Journal of Contemporary Research in the Built Environment ISSN: 2636-4468
Volume 7, Number 1, March 2023 

# FRAMEWORK FOR SECURITY RISK MANAGEMENT OF GOVERNMENT ADMINISTRATIVE FACILITIES IN SOUTH-SOUTH, NIGERIA

***Fernandez Kosisochukwu Chiama***[1]***and Nsikak William Ulaeto***[2]
[1&2]Department of Building, University of Uyo, Akwa Ibom State, Nigeria

## ABSTRACT

**Purpose:** Unpredictability of the nature and magnitude of threats on government administrative buildings in the South-South region of Nigeria draws to light the need for effective facility security risk management frameworks. These frameworks are needed to assess the risks associated with threats and possible approaches to their mitigation or integration. This study proposes a framework for the effective security risk management of government administrative buildings in the South-South region of Nigeria, in a view to ensuring the safety of staff and visitors; the security of functions and equipment; and protection of the integrity of the arms of government that own these facilities.

**Design/methodology/approach:** The study employed a descriptive survey research design approach. Twelve federal and state government secretariate buildings from six states in the South-South region of Nigeria were directly observed. Direct observations provided primary data on facilities characteristics and security structure over twenty-four hours of a regular working day. Using these data, a facility security risk management framework unique to these facilities was developed. The framework incorporated the event tree logic model and qualitative risk matrices. Data obtained from the twelve government administrative facilities were applied to the proposed framework, considering three threats identified from literature to be most likely to occur on these facilities.

**Findings:** Results showed that risk measures were acceptable in all facilities but for facilities labelled DA and FB, for public order incidents and kidnappings respectively.

**Research limitations/Implications**: Threats considered were limited to those that were malevolent and of a "low probability and high consequence" nature. Government administrative facilities considered were federal and state civil service administrative facilities also referred to as secretariat facilities. The study showed that an effective facility security risk management framework was needed to ensure safety and security in government administrative facilities.

**Practical implications:** The study also showed that the framework proposed in this study was quite capable of meeting the need for an effective facility security risk management framework in government administrative buildings.

**Originality/value**: The study sheds light into the preparedness and response of government administrative facilities to threats. The dynamism of the proposed framework promotes the adaptability of these facilities to changing threats, threat likelihoods and consequences. Therefore, enhancing the safety of these facilities.

**Keywords: A**dministrative buildings; Risk management framework; Safety; Security; Threats.

[1] Email: chiamakosiso@gmail.com

# 1. INTRODUCTION

## 1.1. Background of the Study

The occurrence of accidental and malevolent events on public facilities is of great concern to facility managers, security managers, security agencies, government and the general public. This is evident in the huge public outcry, security measures and government policies put in place after the occurrence of these events (National Research Council, 2002). Where the risk of accidental events can be significantly reduced through psychological and direct physical means, the risk of malevolent events requires carefully planned approaches geared towards their mitigation. This is because these events are carefully planned to exploit the vulnerabilities of targeted facilities with no concern for psychological or weak physical measures provided (Clarke, 1992; and Clarke, 1995). Hence, they constitute a serious threat to the targeted facility.

Threats and their consequences could be of various magnitudes and severities, respectively. They could also vary based on the rational of the perpetuators. Classification of threats, take into consideration the magnitude, severity and motives of perpetrators. Classification includes but is not limited to terrorism, sabotage and vandalism (Baybutt and Ready, 2003). However, events of recent years have shown terrorism to be the most frequently occurring threat internationally. Past events of this nature have ranged from "high probability – low consequence" to "low probability – high consequence" cases. Low consequence threats are often aimed at soft targets and low consequence class facilities. Examples include the 2013 Boston Marathon bombing in the USA (Associated Press in Boston, 2013). High consequence threats focus on high consequence class buildings and facilities. Threats on high consequence class buildings often aim at the chain effects of actions, which increases exponentially, the consequences (Ulaeto, Sagaseta and Chryssanthopoulos, 2022). Attack on the Alfred Murray building in Oklahoma, USA (Byfield, Mudalige, Morison and Stoddart, 2014), provides an ideal example of a "Low probability – high consequence" threat, which would have been avoided had effective facility security risk management strategies been put in place. In the case of the Alfred Murray Building, an explosive laden truck was parked and ignited in front of a federal government building. Consequences of this attack would have been either eliminated or significantly reduced, were vehicle parking and access control measures been implemented. Consequences directly resulting from the occurrence of threats may include injuries and psychological trauma to staff, clients and visitors to the facility, loss of life, damage to the structure or the total collapse of the structure, damage to properties and equipment, loss of function of the facility and a dent on the reputation of the government or agency. Mitigation of the likelihood and consequences of these threats are carried out using risk management strategies implemented by facility managers.

Challenges of the past decade have place great demand on the responsibility of facility managers in Nigeria (Agwu, Onwujekwe, Uzochukwu and Mulenga, 2021). This is due to rising insecurity in the country. Nigeria has experienced a spike in the number of malevolent events in the past two decades emanating from the activities Boko Haram terrorist in Northern region, threats from the Indigenous People of Biafra (IPOB) in the South East region, activities of militant herdsmen and most recently the end SARS movement (Onifade, Imhonopi and Urim, 2013; and Ndubuisi-Okolo and Anigbuogu, 2019).

