources and provide situational updates to the relevant stakeholders as per organizational requirements.

- Determine if the current mitigating and response actions (all 5 dimensions) implemented are still sufficient and if further actions are required.

1.3 Recovery

The recovery phase would be a reflective process in which all stakeholders draw upon the lessons learnt from the security incident. Gap analysis and review should be performed on:-

- Adequacy of existing measures put in place in all 5 dimensions namely Intelligence, People, Structures, Systems and Procedures.

Where gaps are identified, more robust measures should be made to address these gaps.

2. PEOPLE

Employees are the greatest asset of an organization. Therefore, the safety of employees should be the primary priority of an organization during a security incident/crisis. From another perspective, an organization's employees also play an essential part in protecting the organization. In particular, management commitment is critical for conveying the importance of physical security to employees across all ranks and files. The management should lead by example to demonstrate their support in this area.

During normalcy, staff members need to be trained and made aware on how to react and respond to security-related incidents. Upon the occurrence of security incidents, swift communication to staff is vital in order to prevent speculation and panic, hence maintaining morale within the organization.

2.1 Mitigation

The mitigation phase would involve conducting appropriate background screening of employees, implementing security awareness and training (A&T) programs as well as having stringent selection criteria for security enforcement personnel within the organization.

2.1.1 Employees and Contractors/ Consultants/ Vendors Background Screening

The organization should conduct background screening and checks in line with regulatory requirements on new employees and external contractors / consultants / vendors prior to them joining or performing work for the organization, especially for employees working in security-related departments.

2.1.2 Security Officers/ Guards

All security officers/ guards must be licensed or exempted by the Security Industry Regulatory Department (SIRD) and should be effectively screened and selected to ensure personnel with integrity are employed.

The SIRD uses a grading system of A, B, C and D to gauge and accredit the operational and service standards of Security Guard Agencies (SGAs). In general, preference should be given to SGAs that are accredited grade B and above.

Prior to employment, security personnel must be appropriately certified through the Security Workforce Skills Qualifications (WSQ) programmes. Upon employment, all security personnel have to be continuously trained in security and safety related procedures including but not limited to:-

- Basic fire fighting
- Basic first aid
- Emergency response and evacuation procedure
- Bomb call/hoax procedure
- Suspected mail bomb / article response
- Basic initial fact finding procedures

The security personnel are also required to regularly participate in drills and exercises in order to familiarize themselves with established procedures and responses.

Security personnel should also be roped under SPF's "Project Guardian" and be trained under the programme on security and terrorism related knowledge.

2.1.3 Mailroom Personnel

All mailroom personnel should be properly trained on the security procedures to identify and handle biological, chemical, weapons, explosives and other suspicious items. Temporary relief personnel should be sourced from renowned and established job agencies that have a ready pool of security cleared personnel.

2.1.4 Security A&T Program

A comprehensive role-based safety and security A&T program is required to be given to all employees. The A&T program should be dynamic and regularly reviewed and updated, to ensure relevancy of the education materials. The program should also look into refresher courses.

The security training program should be designed and formalized to suit various roles of the employees in the organization. Such training can be conducted via traditional classroom style or through exercises as well as online platforms etc. Awareness programs can be delivered in various modes such as through newsletters, brochures, posters, bulletins, info packs etc.

The security A&T program can also include the pre-identification and training of staff that double as security marshal during an incident to support the work of security personnel.

The organization should also consider participating in the SPF's Corporate First Responders program to ensure prioritized return to their facilities (if in the impacted zone during an incident).

Daily security awareness briefing should be conducted for all security personnel.

2.2 Response

The response phase under the People dimension involves managing emergency response teams, staff accounting and management of staff sentiment and morale. This would include:-

2.2.1 Management of Incident

The various emergency response teams must be clear about their duties and areas of responsibility during an incident and that they are able to discharge their roles & responsibilities effectively and swiftly. Organization's Corporate First Responders (CFRs) should be activated where necessary.

2.2.2 Employee Accounting

Where evacuation is invoked, the relevant department / party needs to commence employees accounting where required so that employees in the organization are accounted for.

2.2.3 Employees' Communications

It is very important to manage staff sentiment and morale when a security related incident occurs. This can be achieved through constant communication with the employees via the various communication platforms available in the organization. Human Resources personnel should provide counseling to distraught employees as a result of the incident.

