ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

Level of Implementation of Security Protocols and Clients' Satisfaction on Physical Security in an Establishment Towards Enhanced Safety Regulations

Alexander T. Gendoma[1]

[1]Emilio Aguinaldo College Manila, Philippines

Publication Date: 2025/12/19

Abstract: Various challenges have been identified when it comes to the physical security practices being implemented in the area. In terms of access control, the main issue comes in dealing the people, including employees, who are trying to access important systems or information without permission. On the other hand, when it comes to security assessment, the main problem is keeping up with online threats that constantly change from time to time.

This study evaluates physical security practices, focusing on access control, security assessment, and surveillance, to determine their effectiveness in ensuring safety. The findings reveal high overall satisfaction with security measures, scoring an average, particularly for identification protocols and ID management. Security assessment practices also received a lower rating of underscoring the need for enhancement.

The demographic profile of respondents shows a predominantly young workforce, with most aged 25-34 and a balanced gender distribution. The majority of respondents have significant work experience, while educational levels vary, with a notable proportion having some college education. This suggests a generally experienced and diverse workforce.

Clients report high satisfaction with security measures, especially advanced locks, effective lighting, and video surveillance. Nevertheless, improvements are needed in entrance point security and perimeter surveillance. The study finds no significant impact of age, gender, length of service, or education on security practices, indicating uniform training and organizational culture as evidenced by the non-significant differences.

To address the identified issues, an action plan is developed based on best practices. This plan includes recommendations for enhancing training programs, upgrading access control systems, implementing regular security audits, and improving communication channels for feedback. This structured approach aims to refine security practices and ensure continuous improvement in response to evolving security challenges.

Lastly, for the surveillance and monitoring aspects, maintaining protection and privacy is still one of the main concerns as it involves protecting everyone's privacy. Adopting a comprehensive security approach is recommended based on the indicated issues in physical security practice.

Keywords: *Client Satisfaction, Physical Security, Model of Best Practice.*

How to Cite: Alexander T. Gendoma (2025) Level of Implementation of Security Protocols and Clients' Satisfaction on Physical Security in an Establishment Towards Enhanced Safety Regulations. *International Journal of Innovative Science and Research Technology*, 10(12), 953-981. https://doi.org/10.38124/ijisrt/25dec461

I. INTRODUCTION

Security is more crucial now than it has ever been in this modern, fast-paced society. It is currently one of the sectors with the fastest growth rates. On the news, one almost always hears about harm or loss brought on by security lapses or a lack of security. Physical security is no longer the exclusive meaning of the word "security" in modern times. It contains invisible but incredibly valuable items like electronic data, sometimes known as e-data, such as credit card information or official documents (Maxsenti, 2021; Ralph, 2021).

One cannot stress how important security guards are in today's society. These committed individuals provide security

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

at a variety of venues, including workplaces, institutions of higher learning, banks, and other crucial buildings. However, they also serve to protect people from harm in addition to securing places (CorpSecurity Team, 2021; Security Hire Melbourne, 2023). Celebrities and other high-profile people frequently hire bodyguards or a security guard business to protect them from harm. At events, security personnel use their obvious presence to ward off any potential threats. Additionally, they control crowds and stop unauthorized people from entering restricted areas. Additionally, they can help attendees in case of emergencies like medical problems or evacuations. These physical security measures are crucial in a corporation since it is the duty of a company to preserve not only its workers but also its precious assets and confidential information from any kind of theft, loss, or damage. Effective and dependable workplace security is crucial for any company because it lowers the amount of insurance, benefits, liabilities, and other costs that the firm have to reimburse to its stakeholders. This, in turn, increases corporate income and lowers operational costs (Fernando, 2022).

While the organizations that look after social infrastructure have benefited much from the development and widespread use of information and communication technology, they now confront fresh dangers. In recent years, there has been a growing tendency toward the group-wide consolidation of system administration for reasons of corporate group governance, with an increase in the adoption of measures that safeguard the safety of organizations. Making security measures necessary for both the physical and digital worlds of modern corporate administration (Hamamoto, 2022; Proag, 2020). Organizations have good reason to prioritize physical security. Numerous incidents of inadequate physical security controls in organizations have resulted in theft, information leaks, or, in the worst cases, grave injuries and fatalities (Deloitte, 2022; Security, 2022). If the media learns about a security incident, they frequently make headlines. Stakeholders will be more worried about why controls were not implemented to protect assets, people, and information, regardless of the incident's type. To some extent, physical security has always been taken into account. Why should investing in it be a top priority right now? Making sure the controls that have been in place for a long time are still effective is involved. Physical security management is frequently outsourced or overshadowed by other hazards (Hawkins & Dhami, 2023).

Physical security is the protection of personnel, software, networks, hardware, and data from physical actions and events that could cause serious damage (Sanghavi, 2022). It includes measures such as security guards, surveillance cameras, padlocked or keyed entry tools, and more. It should be considered a primary protection measure of an effective cyber security strategy (Wheelhouse IT, 2022). Security is a combination of technical, administrative, and physical security, but physical security has received little attention due to the focus on online threats (Al-Fedaghi & Alsumait, 2019).

Organizations have good reason to prioritize physical security. Numerous incidents of inadequate physical security controls in organizations have resulted in theft, information leaks, or, in the worst cases, grave injuries and fatalities. If the media learns about a security incident, they frequently make headlines. Stakeholders will be more worried about why controls were not implemented to protect assets, people, and information, regardless of the incident's type. To some extent, physical security has always been taken into account. Why should investing in it be a top priority right now? Making sure the controls that have been in place for a long time are still effective is involved. Physical security management is frequently outsourced or overshadowed by other hazards. Attackers must be present physically to take advantage of physical weaknesses in physical security, such as cutting fiber-optic cables, stealing data servers, and stealing communication equipment. Agents can be responsible for reported security violations and unauthorized use of physical access to systems that get past defenses (Egnyte, 2021; LeTellier, 2019; Resolver, 2018).

The ISO code outlines information security best practices, including risk treatment and assessment, asset management, personnel security, perimeters and barriers, and secure zones to resist natural disasters (Shaikh, 2018). Lack of proper physical security in a corporation can lead to various disastrous outcomes, such as data leakage, corruption, and natural disasters. Physical security measures are essential to protect a corporation's most valuable assets, such as data, equipment, facilities, and employees (Maxsenti, 2021).

In the study done by Steiner, et.al entitled Challenges in Implementing Physical Security Measures in K-12 Schools. The authors discovered that local educational organizations are frequently hindered by a lack of resources (e.g., equipment, manpower), pressure from families and the community, and a lack of knowledge regarding best practices for physical security. There aren't many K–12-specific risk evaluations to help LEAs choose and implement different physical security measures, and data on the efficacy of such solutions is, at best, limited (Steiner, et al, 2021).

Information Security Analysis on Physical Security in University X Using Maturity Model is the title of a paper by Isnaini & Solikhatin. The operations led by the Department of Information Technology and Computer Laboratory at University X are regarded as already conforming to the standard operating procedure in order to achieve the desired result. However, in other circumstances, user awareness of physical security is proven to be insufficient. And the results of the maturity level test in 2,9 support that. Additionally, because the Disaster Recovery Plan hasn't been set up in the framework of Standard Operating Procedures, incidents and risk management have been challenging to handle effectively. To close the gap, information security management in the physical security industry must increase staff capability. This section is crucial for the best possible observance of the established policy by all University X constituents (Isnaini & Solikhatin, 2020).

In another study entitled Towards a Conceptual Foundation for Physical Security: Case study of an IT

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

department. Through the development of a logical description using a flow-based model based on the idea that a security system is a machine, this work has provided a theoretical basis for physical security. The logical flow model is a general approach with a range of potential applications. The findings suggest that a systematic foundation for descriptions of a security process can be provided by the FM (Flow Machine) diagrammatic methodology. Applying the suggested depiction to the security plan of an actual government ministry's IT division serves to illustrate it. As a tool for modeling assaults, a security strategy, and as a predesign schematic specification, the results appear promising. It appears appropriate for planning and training in security as well (Al-Fedaghi & Alsumait, 2019).