The South-South region of Nigeria has not been exempted from this string of events. The Boko Haram terrorist group poses a great threat to government facilities and infrastructure in the South-South region of Nigeria. The same can be said of the IPOB group. However, of greater historical significance, are the agitations of Niger-Delta militancy groups based in the South-South region of Nigeria (Onifade, Imhonopi and Urim, 2013; and Ndubuisi-Okolo and Anigbuogu, 2019). Niger-Delta militants in the South-South region of Nigeria have been responsible for the destruction of government infrastructure and multi-national firms' facilities. They have also been responsible for kidnappings, injuries and fatalities in the South-South region of Nigeria. Though activities of this militant groups have reduced significantly in recent years due to agreements made between the group and the Nigerian government, risks associated with threats from these militant groups remain high in the South-South region of Nigeria (Newsom, 2011). Of important note also, is the "End SARS" movement with protests and attacks carried out Nation-wide and other unrests peculiar to certain institutions and facilities. On 22nd October 2020, a group of "End SARS" protesters attacked and set ablaze an administrative building of the state government-owned Akwa Ibom State Broadcasting

Cooperation (AKBC), located in Uyo, Akwa Ibom State (Ukpong, 2020). Akwa Ibom State is a state in the South-South region of Nigeria and similar incidents were reported in other South-South states (Ukpong, 2020). Most of the events due to these agitations are malevolent and violent with political or social objectives. As such, symbols of government tend to be prime targets. Government administrative facilities are symbols of government's political and administrative presence in a region. This makes them targets for individuals or group nursing grievances against the government. Hence, the need for effective facility security management (National Research Council, 2002).

### 1.2. Statement of Problem

The research problem of this study is concerned with the absence of a strategic framework for effective security risk management of operations, equipment and personnel in government administrative (secretariat) facilities when under threatening circumstances. This makes such facilities susceptible to infiltration, manipulation and exploitation. Security risk management frameworks available in literature cover nuclear facilities (Vasconcelos, Andrade and Jordao, 2011), energy facilities (Biringer and Danneels, 2000), process plants (Baybutt, 2002) and commercial facilities (Liu, Tan, Fang and Lok, 2012). Peculiarities of government administrative facilities, distinguishes them; in terms of the nature of existing hazards, vulnerabilities and motives of threat perpetrators; from other types of facilities.

Vulnerabilities of these facilities are obvious. However, they are not identified and attended to at times of critical security demands. Facility security structures in government administrative facilities are suited for minor criminal acts such as thefts, with of little or no consequence to the ideal functioning of the facility. They have no clear, coordinated response strategies to threats of peculiar natures and show a clear absence of designed physical security features (Achumba, Ighomereho, and Akpor-Robaro, 2013). These should not be the case because government administrative facilities, house high occupancy buildings. Hence, they are of a high consequence class. These are also important buildings since disruptions to government's ability to plan, analyse and execute its policies could have a detrimental effect on the society's development, economy and security.

### 1.3. Aim and Objectives of the Study

The study aims to develop a framework for the effective security risk management of government administrative facilities in the South-South region of Nigeria, in a view to ensuring the safety of staff and visitors; the security of functions and equipment; and protection of the integrity of the arms of government that own these facilities. To achieve this aim, the objectives are to assess characteristics of government administrative buildings for threat identification and consequences classification; model event scenarios for identified threats on government administrative buildings; and develop a framework for the effective risk management of security threats to government administrative facilities.

## 2. LITERATURE REVIEW

### 2.1. Facility Security Management

Facility security management is the process of identifying, implementing and monitoring systems and processes for the protection of people and building assets against loss, misuse, damage or deprivation of use caused by deliberate acts (Queensland Department of Housing and Public Works, QDHPW, 2012). Facility security refers to the physical security of space and hardware, including access control, and maintenance of records, as well as the process for equipment/inventory control. According to Kozlow and Sullivan (2000), facility security management is the protection, and the measures taken toward the protection of a building or other physical location. Organizations use security management procedures for information classification, threat assessment, risk assessment, and risk analysis to identify threats, categorize assets, and rate system vulnerabilities (QDHPW, 2012). Organization's assets, including people, buildings, machines, systems and information assets are identified; and policies and procedures for protecting them are developed, documented and implemented. Building assets should have adequate security systems and processes in place to protect people, property, operational capability and information.

Cotts, Roper and Payant (2010) stated that it was the responsibility of facility managers to understand and apply the principles of physical security to service support organisations so as to provide adequate advice to organisation's security staff and management. Appropriate countermeasures must be put in place taking into consideration likely hazards, threats and consequences.

## 2.2. Hazards, Threats and Consequences

Adedeji and Eziyi (2010) explained that a hazard is a threat which could cause an accident (alternatively, risk source). However, Newsome (2013) cited that, hazards and threats are sources of negative risk, where for hazards the source is in a harmless state but for threats the source in a harmful state. Vasconcelos, Andrade and Jordao (2011) define threat as an entity with motivation, intention and capability to commit a malicious act. Hazard and threats are facility dependent. National Research Council (1991) and Lundberg and Willis (2015) listed hazards in and around buildings to include: fire, explosion, hazardous substance release (nuclear, biological, chemical), security/crime (breaking/entering, vandalism/malicious mischief, information security), environmental condition: noise (internal and external), pathogens (asbestos, radon, toxic materials, indoor pollutants), nuclear and conventional attack: accident (slip/fall) and others.

Proximity of facilities to sources of hazards increases the likelihood for these hazards to be considered as threats to the facility (Baybut, 2002). Baybut (2002) cited that, threats could be external or internal and that threats could be carried out with internal assistance though originating externally. Conventional threats identified from literature include theft/burglary, robbery, public order incidents, sabotage / mischief, stand-off attack with hand thrown devices, explosive attack with mail or parcel bombs, attack against high profile individuals, placement of improvised explosive devices (IEDs), attack by a vehicle carrying improvised explosive devices (VBIEDs), attack with chemical / biological / radiological agents, armed assailant attack and kidnapping (National Research Council, 1991; Biringer and Danneels, 2000; Teicholz, 2001; Baybutt, 2002; Baybutt and Ready, 2003; Cotts, Roper and Payant, 2010; Liu, Tan, Fang and Lok, 2012; Achumba, Ighomereho, Akpor-Robaro, 2013; Onifade, Imhonopi and Urim, 2013; Lundberg and Willis, 2015; and Grant and Stewart, 2017).