2.2.4 Review of Security needs

When an incident occurs, the deployment of additional security personnel should be considered and the increase should be based on the nature of the incident, its impact on the organization and the level of risk elevation.

Further support can be requested from the police. The type and level of support rendered will depend on the nature of the incident and its threat level, among other considerations.

2.2.5 Security Awareness

Security briefings should be conducted to all security personnel and relevant / suitable information should be disseminated to all employees to sensitize staff to suspicious or potential malicious act(s) against the organization.

2.3 Recovery

Recovery phase focus on building back employees' capability to operate the organization's businesses.

2.3.1 Continual physical security protection

After an incident, there is a need to ensure a continued strong presence of security personnel within the organization's premises to provide assurance and a sense of security to employees.

2.3.2 Employees' Communications

Communication with employees should not stop immediately after the incident has ended. Instead, various communication channels should still be available for employees to express their thoughts and viewpoints. Counselors should still be made available for employees.

2.3.3 After-incident Review

An after-incident study should be conducted to review existing measures in screening or training of employees as well as the communications procedures to employees and to make improvements to areas of weaknesses where applicable.

3. STRUCTURES

A resilient building infrastructure is essential to reduce the vulnerability of the organization against security disruptions. Factors such as location, environment, natural physical barrier and general infrastructural protection (e.g. stand-off distance) help to provide security to staff and business.

Stand-off distance is the distance between an asset and a threat. There is no ideal stand-off distance and the range is determined by the type of threat, methods of construction and the preferred level of protection. The recommended range or set back distance is about 3 meters from the common boundaries.

However it is not always possible to achieve ample stand-off distance in an urban environment like Singapore, so maximizing the distance may be the most effective solution.

Business operations in the financial industry are highly diverse; therefore the structure security standard varies from one business to another, due to the difference in risk level. The risk level should be assessed based on 2 key factors:

- Cost of site loss
- Scale of business impact

All properties should be risk assessed so that appropriate structure standards can be implemented. Properties can be defined into the following types:

- Retail Cash Operations (e.g. Cash Vault): processing cash from/to various retails branches or ATM.
- Standalone datacenter
- Vault & Safe room

- Head or regional office
- Disaster recovery site
- Operational Building: operating beyond business hours or /and Office: operating mainly during business hours or/and with significant negotiable, vault, security containment rooms or datacentre.
- Office: operating mainly during business hours or/and with no significant negotiable, vault, security containment rooms and datacentre.
- Retail branches
- ATM, Electronic Banking locations

Depending on the location, an organization can also consider applying the CPTED method (Crime Prevention through Environmental Design) such as soft or hard landscaping for protection.

3.1 Mitigation

When developing the physical security plan for one's facility, it is paramount to identify all critical assets – tangible and intangible – and reduce the risks to them to an acceptable level.

You must take into account the following crucial elements – deterrence, detection, delay and response and then recovery and re-assessment. These mitigation measures make the foundation which any integrated physical security plan must be built on.

The mitigation phase under the Structure dimension would involve conducting assessment of the risk exposure of the building to physical threats as well as putting in effective controls to reduce the probability and

impact of the risk materializing, thus resulting in avoiding severe physical disruption.

3.1.1 Physical Security Vulnerability Assessment (Risk Assessment)

An organization should periodically conduct vulnerability assessment of their properties, including the surrounding neighbourhood, to identify potential natural and manmade threats, areas of physical weaknesses and / or potential single point of failure in the infrastructure setup.

3.1.2 Enhancement Measures

It is crucial that sufficient and appropriate structural physical security measures relevant to the identified threats are being put in place. Some of the good practices include, but are not limited to, the followings:-

a. Location

Different operations need to consider various criteria when deciding on a location – Is the area business-friendly? Does the area satisfy the needs of your business?

When there is an opportunity to choose new office locations, the following locations should preferably be avoided to reduce the vulnerability of the organization:-

- Locations near potential hazards such as petrol kiosks, chemical processing/storage facilities etc. Standalone and non personnel manned facilities such as ATM may not be subjected to this consideration.

- Locations identified by authorities to be vulnerable to security threats.

- Locations identified as flood prone zones.