David Hutter research entitled Physical Security and Why it is Important demonstrates how correctly implemented administrative, technical, and physical controls enable the management and protection of resources for the firm. In order to provide numerous layers of defense in the event that a control is circumvented, these controls should employ the defense in depth strategy. Security methods aid in preventing, denying, detecting, and then postponing attacks on resource acquisition. Site location, facility design and construction, emergency response, and staff controls are examples of administrative controls. Security perimeters, motion detectors, and incursion alarms are examples of physical controls. Smart cards for access control, intrusion detection systems for physical security, security guards, and CCTV systems are examples of technical controls.

The most important asset that physical security is tasked with protecting is the workforce. Basic facility requirements including food, water, energy, and climate control must always be accessible in order to do this. Security of the facilities should always come second to ensuring the safety of the employees. Disaster recovery teams that have been trained should be ready for extreme conditions, such as natural catastrophes. To reduce casualties in these situations, tenant emergency plans should be followed. Business continuity planning and disaster recovery planning can restore business and IT functionality once human life has been secured (Hutter, 2021).

The Evolution of Physical Security Measures: assessing the benefits and implications of using more advances technologies found out that according to their research, security technologies have made some significant positive strides. The majority of security experts concurred that such measures are increasingly prevalent and that they can have a number of benefits. Surprisingly, despite the fact that criminals were aware of the threat posed by technologies, particularly those with advances they were unaware of or could not have predicted, it was people and the higher risk of immediate suspicion they posed that offender valued the most (Gill, et al, 2019).

In another study by Litche, Witte, Termin and Wolf entitled Representing Uncertainty in Physical Security Risk Assessment. According to their paper, society and the scientific community are increasingly recognizing the value of (physical) security. Numerous security assessments of crucial infrastructures are carried out in practice as a result of the rising terrorist threat levels, and academics are constantly putting forth new ideas. While most recently proposed approaches are based on quantitative criteria, practical security risk assessments (SRA) primarily employ qualitative methods. Both qualitative and quantitative techniques struggle with the core issue of inherent uncertainty regarding threats and the capabilities of security measures as a result of ambiguous data or the use of expert knowledge because there is limited proof of real attacks.

To reflect the knowledge about the performance of security measures that is currently accessible, such uncertainties may be represented by, for example, probability distributions in quantitative analysis. This essay focuses on how these uncertainties affect security evaluation and how to take them into account when designing systems. By contrasting the outcomes of an evaluation using distributed input values with a scalar evaluation that does not account for uncertainty, we demonstrate this influence. We further demonstrate that specific security system barriers are the focus of the influence. By performing a quantitative vulnerability assessment as part of the SRA process using an airport structure example, we specifically discuss the robustness of the system. On the basis of these findings, we suggest the idea of a security buffer. This idea reduces the impact of these uncertainties on the actual system performance while accounting for the uncertain knowledge of the input parameters during the design of the security system. By using it on the airport structure's initially determined design, we demonstrate how this approach may be applied for vulnerability evaluation. The case study's findings confirm our presumptions that the security margin can aid in targeted uncertainty consideration and decrease system vulnerability (Lichte, et al, 2021).

Another local study was done by Mabanglo entitled Campus Security Practices" Assessment of Philippine College of Science and Technology. The result in the study shows that campus security in PhilCST is fully implemented, that campus security measures are used along with physical security, document security, and personnel security, and that there is a difference in the perceived level of implementation and campus security measures along the three main areas of security in PhilCST. Finally, the administrators, faculty members, staffs, students, and visitors of PhilCST have different views on the application of campus security and have different experiences and familiarity with the campus security measures adopted by PhilCST. The conclusion reached was that PhilCST is protected and that everyone who works, studies, or visits the campus feels security assurance (Mabanglo, 2020).

The Level of Physical Security, the five security system tiers: Deterrence, Detection, Delay, Response and Recovery.

The five security system tiers are the following: 1. Deterrence. The objective of deterrence is to discourage potential threats or unauthorized access. This can be done through the use of the following: visible security personnel or patrols, security signage (e.g., "CCTV in operation"),

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

fences, gates, and barriers and lighting in and around the premises. 2. Detection. The objective is to identify and monitor unauthorized access or suspicious activity. The measures to do this is through the following: security cameras (CCTV), motion detectors, intrusion detection systems (alarms) and glass break sensors. 3. Delay. The objective is to slow down intruders to provide time for response. Measures to do this are the following: secure locks and deadbolts, reinforced doors and windows, security grilles or bars and access control systems (e.g., key cards, biometric scanners). 4. Response. The objective is to respond to security breaches promptly and effectively. Measures to achieve this are the following: security personnel or guards, law enforcement coordination, alarm monitoring services and emergency response plans and drills. 5. Recovery. The objective is to restore normal operations and mitigate damage after a security breach. Measures includes backup systems and data recovery plans, incident investigation and reporting, insurance coverage and repair and restoration of damaged assets.

Effective physical security requires a comprehensive and layered approach to address a wide range of threats and protect valuable assets. A system of this kind that is intended to obstruct, discover and evaluate the majority of unlawful external and internal activity is known as high-level security. High-level security is achieved once the previously specified precautions have been added to the system, along with the installation of cutting-edge machinery and security surveillance systems (CCTV) with digital, cutting-edge components. High-security lighting (LED); Highly trained armed security officers or unarmed security officers who have been screened for employment (background checks and drug tests) and who are equipped with cutting-edge means of communication, such as dedicated cell phones, two-way radio links to police, and duress alarms. A perimeter alarm system that is remotely monitored at or near the high-security physical barriers. Controls such as biometrics and/or access control are meant to limit access to or inside a facility to authorized personnel. Plans were formally created with the assistance of the police and with their knowledge that dealt with their response to and assistance in the case of various situations at the protected site. Different levels of cooperation with the local law enforcement agencies. Annual evaluations or security audits are carried out. Monthly system checks are performed.

In order to prevent, identify, evaluate, and neutralize all unlawful external and internal activities, maximum security is implemented. It is distinguished by the following features in addition to those already mentioned: a sophisticated, cutting-edge alarm system that is too powerful to be defeated by a single person, remote monitoring in one or more protected locations, tamper indicating with a backup source of power, access control, and biometrics (Hyperproof, 2022; Mishra, 2023). Dedicated to neutralizing or containing any danger against the protected facility until the arrival of off-site assistance, the on-site response team consists of highly qualified, screened, and trained individuals who are armed 24 hours a day. They are also outfitted for contingency operations (Fay & Patterson, 2018; RiskOptics, 2023).

A widely used branch of science known as "risk theory" focuses on the detection of threats, the definition of risks, and the formulation of risk management strategies. The presence of threats in the real world is what defines risk. The risk arises from either consciously regulated behavior or erratic, uncontrolled behavior on the part of each component of a complex. Moments when the elements are interacting directly, whether on purpose or by accident, can occur in the behavior of elements (collision, impact).

Numerous interactions have detrimental effects and are unfavorable. This impact is proportional to the magnitude and direction of the action (measure), where the individual reference objects are involved in negative interactions. This unpleasant interaction is dubbed a “security incident”. The risk theory is applied to determine which threats (or harmful actions) are directed at the reference object and which ones have a greater or lesser impact (EC-Council, 2022; Villanueva, 2022). The goal of risk identification is to identify the worst possible impact of threats and prepare ways to prevent these dangers. Threats should not be allowed to materialize or have a detrimental influence on the reference item as a result of the suggested measures (Nizhebetskyi, 2023; Woods, 2019).

According to the seventh postulate of the safety and security theory, the various forms of safety or security that have been studied and approved by society are what guarantee safety and security. This postulate aims to identify the many forms of security, as well as their fundamentals and traits. Each type of safety and security employs particular techniques to guarantee safety and security concerns. The models for assuring safety or security can be used to generalize and characterize these techniques.

The modeling process is one way to investigate reality. The goal of modeling is to evaluate reality's behavior through the model and comprehend its fundamental nature. In this book, "safety and security models" are meant to be conceptual models that, through the use of language and imagery, convey the essence of ensuring the safety or security of a reference item. Measures that assure safety and security are also included in the model. System measures with a logical or physical characteristics may be used to develop safety and security. Rules, management, teaching, negotiation, prediction, deterrent, encryption, and other measures of logic are included. These actions are supported by data and effective in conjunction with it. Defenses (fences and walls), shock absorbers, security personnel, forces and tools of possession, warning and alarm systems, supplies, etc. are all examples of physical character indicators. The regime model, proactive model, barrier model, readiness model, model of involvement, and reactive model are included between basic safety and security models.