Consequences of threats on facilities could be classified into three major groups: economic, human and environmental consequences. Obodoh, Amade, Obodoh and Igwe (2019) classified consequences of threats to include: financial, socio-political, human related, physical consequences and law/legal consequences. Economic/financial consequences can be described as the consequences associated with money (Janssens et al., 2012; Sandler, 2013; and Lundberg and Willis, 2015). These consequences include: loss of property, loss of annual income/capital investment, loss of materials, loss of investment, clean-up costs, rescue costs, cost of investigation/compensation, treatment of injured people, cost of rebuilding/repair, cost of loss of functionality, cost of replacement/repair of contents, cost of temporary relocation and cost of legal dispute. Socio-political consequences include: loss of reputation, integrity and trust of the host agencies, organisation or government (Obodoh, Amade, Obodoh and Igwe, 2019). Human related consequences are consequences that directly affect human beings or human lives (Grant and Stewart, 2015; Grant and Stewart, 2017; Biringer and Danneels, 2000; Janssens et al., 2012; and Sandler, 2013). They include: loss of lives, injuries, permanent disabilities and psychological trauma.

Environmental consequences of threats on facilities include; provision of hideout for hoodlums, emission of toxic materials to the environment and loss of the benefit of the embodied energy of facility infrastructures due to shortened life cycle (Baybutt, 2002; Janssens et al., 2012; Sandler, 2013; and Lundberg and Willis, 2015). Physical consequences are the consequences of hazards on facilities that are often associated with the physical nature of the building (Grant and Stewart 2015; Grant and Stewart 2017). They include: structural and non-structural damage to the facility, damage to contents, and others. Finally, legal consequences associated with threats on facilities include: death and injury claims, theft and damage claims, legal tussle among stakeholders, among others.

## 2.3. Facility Vulnerability

Vulnerability refers to the propensity of exposed elements such as human beings, their livelihoods, and assets to suffer adverse effects when impacted by hazard events (Cardona, et. al., 2012). It is related to predisposition, susceptibilities, fragilities, weaknesses, deficiencies, or lack of

capacities that favour adverse effects on the exposed elements. Vulnerability is defined to be a combination of the attractiveness of a facility as a target and the level of deterrence and/or defence provided by the existing countermeasures (Ferreira, 2019). Ferreira (2019) defined two interpretations of the concept of vulnerability. The first interpretation saw vulnerability as the probability of the success of an attack, resulting in a certain threat for an infrastructure with certain characteristics. The second interpretation highlighted vulnerability as an infrastructure characteristic, be it physical or procedural, that represents a fragility.

A vulnerability analysis/ assessment, seeks to determine the susceptibility of an infrastructure to attack by an aggressor, or the probability of the success of an attack. The ultimate goal of the vulnerability assessment is to identify the physical characteristics or procedures that makes a particular infrastructure, area, system or event, particularly vulnerable to a range of plausible possibilities of a threat. This makes the vulnerability assessment a vital process for the assessment of risks of threats on facilities.

## 2.4. Risk Management Frameworks

Facility security risk management framework is the first step towards establishing an effective system to safeguard staff and protect facilities. Risk management frameworks should include risk identification, risk measurement, risk control and risk monitoring. Several frameworks exist that provide systematic approaches towards the management of risks associated with the occurrence of threats on facilities.

Baybutt (2002) provided a basis for the assessment of risk for deliberate acts on process plants in the USA. A framework for risk identification, evaluation and decision processes was proposed. This covered risk identification, risk evaluation, risk acceptability, facility modification and operation, as shown in Figure 1.

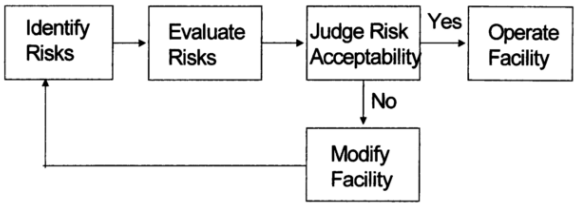


**Figure 1:** The risk identification, evaluation and decision process

Source: Baybutt (2002)

The threat risk matrix presented in Figure 2 was adopted as a means to evaluate the risk. This was carried out using the Relative Risk Measure (RRM). Threat likelihood levels and consequences levels applied in the threat risk matrix were defined and the RRM was also defined using the expression;

$$RRM = \sum_{i=1,m}(R_i \, x \, n_i) \qquad \ldots eqn.1$$

Where, $m$ = highest risk level, $R_i$ = risk value associated with risk level $i$, and $n_i$ = the number of occurrences of the $i^{th}$ risk value.

Threat Severity

| Threat Likelihood | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | Negligible | Very Low | Low | Moderate |
| 2 | Very Low | Low | Moderate | Medium |
| 3 | Low | Moderate | Medium | High |
| 4 | Moderate | Medium | High | Very High |

**Figure 2:** Threat risk matrix

Source: Baybutt (2002)

Vasconcelos, Andrade and Jordao (2011) provided a framework which covered facility security risk management for nuclear and radioactive facilities in Brazil. Risk quantification was based on the generalised relationship;

$$Risk = frequency\ (F) x\ consequences\ (c) \qquad \dots\ eqn.2$$

However, defining the frequency (F) as the product of the initiating event frequency and the probability all safeguards fail, risk associated with occurrence of a threat was further defined as;

$$Risk = [Threats\ (T) x\ Vulnerability\ (V)]\ x\ Consequences\ (c) \qquad \dots\ eqn.3$$

A risk management framework was proposed. This covered the core considerations of risk analysis, risk management, security controls and risk mitigation as summarised in Figure 3.