- Buildings with poor lighting within or surrounding the compound, with few access / escape routes, with no or insufficient CCTV coverage and fire detection / suppression system etc.

b. Provide Stand-off Distance

For medium to high risk facilities, suitable stand-off distance should be provided between buildings and a potential vehicle bomb which might be in a car parked next to the building. Stand-off distances could be achieved by passive measures such as planter boxes, bollards, low screen walls etc or by security measures such as access control, surveillance, detection etc.

c. External Protection

For high risk facilities, robust external perimeter protection which acts as a strong deterrence to potential criminals is highly desired. Wall and fence with at least 1.8m in height should be continuous, sturdy and monitored by CCTVs to create a physical deterrence to unauthorized entry. Adequate lighting should also be installed to spot abnormalities and deter criminal activities. Where possible, Fence Intrusion Detection System (FIDS) can be installed at the installed fencing.

Note: Urban Redevelopment Authority (URA) may have a restriction on fence heights at 1.8 metres.

All properties except non personnel manned facility (e.g. ATM): The number of entry points of a building should be minimized and all approachable access points should be appropriately controlled. Exterior doors and windows on the first and second floor should be of sturdy and fixed construction respectively. External windows, doors and glass walls vulnerable to damage may require protection such as shatterproof film.

It is necessary to strike a balance among the security needs, the cost, the complexity and the architectural impact of meeting the objectives.

d. Internal Protection

All properties except non personnel manned facility: There should be physical barriers between the public and non public areas and constructed to be protected slab to slab. Additional segregation should be considered for sensitive areas.

Teller service: The layout of the property should not allow money to be carried across public spaces when transferred between vault or safe and teller. Access to the back of the teller should be restricted and screened from public view. Teller counter should be sufficiently high and wide to prevent unauthorized access to cash drawers from the public area.

Vault: Defined as a room that is designed for the safekeeping of significant amount of valuables including cash and negotiable or for safe keeping facilities. Depending on the valuable kept; the vault should be constructed to meet the minimum standard of Underwriters Laboratories (UL) Class 1. Each vault should have a lockable day gate and steel door equipped with dual access control devices and preferably with time lock.

ATM, Electronic Banking machines: Automated teller machine (ATM) or Electronic Banking machines is a computerised telecommunications device that provides the client access to a variety of services in a public space without the need for a bank teller.

e. Separation between vulnerable Operation Areas from the main Business Operation Areas

For medium to high risk facilities, high risk operations areas such as Delivery / Loading Bay, Mailroom etc should preferably be situated away from the main business operation areas where possible. If this could not

be done, these high risk operation areas should be situated away from building's critical columns or transfer beams.

These areas should be well lit and installed with CCTVs to provide surveillance of these areas at all times.

The entrance to the Delivery / Loading Bay must be designed with an access control system or security personnel. The gate and access control point should be placed as far away from the building as possible and, ideally, should not be placed under the building and/or below or next to a primary structural element.

Delivery and service vehicles serving the building should be scheduled, subject to access control and monitored.

The Mailroom should be located near the entrance to the building in order to prevent delivery people from unnecessarily entering the building. It should be located to the side of the building and never in or attached to a main structural element such as a building core or staircase.

It is recommended that the Mailroom should have no connection to the building's main ventilation system or opening. The Mailroom should be provided with an electricity and low voltage infrastructure to support X-ray equipment, HHED and other detection equipment.

In short, knowing the core functions of one's facility will enable one to identify the specific critical infrastructure that need protection and to ensure business continuity in the event of an attack.

f. Emergency Power Supply

Emergency electrical power supplies maintain critical building and business operations (e.g. datacenter) functions when normal power supply source fails. The provision of an adequate and reliable alternative supply

of electrical power will minimize risk to employees and customers as well as to building security.

All critical operations areas should preferably be backed by A/C synchronous generator(s) with day tank fuel sufficient for 24 hours of operation. These standby generator(s) should have the capability to automatically detect loss of primary power supply and start operation no longer than 6 seconds after loss of the primary supply. Where required, uninterrupted power supply (UPS) system should be installed to ensure no drop in power after primary supply is cut off and before the standby generator kicks into operation.

All emergency escape signage, emergency lightings, alarms and emergency communication systems should be equipped with battery packs sufficient to continue operation for 2 hours after lost of primary power supply.

g. Protection against flying glass

All properties except non personnel manned facility: With more buildings designed with significant amount of glazing or glass finishes, such materials can shatter into sharp, high velocity fragments in the event of a blast, which have high potential to injure employees and passer-bys. Therefore, it is crucial to protect against flying glass by applying a transparent polyester anti-shatter film to the glass or install laminated glass which is more blast resistant or install a blast resistant secondary glazing on the inside of the existing exterior glazing.