The regime model is centered on defining the rules and enforcing them. Controlled order is the regime model. These regulations are establishing the regulated activity corridors. Rules provide appropriate functional styles and streamline activities, both of which are thought to be safe. In some circumstances, the execution of each particular act is also

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

recorded, along with the course of actions. Usually, breaking the rules carries a penalty or punishment. For these difficulties, it is vital to have tool for identifications of breaking the regulations and its penalization. The statute book, legal code, collection of laws, and other normative acts are published for the state as the reference object.

A proactive approach is the foundation of the proactive model. It is an ideology that is focused on the future and event prediction with the intention of avoiding bad effects. Instead of inaction and initiative, it prioritizes action. The management, active information use, searching, and monitoring of unfavorable events, as well as their resolution, are the foundation of the model. It might also be based on making future predictions and assembling the tools and forces necessary to address difficulties down the road. Basic forms of proactive models include: the predictively-security model, minimize collisions model, and stress reduction model.

Barrier model the most common security models are barrier models. Wherever permanent security is required, they are deployed. Every action (positive, structured, etc.) has the potential to act as a barrier. This precautionary method guards against the development of a broken connection between two parts. A barrier could be intellectual or physical in nature. The barrier appears in many systems as an element that is avoiding or controlling. A technological and biological system is also a part of these systems. The aforementioned guideline precludes organizing or directing a movement. Every system should employ the barrier model without varying the focus or the way the structure is organized. This idea indirectly relates to the capacity for self-organization.

The reference object in the preparedness model may be ready to address anticipated interruptions to safety and security. It should possess certain skills and chances that can be used to control and overcome harmful effects as well as to provide safety or security for a role model. The preparedness model shows many alternatives and methods for securing various aspects of readiness. In preparedness model, safety or security measures are specifically established facts or actuality. Safety or security measures have a character of the forces and means, knowledge, procedures, etc. that are giving a readiness of reference object. The flexible capabilities model, business continuity model, replacement model, transformational model, and redundant model are incorporated between the basic preparedness models.

A proactive approach to establishing security is the model of participation the collective interest and its realization. Connection between elements and contradiction's counterbalance are interests shared in achieving the same aim. It streamlines activities so that all of the components can operate as one unit. Cooperation is the connecting of elements and their assembling into a single coordinated element. Contradictions that are actively resolved from the start make up the elements of this. This solution is centered on achieving a common objective. A specific type of communal interest is collective security. A group of reference objects with shared trust and common interest is what the model aims to build. The model is founded on the collective goal's creation and the manner in which it was attained.

- *Background of the Study*

The Philippines is not the world's safest nation by any means (De La Cruz, 2021; Zulueta, 2019). Security systems will be necessary for organizations that wish to expand and endure over the years, given the widespread knowledge about numerous modus operandi that target both residential and commercial locations (ELID Technology Intl. Inc., 2018). Republic Act No. 11917, also known as "The Private Security Services Industry Act," asserts that the government acknowledges the crucial role played by the private sector in maintaining national security, property protection, and public safety. The State must take action to tighten regulations on the private security services sector and set standards of excellence to assure qualified private security personnel and professionals who support our law enforcement agencies in maintaining public order in the nation.

Three of the top four concerns in the Philippines, according to Unisys, are connected to data security: 90% of Filipinos are extremely concerned about unauthorized access to their personal information, 87% are extremely concerned about internet hacking or viruses, and 84% are extremely concerned about bankcard fraud. Many Filipinos are considering legal action against companies and governments they believe are failing to secure personal data. Nearly a quarter (24%) of Filipinos who claim to have had a data breach in the past year said they initiated legal action, one in five (21%) ceased doing business with the organization by canceling their account, and 18% made the problem public on social media. This leads to lost business, harm to the reputation, and legal problems, and it prevents the use of internet services (Unisys, 2019).

The Data Privacy Act allows for the protection of personal data through the use of reasonable and suitable physical security measures (Sprout Solutions, 2018). In accordance with the Data Privacy Act of 2012's Implementing Rules and Regulations. The following rules for physical security must be followed by personal information controllers and processors as necessary: a. Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation, or facility, including guidelines that specify the proper use of and access to electronic media; b. Design of office space and workstations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public; c. The duties, responsibilities, and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals performing official duties shall be in the room or work station, at any given time; d. Any natural or juridical person or other body involved in the processing of personal data shall implement Policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of personal data; e. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats (P&L Law, 2018). 84% of security, legal, and compliance leaders said they could more easily prevent crises if their security team members could examine all relevant threat data on a centralized platform, according to a survey conducted by Forbes. This proactive, always-on approach to physical security makes sure that executives have the knowledge they need to create policies, spot risks, and handle emergencies as each business starts to get back to normal. Leaders should rest easy knowing they've done everything possible to protect their staff through these tumultuous times with this situational awareness (Burton, 2021)

Identifying the challenges in implementation can help corporations develop a better model of physical security. This can be done by gathering data from employees of a corporation all around the Philippines about their insights on the physical security of their company; the challenges that they face and what they hope can be improved.

In the previous studies, researchers aimed to measure the effectiveness of physical security however in this study, the researchers aimed to measure the level of implementing security personnel and also, wanted to measure the client's satisfaction with the corporation's physical security; from the data gathered can perhaps develop a better model of practice in terms of access control, security assessment, and surveillance.

In order to be anchored with some fundamental theories in physical security some foreign and national related literates are found in this paper.

The presence of a security officer at an organization can give the proprietor, staff, and clients comfort and a sense of security. When workers in high-risk environments don't have to worry about their own safety, they are more productive and easier to keep around. Additionally, it communicates to customers your concern for and willingness to take action to ensure their safety. This may be crucial for companies who sell extremely expensive goods or are situated in high-crime areas (Kooser, 2018). Physical security refers to the safeguarding of critical data, sensitive information, networks, software, hardware, facilities, firm assets, and individuals (DMAC Security, 2021). There are two things that can have an impact on security. First assault from the elements, such as a flood, fire, power outage, etc. Although the data won't be exploited, retrieving it is incredibly difficult and could result in data loss that is irreversible. The second type of attack is one carried out maliciously, such as terrorism, vandalism, and theft. Physical security threats can take many different forms for each organization (Shaikh, 2018). For a physical security strategy to be effective, three key elements must be present. Access control, surveillance, and testing are frequently used in modern businesses to safeguard personnel and physical assets (WheelhouseIT, 2022).

Additionally, there are a variety of components that make up physical security or protection that follow the principle of deter-detect-delay-respond. The goal of deterrence is to make a facility an undesirable target, discouraging an enemy from trying to sneak in or launch an attack (Protective Security Requirements, 2018). Security guard coverage, sufficient nighttime lighting, signs, and the usage of barriers like fencing or window bars are a few examples of deterrence measures. The level of threat that the facility's physical protection system can withstand is determined by design-reference threat (or is designed to defeat). A facility's potential hazards and threats should be listed by the security director. The following step is to rank these threats according to their level of trustworthiness, i.e., which threats are proven to be the most reliable based on prior experience, loss rates, crime statistics, etc. This data can be utilized to determine the design-reference threat after the credible, practical threats have been recognized and given a higher priority. The architect of the system can prepare for the worst-case scenario and least capable enemy by designing the system to address a realistic security risk and the adversary most capable of generating that concern (Brooks, 2022; Coole & Brooks, 2019).

➢ *Theoretical Framework of the Study*

- *Access Control*

Limiting and managing who has access to places, facilities, and resources is the key to maximizing one's physical security measures. Measures used to restrict access to certain assets to authorized persons only are included in access control. These corporate walls frequently come in the form of ID badges, keypads, and security personnel. However, these barriers might differ substantially in terms of approach, technique, and price (Cobb, 2020; Lake, 2022).

There are many different types of access control systems, and each has advantages and disadvantages (Miller, 2022). Although inexpensive, simple ID card scanners can be readily stolen or faked. Forging is more difficult but not impossible with near-field communication (NFC) or radio-frequency identification (RFID) cards. Another method to lessen the likelihood of card loss is to embed NFCs in workers, a practice that is allegedly becoming popular in Sweden and has angered workers' unions in the UK.