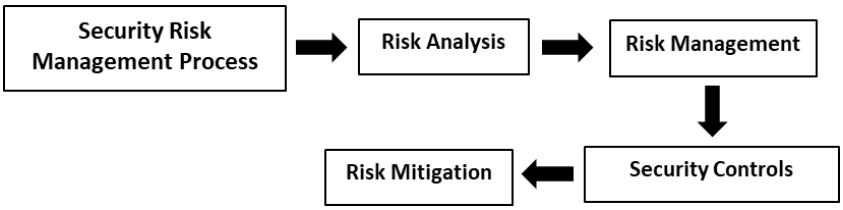


**Figure 3:** Framework for security risk management

Source: Vasconcelos, Andrade and Jordao (2011)

Liu, Tan, Fang and Lok (2012) provided a framework for the physical security risk management of commercial facilities to terrorist acts in Singapore. Risk ratings for each asset and threat pair were obtained using the relationship shown in Equation 4. Using a five-point rating scale, each level of rating was clearly defined.

$$Risk\ rating\ = Threat\ rating\ x\ vulnerability\ rating\ x\ Impact\ rating\ \dots eqn.4$$

Cases covered in literature were related to facilities distinctively different from government administrative facilities. Threats, facility characteristics, vulnerabilities and consequences are all unique to the facilities and the locations the frameworks were designed for. Considerations for government administrative buildings in the South-South region of Nigeria must also be unique to the threats, facility characteristics and consequences in this region. Hence, the essence of this study.

## 3. METHODOLOGY

### 3.1. Research Design, Study Area and Population

This study employed a descriptive survey research design. The descriptive survey is used to systematically and accurately describe the characteristics of a study population. The descriptive research design was used because the study relied majorly on primary data collected through direct observation of sampled facilities. The South-South geo-political zone of Nigeria is the study area as shown in Figure 4. The South-South geopolitical zone consists of Akwa Ibom, Bayelsa, Cross River, Delta, Edo and Rivers states. It is located in the Niger-Delta region of Nigeria, covering a land mass of over 29,100 km and lying between longitude 5.05$^{o}$ E and 7.35$^{o}$ E and latitude 4.15$^{o}$ N and 6.010$^{o}$ N (Adewuyi, Idoro and Ikpo, 2014).

The South-South zone is faced with high underdevelopment, high poverty rate and shortage of basic infrastructure, despite its vast contribution to the national wealth through crude oil extraction. This led to the development of militant groups with grievance to the Federal and State governments occasionally expressed through kidnappings of government and oil facility personnel, bombings and sabotage of oil facilities and other infrastructure (Achumba, Ighomereho, and Akpor-Robaro, 2013; and Onifade, Imhonopi and Urim, 2013).

The population of this study consisted of government administrative facilities (secretariat facilities) in the South-South geo-political zone of Nigeria. These facilities house high consequence class buildings. They represent the presence of the federal and state governments in a region, and they house government administrative arms, agencies, commissions and ministries. A minimum of one secretariat building each for the federal and state ministries exists in each state in the South-South

region of Nigeria and most of these are located in the state capital for ease of interaction with the public and other sister government agencies. This gives a total of twelve (12) facilities from the six South-South states. For this study, the Sample population was taken to be the total population. These comprised of twelve Federal and State government administrative buildings. This was adopted because the size of the population of the study was found to be manageable in terms of time and cost, therefore eliminating the need to sample.

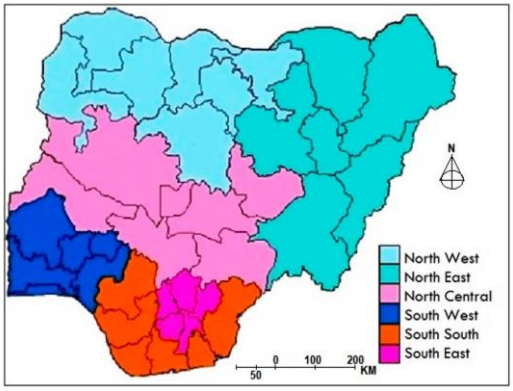


**Figure 4:** South-South Geopolitical Zone

Source: Jetty Image (2021)

## 3.2. Data Collection and Analysis

Two types of instruments were used to collect data for this study. They were secondary data sources and structured direct observation checklists. Data used in this study was qualitative in nature. This was due to the nature of instruments used and difficulty of access to sensitive security data from the facilities and from security agencies in the South-South region of Nigeria.

Letters were forwarded to facility managers to seek their consent for investigation of their facilities. A structured direct observation check-list was prepared. The check-list contained questions which when responded to at the facilities, provided primary qualitative data on the facilities' physical characteristics and features (natural and artificial), personnel details, space planning and general organisation. Management of data obtained took into consideration possible security implications. Therefore, data collected was treated confidentially, during data gathering, processing, analysing and reporting.

The data collected was analysed using descriptive statistics, risk matrices and logic models. Since a five-point Likert scale was adopted for data collection, 5x5 matrices that satisfied the relationship defined in Equation 3 (Vasconcelos, Andrade and Jordao, 2011) was adopted. Risk matrices presented in Figure 5 and Figure 6 below were used in the study.

| Likelihood Threat occurs and Evades Protective Measures | | Facility Vulnerability | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Likelihood of Occurrence of Threats | 1 | Very Low | Very Low | Low | Low | Moderate |
| | 2 | Very Low | Low | Low | Moderate | High |
| | 3 | Low | Low | Moderate | High | High |
| | 4 | Low | Moderate | High | High | Very High |
| | 5 | Moderate | High | High | Very High | Very High |

**Figure 5:** Risk Matrix: Likelihood threat occurs and evades protective measures in the facility

| Risk Measure Associated with Occurrence of Threat | | Consequences | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| Likelihood threat occurs and evades protective measures | 1 | Very Low | Very Low | Low | Low | Moderate |
| | 2 | Very Low | Low | Low | Moderate | High |
| | 3 | Low | Low | Moderate | High | High |
| | 4 | Low | Moderate | High | High | Very High |
| | 5 | Moderate | High | High | Very High | Very High |

**Figure 6:** Risk Matrix: Risk Measure Associated with Occurrence of Threat in the facility

# 4. PRESENTATION AND DISCUSSION OF RESULTS

## 4.1. Facilities Characteristics

Twelve facilities were considered in this study. Facilities assessed were federal and state administrative (secretariat) facilities in the South-South region of Nigeria. Data obtained through direct observation of these facilities are as shown in Table 1. Facilities were labelled AA, AB, BA, CA, CB, DA, DB, EA, EB, FA and FB. The first letter represented the state the facility was located in and the second letter represented the arm of government that owned the facility. Facility labelling was adopted in this study for security and safety reasons. Table 1 shows that number of buildings in these facilities range between 1 and 15. Facility square areas ranged between 2000 $m^2$ and 297000 $m^2$. Of the twelve facilities, facility CB was found to have a building with the largest floor area (14000 $m^2$) but facility BB had the highest number of storeys (18). The average population of staff, and visitors in these facilities during peak periods ranged from 300 in facility DB to 1500 in facilities AB and BB. Figures 7, a and b, show drone photos of facilities AA and AB taken during direct observation of the facilities.