Window frames holding these glazing should also be designed properly to achieve the intended result. In other words, securing the anti-shatter film to the frame with a mechanically connected anchorage system further reduces the likelihood of the glazing system exiting the frame.

h. Critical Equipment

All properties except non personnel manned facility: Critical equipment is defined as equipment that is essential for building and business operations and building evacuation. Critical equipment may include (but is not limited to) machines that support electrical power supply (e.g. transformer and generator set), water supply, air supply (e.g. air handling unit and chiller room), communication & network and fire protection system. These equipments should be located in areas which are well away from potential threats. They should therefore not be close to public car park or public areas. If this is not possible, then the rooms must be built with adequate protection. Entrances to the rooms should be locked at all times, controlled by an access control system, CCTV and intruder detection system. Access should only be permitted for authorized personnel.

Finally measures against flooding should be considered for these equipments.

i. Air Intakes

With air intakes providing fresh air to the Air Handling Unit (AHU) to be used by the central air conditioning system of the building, these intakes can be vulnerable to sabotage such as chemical-biological contamination. As such, all air intakes for the building should be protected and access by unauthorized persons prevented. Where possible, they should be situated at high ground where access to them is not possible by simple means.

3.2 Recovery

The recovery phase would involve a vulnerability assessment as well as a structural analysis of the organization physical compound.

3.2.1 Structural Analysis

Structural professionals, together with BCA, SCDF as well as other relevant government authorities, should be engaged to review and ascertain any damage or potential damage to the organization compound so as to ensure that appropriate actions can be taken to ensure safety of the employees and customers.

3.2.2 Vulnerability Assessment

Security personnel are to conduct an assessment of the organization compound to identify any potential vulnerability in the physical security protection of the organization compound. Rectification must be done as soon as possible to restore the protection to the level before the incident.

3.2.3 After-incident Review

An after-incident study should also be conducted to review potential weaknesses in the existing structural physical protection and make physical and/or procedural improvements to strengthen these weaknesses.

REFERENCES

- Ministry of Home Affairs - Guidelines for Enhancing Building security in Singapore (GEBSS), updated as at July 2010.

4. SYSTEMS

With the advent of technology, organizations are turning to more sophisticated equipment to ensure security protection within their premises. Integrated systems such as Closed Circuit Televisions (CCTVs) greatly facilitate the monitoring and surveillance of premises as they can be administered to operate 24/7, thereby complementing monitoring by security personnel.

4.1 Mitigation

This phase involves the selection and implementation of appropriate security systems in order to improve the physical security protection of the organization. Listed herewith are some of the suggested systems that should be implemented:

4.1.1 CCTVs

The primary purpose of a CCTV system is to support and enable the overall management of a premises security. Video surveillance facilities are an aid to security monitoring, especially of vulnerable or sensitive areas. CCTV systems may also act as an investigative tool as a post-incident source of evidence, or may deter potential criminals/terrorists if they perceive that their actions are being monitored.

Sufficient numbers of CCTV cameras should be installed in strategic/remote locations such as perimeter fencing and building perimeter (where applicable), lobbies, teller counters, ATMs, offices, data centres, vaults and critical equipment rooms etc. to provide coverage as well as to act as an overt deterrent. Suggested guidelines are as follows:

- Common Areas : Cameras in common areas should be situated where they cannot be easily evaded, damaged or obscured and should be visible to members of the public. Where headroom is restricted and

cameras may obstruct public passage, cameras should be mounted in recesses so as to avoid the possibility of injury to members of the public.

- Entrances & Exits: All external public access doors, emergency exits and vehicle entrances/exits (e.g. at the gantry point of car parks), loading bays and lift lobbies should be fitted with cameras that provide a clear, unobstructed 'face on' image of all persons entering/exiting including vehicle type and registration no. entering/exiting such areas.

- Cash Handling Areas/Teller Counters: There must be CCTV camera coverage at the cash handling areas/teller counters to record activities and that such camera activity and be able to provide a clearly identifiable[1] (not less than 120% R) image of the person.

- Self Service Machines (ATMs, CDMs etc) at Electronic Banking Lobbies: The CCTV system installed should provide a clearly recognizable (not less than 50% R) image of the person using the machine. For drive up facilities, it is recommended that a CCTV camera be positioned to view the vehicle/license plate.