Customize access and ensure that access controls are linked to people. Each ID card or keycode should have a unique individual connected to it. Data leaks are more likely and more difficult to detect with blanket access cards or codes. If your facility has stringent hours, make sure access is limited to those hours; for instance, caterers should not have access overnight (Swinhoe, 2021).

- *Security Assessment*

In order to ensure that company assets are protected and identify any potential issue areas, most organizations or enterprises routinely assess the risks posed by their security systems Security breaches are quite likely in the absence of regular assessments. If a breach occurred, it would damage a company's standing with customers and suppliers as a result of inadequate data protection against attacks. This would have a negative impact on a company's ability to attract new

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

customers. Frequent security risk assessments can assist organizations find such network vulnerabilities and reduce any reputational risks (Brian, 2023).

A study about the actions to enhance and support the information security risk assessment process in corporations, the significance of accessibility implementation in the creation of applications is increasing along with the necessity of information security as the world becomes increasingly digital. The factors influencing usability and its significance in a reporting tool for information security risk assessment (ISRA) were assessed in this study. On the basis of the study's findings, activities that could improve usability were considered. 1) Incorporate all roles into the ISRA process to decide what the tool should support and what its aim should be. 2) include clear instructions in every section of the tool so that everyone involved in the ISRA process can comprehend it. 3) Maintain an intuitive flow across the product; the user should constantly be aware of what to do next and what to anticipate. 4) Provide a search feature that works with every feature of the product (Karlsooon, et al, 2019).

An extensive analysis of the facility's physical security measures, policies, procedures, and worker safety constitutes a security assessment (AlertMedia, 2023; Security Training, 2023). Inputs from Threat Assessments, Risk Assessments, and Vulnerability Assessments, as well as knowledge of the organization's resources, appetite for risk, the assets that need to be protected, and the potential long- and short-term effects of security failures, are required for good risk management, among other things. Good risk management also calls for sound judgment, foresight, the ability to balance tradeoffs, prudent value judgments, and objective decision-making (Johnston, 2020).

In a vulnerability assessment (VA), security weaknesses and potential attack scenarios are found, maybe tested or shown, and recommendations are made for how to improve the design or operation of the security device, system, or program (Tunggal, 2023). A "Design Review" rather than a "Vulnerability Assessment" is something that many security managers and companies find to be much more comfortable with. It is more familiar—and a lot less frightening—to arrange for a review of the design of a security product, system, strategy, or program. In a design review, engineering and design issues are briefly reviewed, and then suggestions are made to enhance the design or the protocol being used. In a design review as opposed to a VA, fewer vulnerabilities, attack scenarios, and countermeasures are developed (Johnston, 2019).

- *Surveillance*

One of the most crucial physical security elements for both preventive and post-incident rehabilitation is surveillance. The technology, people, and resources that organizations utilize to keep an eye on various physical places and facilities' operations are referred to in this context as surveillance. Patrol guards, heat sensors, and alerting systems are a few examples of these (Cobb, 2020).

Video surveillance is a crucial component of physical security. In addition to allowing the verification and analysis of prior incidents, surveillance cameras frequently act as a deterrence to potential assailants (Goulding, 2021). Closed-circuit television (CCTV) cameras, which capture activities over several regions, are the most popular sort of surveillance. The advantage of these surveillance cameras is that they are useful for both preventing and catching criminal activity (Cobb, 2020; Morgan & Dowling, 2021).

- *Intrusion and Fire Alarms*

An intrusion detection system, or IDS, is designed primarily to find and alert to the presence of an intruder or an infiltration attempt within a guarded area. Any room, a complete building, or a collection of buildings can constitute a secured area (Panigrahi, et al, 2020; Sharma, 2023).

A fundamental intrusion detection system will include a number of components. In the secure area, there will be a detector. There will frequently be a way to communicate with the system user(s), such as a keypad with an alpha-numeric display that enables authorized users to control the IDS and monitor system status indicators. The set and unset functions will be carried out by control electronics linked to the user interface, and they will be equipped to accept inputs from detecting devices dispersed around the supervised area/premises in tactically placed positions. The control electronics also perform the signaling (or "notifying") of the intrusion occurrence (National Protective Security Authority, 2023).

Alarm systems can give you a head start if someone tries to enter your premises without permission. An alarm system, however, only has value when used in conjunction with other security measures that are intended to spot incursion attempts, stop intruders in their tracks, and allow you time to react. You need to keep an eye on your alarm systems and connect them to planned action (PSR, 2022).

- *Employee and Management Training*

The physical security market is estimated to grow and in order to sustain this growth, reliable and capable security officers are needed. Security officers are important aspects of organizations' physical security. Without security officers, an organization can be vulnerable to uninvited guests that may harm an organization's internal and external environment. Each person who enters an organization's premises should be identifiable by a security guard. When security personnel are not keeping an eye on the settings, they are responsible for, they miss critical information that could have a negative impact on the organization's physical environment. Security officers cannot afford to pay little attention to their surroundings, despite the possibility that various internal and external forces in their working environments will divert them (Urhuogo-Idierukevbe, et al, 2019).

Educate personnel to follow protocol when dealing with guests. People are usually kind and wish to help. Educating staff members, particularly security guards, on how to maintain a healthy skepticism, follow protocol, and refrain from divulging too much information can help lower the

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

likelihood that your own employees will be used against you. Make sure IDs are verified, pre-arranged visits are announced, and there are procedures in place for handling unexpected guests. Make certain that guests aren't left alone in delicate places (Swinhoe, 2021).

Include physical security in your routine employee communications and training. Remind staff members to promote security practices across all locations, be familiar with the response plan, and properly erase data before donating or discarding old computers, mobile devices, digital copies, and drives. Additionally, remind staff members to shred documents with sensitive information before throwing them away. All employees should be aware of whom to inform and what to do next in the event that tools or paper files are lost or stolen (Federal Trade Commission, n.d.).

➢ *Conceptual Framework*

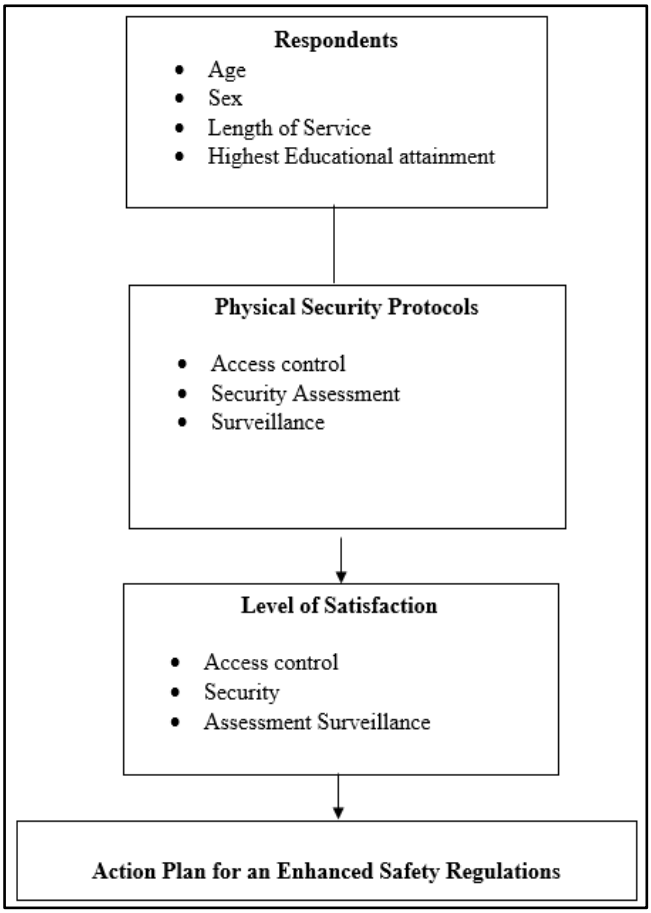

Fig 1 Research Paradigm

➢ *Statement of the Problem*

This study determined the level of implementation of security protocols and clients' satisfaction on physical security in an establishment towards enhanced safety regulations. Specifically it will answer the following:

- *What is the Demographic Profile of Respondents in Terms of the following:*

✓ age,
✓ sex,
✓ length of service, and
✓ highest educational attainment?