(a)  (b) 

**Figure 7:** Aerial drone photographs of (a) Facility AA (b) Facility AB

All twelve facilities were fenced, with gates and the visible presence of armed security personnel belonging to public security outfits. Facilities were located at accessible locations, in developed districts of state capitals. Physical protective measures adopted within facilities were designed primarily for access control of people and vehicle speed control. No hazardous or highly flammable materials depots were seen at these facilities except for small diesel storages facilities. Diesel stored were for power generators which severed as back up to intermittent and unreliable public power supply. It was observed that security components and personnel activities were designed with emphasis on the security of the main buildings and their primary accesses. Buildings were of reinforced concrete frames with walls made of concrete blocks. Windows were made of glass with steel burglary proofs. CCTV, electronic card locks and other CPTED components were not readily adopted in these facilities. Parts of buildings with high population or critical structural elements were unprotected. Access to these parts of buildings was easily available to visitors and vehicles. Where offsite parking or parking was provided with sufficient safe distance from critical parts of the facilities, vehicle access controls were not enforced.

Facilities characteristics show that most federal and state secretariate facilities in the South-South region of Nigeria posse buildings with floor area approximately 2000 $m^2$ or greater. These categorises them into the 2b upper risk group or high-risk group (group 3) of the Eurocode 1-7 (CEN, 2014), based on consequences of localised failure from unspecified causes. Therefore, a greater level of protection is required for buildings in these facilities.

**Table 1:** Facilities Characteristics

| Facility Designation | Number of Buildings | Area of Facility ($m^2$) | Area of largest Building ($m^2$) | Number of Storeys | Average Population |
|---|---|---|---|---|---|
| AA | 1 | 57500 | 4200 | 3 | 800 |
| AB | 13 | 297000 | 1500 | 3 | 1500 |
| BA | 1 | 24700 | 1800 | 8 | 900 |
| BB | 15 | 2000 | 3500 | 18 | 1500 |
| CA | 1 | 34000 | 4500 | 3 | 800 |
| CB | 3 | 104000 | 14000 | 5 | 1400 |
| DA | 1 | 27000 | 4200 | 4 | 800 |
| DB | 8 | 62370 | 750 | 2 | 300 |
| EA | 1 | 34500 | 4200 | 4 | 800 |
| EB | 7 | 48000 | 2000 | 9 | 1400 |
| FA | 2 | 35000 | 6400 | 3 | 800 |
| FB | 12 | 150,000 | 4000 | 3 | 1000 |

## 4.2. Logic Modelling of Event Scenarios

Logic modelling of event scenarios was carried out using the Event Tree Analysis. After a careful analysis of possible event scenarios for all threats identified, the model shown in Figure 8 was found to cover all possible scenarios. Threats could be of external or internal sources. Where external initiators work with internal collaborators, mitigating measures could be easily neutralized. Threats of this nature could be classified as external if internal collaborators lack the capacity to completely execute planned acts on their own. Likelihood of failure of mitigating measures could be analysed to greater details using the Fault Tree Analysis technique. This is important as it provides detailed information on vulnerabilities measures within the facility.

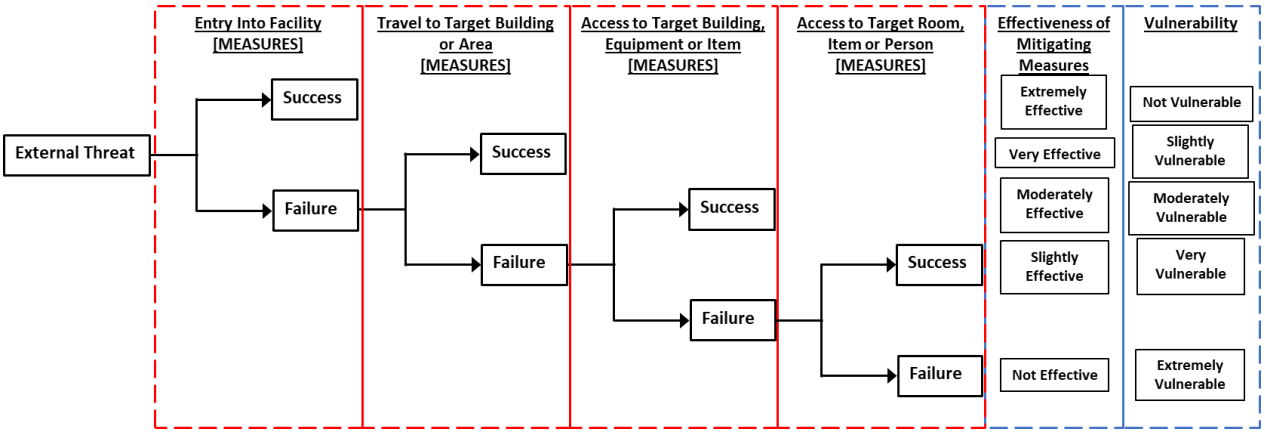


**Figure 8:** Event Tree Model for scenario identification and logic modelling for threats occurrence in government administrative facilities