- In sensitive areas such as Vaults, Safe Rooms & Data Centre, the CCTV cameras should be installed and focused at the entrance/exit. Depending on the usage, CCTV cameras should also be installed to record in-room activities (e.g. access to the safes/vaults).

[1] The categories are measured by relating the views to the image height of a standard test target 1.6 m high. When the image of the target fills the screen vertically the image height is said to be 100%R., where "R" is the abbreviation of "Rotakin".

The CCTV system should be operated on a 24/7 basis and all motion footages recorded. Images should not be kept longer than necessary but as a basic guide, CCTV storage systems should have sufficient storage capacity for no less than 28 days. Image resolution should preferably be in colour and sufficiently clear to ensure that persons are recognisable.

CCTV recording equipment should be located in a secured facility which can be accessible by authorized personnel only.

4.1.2 Electronic Access Control System (EACS)

Access control is the ability to regulate movement into specific areas or to access critical assets. Maintaining an effective EACS is a fundamental principle of good access control management.

Access control should be established at all relevant and appropriate entrance/exit points within the organization. In customer facing areas such as building lobbies and bank floors, it may not be possible to implement stringent access control procedures; however, access into the sensitive areas of the office/buildings must be strictly controlled and monitored via the access control system.

A good practice is for the organization to create security level zoning with role-based access privileges. Examples and definition of possible zones may be as follows:-

Accessibility Controls	Definition	Accessible to
None	Public Areas	All
Limited	Visitors Areas	All employees and visitors with names pre-submitted to Security Office
Moderate	Employees Common Areas/offices etc	All employees
High	Restricted Areas	Selected employees

ECS controlled turnstiles and doors should be set up at all main entrance/exit points. Magnetic door lock systems, activated by the organization's access card system, should be implemented and operated 24/7.

Dual access control measures should be considered at High Risk/Sensitive area/Restricted area (e.g. Data Centre). The EACS should be supported by a back-up power supply.

A periodic review of user access rights should be conducted to ensure that only authorized entrants are able to move within controlled areas.

Access to emergency escape stairwells should be controlled. Any unauthorized attempt to access such doors may be denied electronically or may trigger an appropriate alarm signal either to a remote alarm monitoring centre such as the Security Post or locally.

Employee access card (biometrics/swipe/proximity type preferably photo-ID) should be issued to all employees. They should be educated and reminded to display their passes whenever they are within organizational controlled areas. Employees can only gain access into zones based on their pre-assigned roles. Organisations should operate an effective

joiner/mover/leaver process, with leaver notification being automatically issued in a time efficient manner to the Security Control Office as part of this process.

4.1.3 Visitor Management System (VMS)

VMS refers to the tracking of the usage of a building or facility by non-staff. VMS records the movement of visitors and provides documentation of visitor's intended whereabouts. These systems are frequently used to complement building security and access control systems.

All visitors visiting the controlled area should be pre-registered with the controlling department. This may vary from organization to organization but may be the Facilities and/or the Security Office. Visitors should generally be restricted to lower security level zones and be accompanied by at least one employee.

The use of VMS is encouraged, and where not deployed, the organization should practice a sign-in/out process.

4.1.4 Car Park System

Many crimes occur in car park areas. Such crimes can be reduced by implementing appropriate security design changes and effective management practices.

All car park entrances and exits should be installed with a gantry control system operating on a 24/7 basis. When the car park is closed, roller shutters should be installed to prevent access.

CCTV cameras should be installed at strategic locations within the car park, with priority given to entrance and exit points. The car park should

also be well lit and Security Officers should conduct regular patrols in the car park areas to deter crime.

Employees' and visitors' parking lots should be separated where possible. Visitors should not be designated parking lots adjacent to critical Mechanical & Electrical (M&E) installations or other critical facilities. Parking facilities should be suspended at times of high external threat levels as part of an escalation plan.

4.1.5 Alarm System

Alarm systems installed in buildings are aimed at detecting unlawful, unauthorized intrusion and duress entry into an area. The alarm system monitors a variety of alarm detection/ triggering devices (for example, panic buttons, motion detectors, door contacts etc). Upon activation of any alarm, the system will either activate a local siren and/or transmit the alarm signal to a remote alarm monitoring centre or directly to the Police.