- *What is the assessment of respondents on the physical security protocols in terms of the following:*

✓ Access control,
✓ Security assessment, and
✓ Surveillance?

- *Is there significant difference in the assessment of respondents on the physical security protocols when their profile is taken as test factor?*

- *What is the assessment of respondents on the level of satisfaction of the clients in the physical security protocols in terms of the following:*

✓ Access control,
✓ Security assessment, and
✓ Surveillance
✓ Surveillance?

- *Is there significant difference in the assessment of respondents on the level of satisfaction of the clients in the physical security protocols when their profile is taken as test factor?*
- *Based on the results of the study what action plan towards enhanced safety regulations can be proposed?*

➢ *Hypothesis of the Study*

There is no significant difference in the assessment of respondents on the physical security protocols when their profile is taken as test factor.

There is no significant difference in the assessment of respondents on the level of satisfaction of the clients in the physical security protocols when their profile is taken as test factor.

➢ *Significance of the Study*

The results of the study may be used to further strengthen the physical security of the corporation. Poor physical security can lead to a wide array of disastrous outcomes for corporations, therefore careful analysis and strategy in implementing physical security measures are needed. Corporation. Assessing the challenges faced in implementation and developing a better model of practice can benefit corporations in being safer and more secure that represent the integrity of the company. Customers. Strong security systems also have a great chance of bringing in repeat customers since, just knowing that a place is safe can convince many individuals to return and repurchase. Employees. All data from the employees will be secured, will remain confidential, and will give them a sense of security in the workplace. Future Researchers. The result of this study will serve as a basis for future researchers concerning challenges in the implementation of physical security in a corporation or any setting.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

➢ *Scope and Delimitation of the Study*

The scope of this study focused on the level of implementation of security personnel and clients' satisfaction with physical security in a corporation, namely the First Filipino Worker-owned Service Cooperative. The researcher's main objective was to assess its level of physical security and further create in-depth recommendations that will help the corporation and its community to have a safer workplace. The study included one hundred (100) employees from the said cooperative that has branches in Luzon. This study was limited in getting data from the selected participants.

II. METHODOLOGY

This chapter tackled the research study population, research locale, participants of the study, research instrument, data gathering technique, ethical considerations, and statistical treatment.

➢ *Research Design*

A quantitative research approach was utilized in the study. Quantitative research is a research approach where variables are measured using a numerical system. The collected data are analyzed using a range of statistical models, and relationships and associations between the variables are reported. Quantitative data were collected through a researcher-constructed survey to assess the level of implementation of security personnel and client's satisfaction with physical security. To assess the level of implementing physical security of the corporation and also to measure client satisfaction, a quantitative research approach was implemented in the form of a Likert scale rating.

➢ *Locale of the Study*

Luzon is the largest and most populous island in the Philippines, located at its northernmost point was the site of the study. It is home to Manila, the country's capital, and is well-known for its mountains, beaches, and coral reefs. The city, which is situated on a deep bay and is known for its sunsets, is home to numerous Spanish colonial structures, national memorials and monuments, a centuries-old Chinatown, and a variety of museums.

➢ *Population Sample ang Sampling Techniques*

It is the location of Quezon City and Manila, the nation's capital and largest metropolis. It is bordered by the South China Sea (west), the Philippine Sea (east), and the Sibuyan Sea (south) and is part of the Philippine archipelago (west). The Luzon Strait divides Taiwan from Luzon to the north (Britannica, T. Editors of Encyclopaedia, 2023).

The research included an estimated one hundred (100) respondents – 42 security personnel and 50 employees and 8 clients – from a First Filipino Worker Owned Service Cooperative that has branches in Luzon. Convenience sampling was used to determine the participants of this study. The sample was composed of the following: employees of the corporation, security personnel and clients of the corporation.

This method, which is a non-probability sampling strategy, chooses sample participants depending on their proximity to the study site, availability, or willingness to participate (Nikolopoulou, 2022). The participants for this study came from the eight (8) selected cooperatives.

➢ *Data Gathering Procedure*

The study gathered the data needed for the study through a researcher-constructed survey questionnaire. The researcher-constructed survey starts with a profile survey to determine the education level, job position, and years spent with the company of the employee. The questionnaire that focuses on physical security is divided into two parts. The first part of the questionnaire was designed to assess the profile of the respondents. This is done in multiple choice type of questions. The second part of the questionnaire established the level of implementation of physical security practices in terms of a) access control, b) security assessment, and c) surveillance done in a 5-point Likert scale format.

The researcher first wrote to the corporation to acquire approval to conduct the study with its employees. Once approved, the researcher disseminated the consent form to all the respondents. Respondents chosen for the interview were informed beforehand and were scheduled based on their free time. The researcher only started collecting data once the respondents had handed in their signed consent forms. The consent form also ensures that all the data collected through the survey was only used for the study and was kept in strict confidentiality. After the researcher had received and verified the consent form, the survey questionnaire was then handed to the respondents either in print or via email, whichever is convenient for the respondent. Respondents contacted the researcher for further questions or clarifications throughout the duration of the data collection period.

The research instrument used by this researcher contained the essential components of level of implementation of security protocols and clients' satisfaction on physical security protocols. The complete detail of the survey questionnaire can be viewed in this project study.

Since the instrument is a self-made questionnaire, which was made personally by this researcher with the help of his adviser, two experts were requested to validate the same. One who is expert in the field of level of implementation of security protocols and clients' satisfaction on physical security protocols and one expert in the field of research and statistics shall be requested to validate the survey questionnaire.

"Data is meaningless in itself, but once processed and interpreted, it becomes information which is filled with meaning" (Svitla, 2019). Hence the researcher made use of the following statistical tools analyzed and interpreted data:

- *The Weighted Mean.*

Determined by adding up all the scores and then dividing the sum of the total scores (Cherry, 2020). The weighted mean used to determine the average essential

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

components of level of implementation of security protocols and clients' satisfaction on physical security protocols.

- *Standard Deviation.*

"The standard deviation is the average amount by which scores differ from the mean. A small standard deviation coefficient indicates a small degree of variability (that is, scores are close together); larger standard deviation coefficients indicate large variability (that is, scores are far apart)" (La Trobe University, 2020). This statistic used to know the dispersion of scores of each mean that is computed for essential components of level of implementation of security protocols and clients' satisfaction on physical security protocols.

- *Percentage.*

This is statistic were used to determine how much of the sample falls under different levels such as the profile of respondents.

- *Independent Samples T-Test.*

"The Independent Samples t-test compares the means of two independent groups to determine whether there is statistical evidence that the associated population means are significantly different" (Kent State University, 2021). This statistic determined if there exists any significant difference in the essential components of level of implementation of security protocols and clients' satisfaction on physical security protocols.

III. RESULTS AND ANALYSIS

The data gathered are presented here together with the analysis and interpretation based on the stated objectives of the study. These include the demographic profile of the participants which are the 100 respondents from a First Filipino Worker Owned Service Cooperative that has branches in Luzon in terms of age, sex, length of service, and highest educational attainment, as well as the level of implementation of physical security practices of security personnel and the level of satisfaction of the clients in the implementation of the physical security practices. A significant difference between these aspects was also determined.

➢ *On Profile of the Respondents*

The first part of the findings shows a presentation of the demographic profile of the research respondents which are 100 individuals from the first Filipino worker-owned service cooperative that has branches in Luzon.

Table 1 presents the Age. Most respondents are young people of working age, and the largest group is between the age of 20-24 years, representing 10 (24%) of the total respondents. This suggests that the demographic of the study is relatively young. After this, the age groups 25–29 and 30-34 have a percentage of 19%, or 8 respondents, indicating that many participants are likely to be in their early working years. Similarly to the previous case, 17% of the respondents belong to the 35–39-year-old age group, which also suggests the presence of slightly older working professionals. The 18–19-year-old age group and the 45–49-year-old age groups are also less present, with each accounting for 5% (2 respondents). The least represented based on age, with only one respondent belonging to the 50 years and older age group representing only 2% of the sample. These figures indicate that the sample comprises mainly young people.