Success or failure associated with each event in Figure 8 refers to the effectiveness of mitigating measures against the threat considered. The inability of mitigating measures to successfully terminate the threat before the perpetuators accomplish their objective shows the general ineffectiveness of existing measures and vulnerability of the facility. Relationship between effectiveness of mitigating measures against threats and vulnerability of the facility has been defined by Biringer and Danneels, (2000) as shown in Equation 5, where $P_V$ is the probability that security system is not effective against the attack (that is the probability that the facility is vulnerable) and $P_E$ is the probability that security system is effective against attack.

$$P_V = 1 - P_E \qquad \ldots eqn. 5$$

## 4.3. Proposed Facility Security Risk Management Framework

A framework was developed based on established relationships between security risk management components. The framework developed is novel and customized to suit the uniqueness of threats and organizational management methods observed in government administrative facilities in the South-South region of Nigeria. This framework is as shown in Figure 9. The framework presented is simple enough to be applied by Managerial Decision Makers within these facilities, with only little training needed. It covers varying national or state threat levels. In addition, it is applicable to different threats and takes into consideration scenarios which are unique to prevailing circumstances. Existing risk mitigation measures are also taken into account. This makes the framework adaptable to changing threat level, threat nature, and facility characteristics.

The framework commences with the analysis of threats. Threats are identified and their likelihood estimated based on the National/State state of alert, existence of threat, capability of the perpetuators, their interest in the facility and intelligence report on perpetuators targeting the facility. This was as adopted in Biringer and Danneels (2000). Scenario Logic Modelling is then carried out using the Event Tree Modelling technique after an assessment of the characteristics of the facility. A vulnerability analysis is carried out taking into consideration Scenario logic Models, existing mitigating measures and their likelihood of failure (or effectiveness). The risk measure is estimated using risk matrices presented in Figures 5 and 6. If the risk measure obtained is not acceptable for a particular threat, existing mitigating measures could be optimized or additional mitigating measures introduced based on the findings of the vulnerability analysis. The process is iterated until the risk measure is acceptable and integrated to the facility risk management framework. Where mitigating measures required are not feasible, risk acceptability levels could be made As Low As Reasonably Possible (ALARP) and integrated into the risk framework.

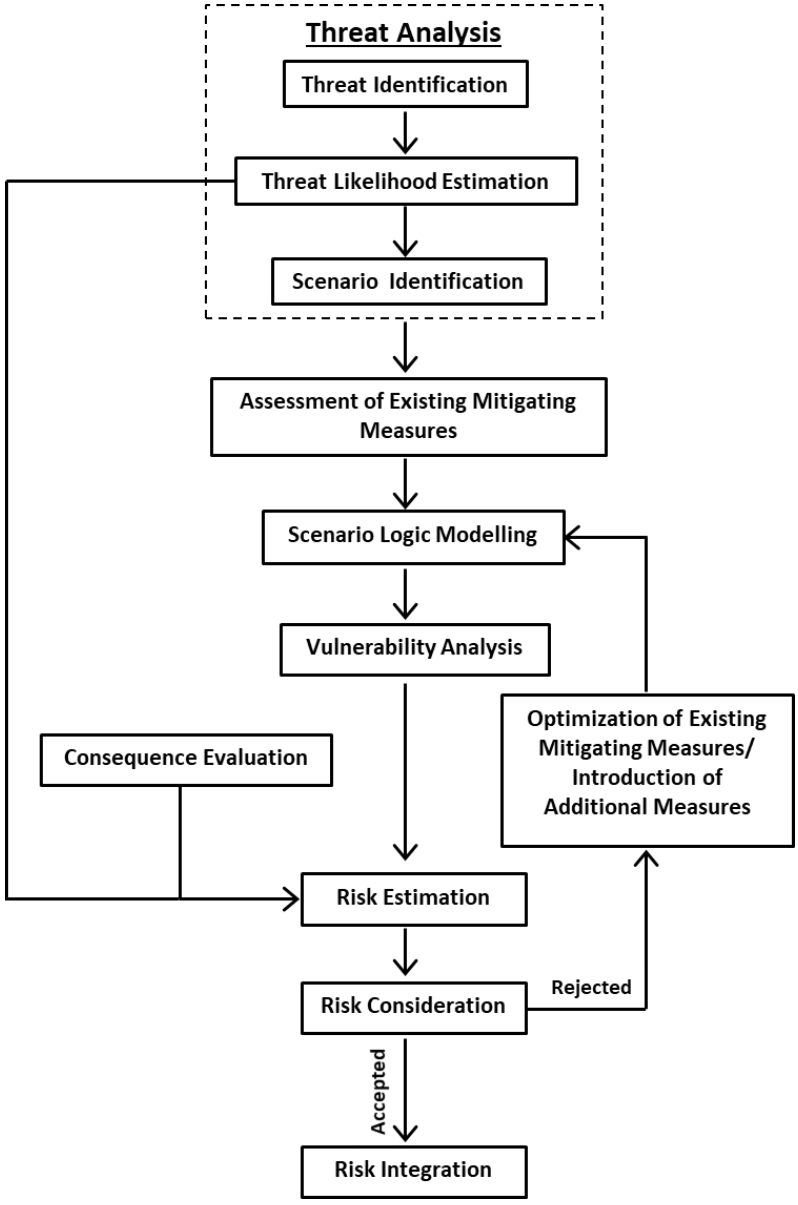


**Figure 9:** Facility security risk management framework

## 4.4. Application of Proposed Facility Risk Management Framework

The proposed facility risk management framework was applied to the twelve government administrative facilities in the six states of the South-South region of Nigeria. At the time of observing the facilities, the Heightened State of Alert in the states of the region had been downgraded to a level equivalent to two, on a five-point scale. Three threats with the most likelihood of occurrence, as determined in Chiama (2023), were considered. These were kidnapping (KID), public order incident (POI) and armed assailant attacks (AAA). Result of application of this framework is as shown in Table 2.