For high risk areas, back-up transmission capability should be incorporated in the alarm system. The system should be also equipped with independent back-up power source and a control panel placed in a secured area.

Alarm sensors should be installed along the perimeter fencing (where applicable), doors and windows. Safes, vaults, ATMs and other identified high value assets should also be protected by a security alarm system.

Duress alarms should be installed at cash handling/processing areas, teller counters, vault rooms, reception desk, guard's location etc.

4.1.6 Guard Tour Management System (GTMS)

The use of GTMS is encouraged to ensure a systematic approach, providing adequate security coverage within all strategic and vulnerable areas.

Guard tour checkpoints should be established near the entrances, exits (especially those that are obscured), risers, water tanks, air handling units (AHU) etc. The frequency and guard tour routes should be in accordance with a predetermined plan, which should include varied frequency and routes to avoid elements of predictability.

4.1.7 Mailroom Security System

Subject to a risk based assessment, provision of special equipment in mailrooms to detect explosive/toxic substances etc such as X-ray scanning machines, access control, security zoning, CCTVs and alarm system may be considered.

4.2 Response

The response phase involves the activation of relevant security control systems to address an impending security disruption.

4.2.1 Panic / Intruder Alarm Activation

The Duress/Intruder Alarm System should have the following features:-

- Silent alarm which will alert the security control room or an alarm monitoring centre

- Integrated with the CCTV system so that when the alarm is activated, the CCTV system should switch from time-lapse recording to almost real-time recording.

4.2.2 Enhanced EACS & VMS

- Security personnel should conduct thorough security checks on employees, vehicles entering into the organization's compound.

- Restrictions to be considered on visitors/contractors entering the compound facilities during the response phase. In a situation where this is not possible, there should be enhanced security checks conducted on all visitors.

4.3 Recovery

The recovery phase may include resetting security systems, follow-up action to analyze images, review of access logs, collation of evidence and a post mortem on preparedness and response. Enhancements to systems should be made where vulnerabilities are identified.

5. PROCEDURES

Administrative controls such as Standard Operating Procedures (SOPs), guidelines and plans would help to strengthen the security structure and systems put in place to deter physical security disruption. It also improves the readiness of an organization to manage a security incident.

5.1 Mitigation

The mitigation phase would normally involve putting in place all the relevant procedures and SOPs for operations and plans related to physical security.

5.1.1 Formulation of procedures

All security related procedures should be formulated and disseminated to all relevant staff. Some of the SOPs should include:-

- Security Personnel Operation Manual

This manual should include all the knowledge required by the security personnel pertaining to the organization's security prevention, detection and correction systems such as the alarm systems, security zoning, patrol routes etc.

- Access Controls Procedures

Access Controls procedures should spell out all the checks and controls required of all the different access points in the building / organization, including car parks, office compound and perimeter compound.

- Mailroom Security Operation Manual

A security operation manual should be drawn up to guide mailroom employees on the “Dos’” and “Don’ts” with respect to maintaining a secure mailroom operating environment.

- Critical Utilities Maintenance & Services SOPs

SOPs should be established to ensure that critical infrastructure (such as AHU, power switchboards, PBX room etc) are subjected to routine maintenance. In addition, the SOPs should ensure that access to these areas is strictly restricted to authorized personnel only.

- Emergency Response Procedures

Emergency Response Procedures should be established and disseminated to all employees to guide them with the correct response actions in dealing with a security incident or emergency. Such procedures can be disseminated via the Security A & T programme.

- Office Workstation Practices

Guidelines should be issued to all employees with regard to the adoption of good practices (i.e, clean desk policy etc) to guard against physical security threats. These guidelines should complement the Security A&T Plan.

- Security A & T Plan

There is a list of possible guidelines and procedures to be set up for physical security protection. The organization should ensure that all the procedures formulated should be propagated to the relevant employees.

In this regard, a systematic Security A&T programme should be drawn out to ensure that all relevant employees are aware of and updated on all the standing emergency procedures.

5.1.2 Exercises & Drills

Regular security-related exercises and drills should be conducted so that employees are constantly updated and made aware of the various emergency response procedures as well as to identify and address gaps in the emergency plans and SOPs.

5.2 Recovery

The recovery phase primarily involves conducting an after-incident study on the effectiveness of the procedures in place and to make the relevant and appropriate amendments to the procedures that require enhancements. Revised procedures should be propagated to the relevant personnel.