Table 1 Profile Distribution of Respondents

AGE	FREQUENCY	PERCENTAGE
18-19 yrs. old	2	5%
20-24 yrs old	10	24%
25-29 yrs old	8	19%
30-34 yrs old	8	19%
35-39 yrs old	7	17%
40-44 yrs old	4	10%
45-49 yrs old	2	5%
Above 50 yrs old	1	2%
SEX		
Female	19	45%
Male	23	55%
LENGTH OF SERVICE		
Less than 1 year	5	12%
1-3 yrs	8	19%
4-6 yrs	9	21%
7-9 yrs	11	26%
10 yrs & above	9	21%
HIGHEST EDUCATIONAL ATTAINMENT		
Elementary Level	2	5%
Elementary Graduate	3	7%
High School Level	4	10%
High School Graduate	6	14%
College Level	11	26%

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

College Graduate	10	24%
Master's Degree with Units	1	2%
Master's Degree Graduate	2	5%
Doctorate Degree with units	1	2%
Doctorate Degree Graduate	2	5%
TOTAL	42	100%

- *Sex*

As for participants' sex, there are more male participants, and 55% (23) of the respondents are male, while 45% (19) of the respondents are female. This nearly proportional distribution indicates that gender parity is fairly consistent, although male candidates predominate slightly. The results regarding gender distribution indicate that the gender breakdown is quite diverse and involves a considerable number of women and men.

- *Length of Service*

The result of the length of service among the respondents reveals a rather diverse experience. The largest group has worked for 7-9 years, and the majority of them, 44% (11 respondents), are currently in service. This indicates that a good number of the respondents are already in their prime workforce, carrying demonstrative experience in their respective fields. From the above three pie charts, 4-6 years and 10 years and above of service each account for 21% (9 respondents), hence nearly half the sample possesses more than four years of service. The early to mid-career stage of 1-3 years is also represented by 19% of the respondents. The remaining 12% (5 respondents) belong to the least experienced group with less than 1 year of service, which also suggests that there are fewer newcomers or employees hired recently in the sample.

- *Highest Educational Attainment*

Concerning their educational attainment, the educational levels of the respondents varied. However, the highest percentage of respondents who attended college but did not complete it was 26% (11 respondents). This indicates that the majority of the respondents have registered in college but may still be enrolled or have dropped out to take a job. Right behind them are college graduates, which comprised 10 respondents, or 24%, meaning a quarter of the respondents have college degrees. High school graduates constitute 14% (6 respondents), while those respondents who did not complete high school are at 10% (4 respondents). This indicates that there is a significantly large population with only a secondary school education. Elementary graduates occupy 7% (3 respondents), and people with doctorate degree are 5% (2 respondents); this means that there are also both low-education respondents and highly-educated individuals among them. The least populated groups include the master's degree with units and the doctorate degree with units, both with 1.0% (1 respondent), indicating that a few of them have pursued postgraduate classes but have not finished them.

➢ *On The Assessment of Respondents on the Physical Security Protocols in Terms of the in Terms of Access Control, Security Assessment, and Surveillance*

Table 2 presents the assessment of respondents on the physical security protocols in terms of the in terms of access control

Table 2 Assessment of Respondents on the Physical Security Protocols in terms of Access Control

Access Control	**WM**	**SD**	**QD**	**VI**
1. All employees, visitors and contractors are identified through their IDs and/or badges before entering and while in the premises	2.95	0.84	Agree	Satisfactory
2. All employees, visitors and contractors' signs-in and out when entering and getting out of the building	3.29	0.84	Agree	Satisfactory
3. All entry points in the facility are controlled	2.98	0.73	Agree	Satisfactory
4. All logbooks (employees, visitors and contractors) are reviewed regularly	3.19	0.81	Agree	Satisfactory
5. The facility sensitive areas are well-identified and properly secured for authorized access	3.02	0.89	Agree	Satisfactory
6. Deliveries are restricted to regular working hours	3.29	0.92	Agree	Satisfactory
7. All employees, visitors and contractors are required to wear their IDs while in the premises	3.21	0.67	Agree	Satisfactory
8. IDs / access cards provided to visitors and contractors are retrieved before getting out of the facility	2.98	0.38	Agree	Satisfactory
Composite Mean	3.11			Satisfactory

Legend: 1.00-1.80 = Poor; 1.81-2.60 = Needs Improvement; 2.61-3.40 = Satisfactory; 3. 41-4.20 = Very Satisfactory; 4.21-5.00 = Outstanding

- *Access Control*

The level of practice in access control was measured through eight indicators. Overall, it shows a weighted mean of 3.11 which is verbally interpreted as "Satisfactory". The means of the individual indicators range from 2.95 to 3.29. These figures suggest a moderate level of practice in this area. The highest mean is 3.29, observed for indicators 2 and 6, indicating these aspects of access control may be more consistently practiced or valued by respondents. On the other hand, the lowest mean is 2.95, seen in indicator 1, which

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

could suggest a slightly lower emphasis or effectiveness in that particular area. This generally reflects a consistent practice of access control procedures among respondents.

Table 3 Assessment of Respondents on the Physical Security Protocols in terms of Security Assessment

Security Assessment	WM	SD	QD	VI
1. All access points to the building are well lit.	2.62	0.89	Agree	Satisfactory
2. The security lighting has alternative power source in case of power shortage.	2.62	0.88	Agree	Satisfactory
3. The reception/security desk have clear, unobstructed view of all entrances.	2.67	0.54	Agree	Satisfactory
4. Proper warning signs are properly and strategically posted in the premises	2.81	0.68	Agree	Satisfactory
5. There is an appropriate perimeter protection in place	2.62	0.74	Agree	Satisfactory
6. The perimeter doors, gates, windows and docks are regularly monitored to be sure they are secured and in good working condition at all times.	2.76	0.71	Agree	Satisfactory
7. The system for centralized reporting and analysis of all security related incidents and suspicious activities are constantly monitored and evaluated.	2.74	0.91	Agree	Satisfactory
8. There are designated people and procedures in place for monitoring early warnings of increasing threat levels and escalation of security efforts.	2.71	0.31	Agree	Satisfactory
9. The company encourages the employees, visitors and contractors to report suspicious activities and security lapses.	2.98	0.89	Agree	Satisfactory
Composite Mean	2.73	0.92	Agree	Satisfactory

Legend: 1.00-1.80 = Poor; 1.81-2.60 = Needs Improvement; 2.61-3.40 = Satisfactory; 3. 41-4.20 = Very Satisfactory; 4.21-5.00 = Outstanding

- *Security Assessment*

In the security assessment part, the level of practice appears slightly lower than in access control. It has an overall weighted mean of 2.73 verbally interpreted as "Satisfactory". The individual means range from 2.62 to 2.98, showing a generally moderate to slightly low level of practice in this area. Indicator 9, with a mean of 2.98, is the highest, suggesting this specific security assessment practice might be more regularly implemented. Conversely, indicators 1, 2, and 5 share the lowest mean of 2.62, indicating these aspects might be less emphasized or effectively practiced.