**Table 2:** Result of application of proposed framework to case study facilities

| Facility | Likelihood | | | Vulnerability | | | Consequence | | | Risk measure | | | Risk consideration * | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | KID | POI | AAA | KID | POI | AAA | KID | POI | AAA | KID | POI | AAA | KID | POI | AAA |
| AA | 3 | 2 | 1 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | A | A | A |
| AB | 3 | 3 | 2 | 2 | 3 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | A | A | A |
| BA | 3 | 3 | 1 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | A | A | A |
| BB | 3 | 3 | 3 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | A | A | A |
| CA | 3 | 3 | 3 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | A | A | A |
| CB | 3 | 3 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | A | A | A |
| DA | 3 | 2 | 3 | 3 | 3 | 1 | 2 | 3 | 2 | 2 | 3 | 2 | A | M | A |
| DB | 3 | 3 | 1 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | A | A | A |
| EA | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | A | A | A |
| EB | 3 | 3 | 2 | 3 | 3 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | A | A | A |
| FA | 3 | 3 | 3 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | A | A | A |
| FB | 3 | 3 | 2 | 3 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | M | A | A |

**A Risk Acceptability Limit of 2 (Low) was adopted; A = Accept; M = Mitigate.*

A risk acceptability limit of two (2) was adopted in the evaluation. The three threats considered were found equal to or below the acceptability levels except for public order incidents and kidnappings in facilities DA and FB respectively. Therefore, while risk measures for other threats in the twelve facilities were acceptable, additional measures were needed for public order disturbances and kidnaping in facilities DA and FB respectively, otherwise these Risks were made ALARP and integrated.

Public order incidents involve unarmed crowds, whose number could overwhelm security personnel and pull-down gates, wall and doors. The use of armed personnel against such a threat is inappropriate (Sampson, 2010). However, facilities are not equipped with the non-lethal resources needed to effectively manage such a threat. This could explain the moderate vulnerability rating of facilities to this threat.

Asides cases of facilities DA and FB located in states with known reputation for kidnapping and other armed militant activities, risk measures evaluated were reflective of the prevailing level of heightened state of alert, at the time of observation. This implies that increases in any of the components of threat likelihood, due to political, social, religious or economic issue, would have significant impacts on the risk measure and risk consideration as noted in Biringer and Danneels (2000). Therefore, regular assessments are important to keep management and staff informed on the prevailing facility and organisation risk rating.

## 5. CONCLUSIONS AND RECOMMENDATIONS

A framework for the effective risk management of security threats to government administrative facilities was developed which satisfied the requirements of the objectives of the study. The applicability of this framework was shown in case studies involving the three most likely threats on government administrative buildings identified in literature. Results showed that risk measures for these threats were acceptable except for the case of public order disturbance in facility DA and kidnapping in facility FB, where the risk measures were found unacceptable, with a risk acceptable limit of "Low".

Therefore, it is concluded that:

- risk associated with identified threats in government administrative facilities varies as factors affecting risk components are constantly changing, hence a dynamic strategy for measuring risk is needed in government administrative facilities;
- an effective facility security risk management framework is needed to ensure safety and security in government administrative facilities; and
- the framework proposed in this study is quite capable of meeting this need.

On the premise of the conclusions above, the study proposes the following recommendations.

- All departments and agencies housed in government administrative facilities should be assigned responsibilities towards their integration into the facilities security risk management framework. All staff should be trained on their responsibilities towards safety and security of themselves, their equipment, their areas of operations (physical or cyber), their visitors and their clients.
- Regular risk assessments should be carried out on these facilities. Frameworks adopted should incorporate factors influencing risk components. Measured risks should be compared against benchmarks with definitions acceptable to the stakeholders. Risk measures and acceptability limits should be communicated to units, departments and agencies housing the facilities.

## 6. LIMITATION OF THE STUDY

Threats considered are limited to those that are malevolent. Threats considered are also of a "low probability and high consequence" nature. Since such threats may be constituted of smaller acts such as theft, vandalism and sabotage, these smaller acts were considered in view of their primary motives.

Government administrative facilities considered were federal and state civil service administrative facilities also referred to as secretariat facilities. Where several facilities exist in any state within the study area, the primary facility was adopted.

## REFERENCES

Achumba, I., Ighomereho, O., and Akpor-Robaro, M., (2013). Security challenges in Nigeria and the implications for business activities and sustainable development. *Journal of Economics and Sustainable Development*, 4(2), pp. 79-99.

Adedeji D. and Eziyi O. I., (2010): Urban Environmental Problems in Nigeria: Implications for Sustainable Development, *Journal of Sustainable Development in Africa;* 12(1):124-145.

Adewuyi, T., Idoro, G. and Ikpo, I. (2014). Empirical evaluation of construction material waste generated on sites in Nigeria. *Civil Engineering Dimension*, 16(2).

Agwu, P., Onwujekwe, O., Uzochukwu, B., and Mulenga, M. (2021). Improving service delivery at primary healthcare facilities for achieving Universal Health coverage: Examining the effects of insecurity in such facilities in Enugu State, Nigeria. *South Eastern European Journal of Public Health (SEEJPH)*, 2021(2):1-10. doi: 10.11576/seejph-4319.

Associated Press in Boston (2013, September 25). Boston Marathon hit by double explosion. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/apr/15/two explosions - boston-maraton.

Baybutt, P. (2002). Assessing risks from threats to process plants: Threats and vulnerability analysis. *Process Safety Progress*, 21(4), 263-275.

Baybutt, P. and Ready, V. (2003). Strategies for protecting process plants against terrorism, sabotage and other criminal acts. *Homeland Defence Journal*, 2(1).

Biringer, B., and Danneels, J. J. (2000). Risk assessment methodology for protecting our critical physical infrastructures. Report SAND2000-3119C of the Sandia Corporation, Lockheed Martin Company for the United States Department of Energy, Albuquerque, United States of America.

Byfield, M., Mudalige, W., Morison, C. and Stoddart, E. (2014). A review of progressive collapse research and regulations. *Proceedings of the Institution of Civil Engineers – Structures and buildings*, 167 (8), 447-456.