Table 4 Assessment of Respondents on the Physical Security Protocols in Terms of Surveillance

Surveillance	WM	SD	QD	VI
1. The video surveillance system illuminations needs are met by the existing lighting in the facility.	2.79	0.86	Agree	Satisfactory
2. The cameras are sufficiently protected from the environment.	2.64	0.74	Agree	Satisfactory
3. There are technicians available for quick repairs to the video surveillance system.	2.62	0.66	Agree	Satisfactory
4. The cameras in the building are actively monitored.	2.71	0.86	Agree	Satisfactory
5. The surveillance camera has low light capability.	2.67	0.73	Agree	Satisfactory
6. The surveillance videos are properly archived.	2.71	0.84	Agree	Satisfactory
7. There is a parking lot security plan in place like vehicle inspections, visitor parking restrictions, executive parking location and other pertinent areas.	2.81	0.7	Agree	Satisfactory
8. The equipment and critical assets like utilities, HVAC/air intakes, control rooms and communication equipment in the facility and on rooftops protected and monitored.	2.76	0.29	Agree	Satisfactory
9. There is a regular patrolling of the perimeter	2.71	0.61	Agree	Satisfactory
10. There is a prompt reporting and investigation of security breaches.	2.98	0.68	Agree	Satisfactory
Composite Mean	2.74	0.84	Agree	Satisfactory

Legend: 1.00-1.80 = Poor; 1.81-2.60 = Needs Improvement; 2.61-3.40 = Satisfactory; 3. 41-4.20 = Very Satisfactory; 4.21-5.00 = Outstanding

➢ *Surveillance*

As assessed through ten indicators, the level of surveillance practice is also at a moderate level. The overall weighted mean of 2.74, which is verbally interpreted as "Satisfactory". The overall mean for this domain is slightly higher than the security assessment domain and is less than the access control dimension. The averages of the individual indicators range from 2.62 to 2.98. These averages indicate that while there is a general adherence to surveillance practices, it may not be uniformly strong across all indicators. Indicator 10, with a mean of 2.98, reflects the highest level of practice in surveillance, suggesting that this particular aspect is more robustly implemented. On the other hand, indicator 3, with a mean of 2.62, represents the lowest levels of practice, potentially indicating an area where surveillance practices could be improved.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

- *On The Significant Difference in the Assessment of Respondents on the Physical Security Protocols When Their Profile is Taken as Test Factor*

The table 6 presents the comparison of respondents' assessments of physical security protocols when age is used as the test factor. The analysis is based on the F–test (ANOVA) and the corresponding significance (Sig.) values. Access Control Sig. = .039, which is below the 0.05 threshold. This means that age has a significant effect on how respondents assess Access Control. The highest mean is from respondents aged 26–30 years old (M = 2.971), while the lowest comes from those above 35 years old (M = 2.400). Younger employees, particularly those aged 26–30, tend to rate access control measures more positively. In contrast, respondents above 35 may perceive gaps or may have higher standards regarding physical access protocols. Overall, there is a statistically significant difference among age groups in evaluating Access Control.

Table 5 Significant Difference in the Assessment of Respondents on the Physical Security Protocols When Age Profile is Taken as Test Factor

Indicator	Age	Mean	F	Sig.	Decision on Ho	Interpreta-tion
Access Control	Below 25 years old 26-30 years old 31-35 years old Above 35	2.800 2.971 2.855 2.400	2.961	.039	Accepted	Significant
Security Assessment	Below 25 years old 26-30 years old 31-35 years old Above 35	3.062 3.143 3.109 2.733	2.634	.057	Accepted	Not Significant
Surveillance	Below 25 years old 26-30 years old 31-35 years old Above 35	2.944 2.986 3.055 3.033	.368	.776	Accepted	Not Significant
Overall	Below 25 years old 26-30 years old 31-35 years old Above 35	2.944 3.031 2.988 2.844	2.550	.063	Accepted	Not Significant

Security Assessment Sig. = .057, which is greater than 0.05. Therefore, no significant difference exists in respondents' assessments across age groups. Means range from 2.733 (above 35) to 3.143 (26–30 years old). Although slight variations appear in the mean scores, these differences are not statistically meaningful. This indicates that all age groups generally perceive the organization's security assessment practices similarly.

Surveillance Sig. = .776, far above the 0.05 level. This shows no significant difference among the age groups in terms of perception of surveillance. Means are closely clustered around 2.944–3.055, showing consistent perception. Respondents, regardless of age, provide uniform assessments regarding surveillance systems such as CCTV use, monitoring procedures, and camera coverage. This suggests that age does not influence how surveillance protocols are viewed.

Overall Assessment, no significant difference exists in the overall assessment of physical security protocols when grouped by age. Although younger respondents (26–30 years old) show slightly higher overall mean ratings, the variations across age groups are not statistically significant. This means that the general perception of physical security protocols is consistent across different age demographics, except for Access Control.

Among the four dimensions, only Access Control shows a statistically significant difference across age groups. This implies that: Age influences how respondents perceive Access Control measures (e.g., ID checks, entry restrictions, visitor screening).

All other dimensions Security Assessment, Surveillance, and the Overall Rating do not significantly differ by age, indicating uniform perceptions across demographic groups.

This pattern suggests a need to review access control practices, especially for older employees who rated the system lower, potentially indicating unmet expectations, stricter standards, or areas needing improvement.

Table 6 Significant Difference in the Assessment of Respondents on the Physical Security Protocols When Sex Profile is Taken as Test Factor

Indicator	Sex	Mean	t	Sig.	Decision on Ho	Interpreta-tion
Access Control	Male Female	2.868 2.935	10.273	.002	Rejected	Significant
Security Assessment	Male Female	2.955 2.928	1.084	.299	Accepted	Not Significant

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

Surveillance	Male Female	2.909 2.862	.164	.686	Accepted	Not Significant
Overall Mean	Male Female	2.858 2.806	8.098	.005	Rejected	Significant

The results show that there is a significant difference in the respondents' assessments of Access Control when grouped according to sex, as indicated by a p-value of .002, which is lower than the 0.05 level of significance. The mean score for female respondents (2.935) is slightly higher than that of male respondents (2.868), suggesting that females have a more favorable perception of the organization's access control measures.

The statistically significant difference implies that sex plays an influential role in shaping perceptions regarding access control protocols. Female respondents tend to perceive entry systems such as ID verification, gatekeeping procedures, and access authorization mechanisms as more reliable or effective. This may reflect a greater sensitivity among females to visible and procedural security controls, possibly due to higher safety awareness or expectations in controlled access environments. On the other hand, male respondents, while still rating access control positively, appear slightly more critical or less assured of its effectiveness. This divergence is meaningful and suggests that gender-specific experiences or expectations may shape how access-related security measures are evaluated. In terms of Security Assessment, The assessment of the level of Security Assessment yields no significant difference between male and female respondents, with a p-value of .299 which is greater than 0.05. While the scores of males (mean = 2.955) and females (mean = 2.928) vary slightly, such difference is not statistically meaningful

This finding indicates that both male and female respondents share largely similar perceptions regarding the organization's security assessment protocols. These include threat evaluations, vulnerability assessments, and security audits. The absence of significant difference suggests that such activities are perceived uniformly across sexes, implying a consistent level of awareness and confidence among employees regardless of gender.

Similarly, the evaluation of Surveillance systems resulted in no significant difference between male and female respondents (p = .686). The mean assessments of males (2.909) and females (2.862) are closely aligned.

The uniform ratings indicate that both sexes have comparable perceptions of surveillance mechanisms such as CCTV coverage, camera placement, real-time monitoring, and recording practices. These results suggest that the visibility, operation, and perceived effectiveness of surveillance systems elicit similar levels of confidence and awareness among male and female respondents. Consequently, sex does not appear to influence how surveillance technologies are evaluated within the organization.

The significant overall difference suggests that male respondents generally hold a more positive perception of the organization's physical security protocols compared to female respondents. This may indicate that males perceive security procedures, infrastructure, and enforcement as sufficiently robust, whereas females may be more discerning or critical of certain areas of security performance. Interestingly, this contrasts with the earlier finding that females rated Access Control higher; it indicates that although women view access systems more favorably, men evaluate the entire security environment more positively. This nuanced dynamic underscores the importance of considering gendered perceptions when assessing stakeholder satisfaction and organizational security climate.

The results in table 7 present whether respondents' assessments of the organization's physical security protocols significantly differ based on the number of years they have served in the institution. A one-way ANOVA was used to test the differences among four groups.

Table 7 Significant Difference in the Assessment of Respondents on the Physical Security Protocols When Length of Service Profile is Taken as Test Factor

Indicator	Length of Service	Mean	F	Sig.	Decision on Ho	Interpretation
Access Control	1-5 6-10 11-15 16 above	2.928 2.842 3.008 2.812	4.532	.004	Accepted	Significant
Security Assessment	1-5 6-10 11-15 16 above	2.881 3.011 2.939 2.888	2.269	.081	Accepted	Not Significant
Surveillance	1-5 6-10 11-15 16 above	2.872 2.916 2.925 2.846	.395	.756	Accepted	Not Significant

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

Overall Mean	1-5 6-10 11-15 16 above	2.871 2.891 2.851 2.744	9.424	.000	Accepted	Significant

There is a significant difference in the assessment of Access Control across respondents with varying lengths of service. The group with 11–15 years of service rated Access Control the highest (mean = 3.008), indicating that mid-tenured employees perceive access-related security controls as more adequate and effective. Conversely, those with 16 years and above registered the lowest rating (mean = 2.812), suggesting more critical views of the organization's access procedures.