Cardona, O.D., M.K. van Aalst, J. Birkmann, M. Fordham, G. McGregor, R. Perez, R.S. Pulwarty, E.L.F. Schipper, and B.T. Sinh, 2012: Determinants of risk: exposure and vulnerability. In: Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation [Field, C.B., V. Barros, T.F. Stocker, D. Qin, D.J. Dokken, K.L. Ebi, M.D. Mastrandrea, K.J. Mach, G.-K. Plattner, S.K. Allen, M. Tignor, and P.M. Midgley (eds.)]. A Special Report of Working Groups I and II of the Intergovernmental Panel on Climate Change (IPCC). Cambridge University Press, Cambridge, UK, and New York, NY, USA, pp. 65-108.

CEN. (2014). Eurocode 1: Actions on structures (BS EN 1991-1-7:2006 +A1:2014). https://doi.org/ISBN 978 0 580 83725 8

Chiama, K.F. (2023). Risk management of threats on government administrative facilities in South-South, Nigeria. MSc. Dissertation, Department of Building, Faculty of Environmental Studies, University of Uyo, Nigeria.

Clarke, R. V. (1992). *Situational Crime Prevention: Successful Case Studies* (2nd ed.). New York, USA: Harrow and Heston.

Clarke, R. V. (1995). "Situational Crime Prevention". In M. Tonry and D. P. Farrington (Eds.), *Building a safer society: strategic approaches to crime prevention* (Vol. 19, pp. 127-141). Chicago, USA: The University of Chicago press.

Cotts, Roper and Payant, (2010). *The Facilities Management Handbook* (3rd ed.). New York, USA: The American Management Association.

Ferreira, A. (2019). Vulnerability analysis in critical infrastructures: A methodology. *Security defence quarterly*, 24(2), 65-84. https://doi.org/10.35467/sdq/108665

Grant, M. J. and Stewart, M. G. (2015). Probabilistic risk assessment for improvised explosive device attacks that cause significant building damage. *Journal of performance of constructed facilities*, 29 (5), 1– 9.

Grant, M. J. and Stewart, M. G. (2017). Modelling improvised explosive device attacks in the west – assessing the hazard. *Reliability engineering and system safety*, 165 (1), 345-354.

Janssens, V., Dermot, W.O. and Chryssanthoupoulos, M. K. (2012). Assessing the consequences of building failures. Structural Engineering International, 22 (1), 99-104.

Kozlow, C. and Sullivan, J. (2000). Jane's Facility Security Handbook. Alexandria, Virginia, USA: Jane's Information Group.

Liu, C., Tan, C., Fang, Y. and Lok, T. (2012). The security risk assessment methodology. *Safety science and engineering in China, Volume 43*. Proceeding of the International Symposium on Safety Science and Engineering in China (pp. 600-609), Beijing, China. Procedia Engineering, Elsevier Procedia.

Lundberg, R. and Willis, H. (2015). Assessing homeland security risks: A comparative risk assessment of 10 hazards. Homeland security affairs, 11 (10), 1-24.

National Research Council (1991). Uses of risk analysis to achieve balanced safety in building design and operations. Washington D.C. The National Academic Press.

National Research Council (2002). Making the Nation Safer: The role of science and technology in countering terrorism. Report of the National Research Council, The National Academies Press, Washington, D.C. https://doi.org/10.17226/10415.

Ndubuisi-Okolo P., and Anigbuogu T., (2019). Insecurity in Nigeria: the implications for industrialization and sustainable development. *International Journal of Research in Business Studies and Management*, 6(4), 7-16. https://www.ijrbsm.org/papers/v6-i5/2.pdf

Newsom C. (2011). Conflict in the Niger Delta: More than a local affair. Special Report of the US Institute of Peace. http://www.jstor.org/stable/resrep12205.

Newsome B. (2013). *A practical introduction to security and risk management* (1st ed.). London, UK: SAGE publications.

Obodoh, D., Amade, B., Obodoh, C. and Igwe, C. (2019). Assessment of the effects of building collapse risks on the stakeholders in the Nigerian built environment. *Nigerian Journal of Technology, NIJOTECH*, 38 (4), 822-831.

Onifade, C. and Imhonopi, D., and Urim, U. (2013). Addressing the insecurity challenge in Nigeria: the imperative of moral values and virtue ethics. *Global Journal of Human and Social Science*, 13(2), 53-63. https://core.ac.uk/download/pdf/16701001

Queensland Department of Housing and Public Works, (2012). Security management of government buildings. Report of the Queensland Department of Housing and Public Works, Queensland Government, Brisbane, Australia.

Sampson, I. T. (2010). The right to demonstrate in a democracy: An evaluation of public order policing in Nigeria. *African Human Rights Law Journal*, 2(1), 432-456.

Sandler, T., (2014). The analytical study of terrorism: Taking stock. *Journal of Peace Research*, Volume 51 (2), 257-271. DOI: 10.1177/0022343313491277

Teicholz E., (2001). Facility Design and Management Handbook. New York: McGraw-Hill.

Ukpong C. (2020, October 22). #EndSARS: Hoodlums set fire on TV station in Akwa Ibom. Premium Times News. https://www.premiumtimesng.com /regional/ south-south-regional/422560-endsars-hoodlums-set-fire-on-tv-station-in-akwa-ibom.html.

Ulaeto, N. W., Sagaseta, J. A and Chyssanthopoulos, M. (2022). Horizontal Collapse Propagation of Concrete Flat Slabs Supported on Columns. Journal of Structural Engineering, American Society of Civil Engineers (ASCE), 148(2), DOI: 10.1061/(ASCE)ST.1943-541X.0003245.

Vasconcelos, V., Andrade, M. C. and Jordao, E., (2011). Use of risk assessment methods for security design and analysis of nuclear and radioactive facilities. Proceedings of the International Nuclear Atlantic Conference, INAC, Belo Horizonte, MG, Brazil, October 24-28. ISBN: 978-85-99141-04-5