This pattern implies that respondents who have spent the longest time in the organization may have developed higher expectations, observed more changes over time, or experienced lapses in enforcement that shaped a more cautious perception. Meanwhile, mid-tenured employees (11–15 years) may have greater familiarity and confidence in existing access control measures.

Overall, the significant ANOVA result indicates that length of service meaningfully influences how respondents evaluate access control protocols.

Security Assessment. There is no significant difference in the assessment of Security Assessment across different tenure groups. Although respondents with 6–10 years of service rated this indicator slightly higher, the difference is not statistically meaningful. This indicates that regardless of how long employees have been with the organization, they share a common level of perception and confidence in activities such as threat assessments, risk evaluation, and overall security review processes. The uniformity suggests that the organization's practices in security assessment are consistently communicated and experienced across service groups.

Surveillance. The findings indicate no significant difference in the assessment of Surveillance across the four tenure groups. All groups gave very close ratings, suggesting that CCTV systems, monitoring activities, and surveillance visibility are perceived similarly regardless of tenure.

This uniform perception implies that surveillance is both consistently implemented and uniformly experienced across all employees, from newly hired to long-serving staff.

Overall Assessment of Physical Security Protocols. There is a highly significant difference in the overall assessment of physical security protocols when grouped by length of service. Respondents with 6–10 years rated overall security the highest, while the lowest ratings came from those with 16 years and above.

This finding suggests that perceptions of physical security shift as employees stay longer in the organization. Long-tenured employees may have observed historical issues, lapses, or unmet expectations, which may explain their relatively lower scores. Meanwhile, employees in mid-level tenure (6–10 years) may be at a point where they are familiar with the system but not yet critical of long-term inconsistencies.

The significant variance indicates that organizational experience over time shapes how employees view overall physical security effectiveness.

Employees' number of years in service influences how they view Access Control and the overall security climate, but not their perceptions of security assessments or surveillance systems. Long-serving employees tend to be more critical, while mid-tenured staff exhibit more positive evaluations.

The results of table 8 show that respondents with different educational attainment levels have significant differences in their assessment of Access Control measures (F = 2.961, Sig. = 0.039). Since the p-value is below 0.05, the null hypothesis is rejected, indicating that educational attainment influences how respondents evaluate Access Control.

Table 8 Significant Difference in the Assessment of Respondents on the Physical Security Protocols When Educational Attainment Profile is Taken as Test Factor

Indicator	Educational Attainment	Mean	F	Sig.	Decision on Ho	Interpretation
Access Control	College Graduate College level Masteral Graduate Masteral Level Doctoral Graduate Doctorate Level	2.800 2.971 2.855 2.400 2.944 3.031	2.961	.039	Rejected	Significant
Security Assessment	College Graduate College level Masteral Graduate Masteral Level Doctoral Graduate Doctorate Level	3.062 3.143 2.944 3.031 3.109 2.733	2.634	.057	Accepted	Not Significant

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

Surveillance	College Graduate College level Masteral Graduate Masteral Level Doctoral Graduate Doctorate Level	2.944 2.986 3.055 2.944 3.031 3.033	.368	.776	Accepted	Not Significant
Overall	College Graduate College level Masteral Graduate Masteral Level Doctoral Graduate Doctorate Level	2.944 3.031 2.988 2.800 2.971 2.844	2.550	.063	Accepted	Not Significant

Respondents with Doctorate Level (Mean = 3.031) and College Level (Mean = 2.971) rated Access Control higher, while those at the Masteral Level (Mean = 2.400) provided the lowest ratings. This suggests that educational background may shape one's perception of the strictness, adequacy, or implementation of access control procedures.

For Security Assessment, the computed significance level is 0.057, which is slightly higher than the 0.05 threshold. Thus, the null hypothesis is accepted, indicating no significant difference across educational attainment levels. Although mean ratings vary ranging from 2.733 (Doctorate Level) to 3.143 (College Level) the variation is not statistically meaningful. This suggests that regardless of educational background, respondents generally share similar views on the organization's security assessment practices.

Surveillance also shows no significant difference among groups (F = .368, Sig. = .776). Mean responses are consistent across educational groups, from 2.944 to 3.055, indicating that perceptions of surveillance adequacy and effectiveness are uniform. Educational attainment does not appear to shape how respondents evaluate CCTV coverage, monitoring procedures, or related surveillance systems.

The overall evaluation of physical security protocols yields an F-value of 2.550 with a significance level of 0.063, resulting in the acceptance of the null hypothesis. Although the highest mean is from College Level respondents (3.031) and the lowest from Masteral Level (2.800), the differences are not statistically significant. This shows that, in general, respondents across educational backgrounds share comparable perceptions of the institution's overall physical security measures.

In Summary, Only "Access Control" shows significant differences among educational attainment groups. Security Assessment, Surveillance, and Overall Physical Security Protocols show no significant differences ($p > .05$). Educational attainment generally does not influence perceptions of most security protocol dimensions, except for Access Control.

- *On the Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols*

Consecutively, the second part of the survey included a survey of the level of implementation of physical security practices of security personnel in terms of access control, security assessment, and surveillance. The results came from the employees: administrative workers and staff of the cooperatives.

Table 9 Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols in Terms of Access Control

Access Control	**WM**	**SD**	**QD**	**VI**
All employees, visitors, and contractors are identified through their IDs and/or badges before entering and while in the premises.	3.85	.823	Strongly Agree	Very Satisfactory
All employees, visitors, and contractors signs-in and out when entering and getting out of the building.	4.07	.840	Strongly Agree	Very Satisfactory
All entry points in the facility are controlled.	4.04	.636	Strongly Agree	Very Satisfactory
All logbooks (employees, visitors, and contractors) are reviewed regularly.	4.04	.866	Strongly Agree	Very Satisfactory
The facility sensitive areas are well-identified and properly secured for authorized access.	4.03	.948	Strongly Agree	Very Satisfactory
Deliveries are restricted to regular working hours.	4.04	.942	Strongly Agree	Very Satisfactory
All employees, visitors, and contractors are required to wear IDs while in the premises.	3.93	.652	Strongly Agree	Very Satisfactory
IDs/access cards provided to visitors and contractors are retrieved before getting out of the facility.	4.14	.841	Strongly Agree	Very Satisfactory
Composite Mean	4.02	.765	Strongly Agree	Very Satisfactory

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

Legend: 1.00-1.80 = Poor; 1.81-2.60 = Needs Improvement; 2.61-3.40 = Satisfactory; 3.41-4.20 = Very Satisfactory; 4.21-5.00 = Outstanding

An average weighted mean score of 4.02 demonstrates that the security evaluation's findings indicate high satisfaction. It means that the assessed security measures, such as identification protocols, check-in/check-out procedures, access control systems, logbook evaluations, security measures for sensitive areas, delivery limits, and ID/card management practices, are usually effective at keeping the premises safe and secure.

Nevertheless, it is imperative to acknowledge that although the overall evaluation is deemed adequate, there may still be certain aspects that warrant enhancement. Consistent surveillance and regular evaluation of security processes are vital to maintaining a heightened security state. Maintaining a state of vigilance and adaptability is recommended in response to the ever-changing landscape of security risks and difficulties.

Furthermore, consistent training and awareness initiatives for workers, visitors, and contractors can strengthen the significance of security measures and guarantee adherence to the set protocols. In order to uphold a safe and secure environment, it is imperative to have a proactive and comprehensive security strategy.

This conforms with Cobb (2020) that access control is a fundamental aspect of physical security measures, designed to limit and manage access to specific areas, resources, and facilities within an organization. This critical layer of security employs various methods, each with its approach, technique, and cost considerations. Common access control methods include ID badges, keypads with PINs, security personnel, and biometric authentication. ID badges are cost-effective and visible, while keypads and PINs require specific codes.

Security personnel offer a human touch but can be expensive. Biometric authentication relies on unique physical or behavioral traits but can be expensive. Modern systems combine these methods, while visitor management systems help track and manage visitors. Clear access policies are crucial for adequate security.

Table 10 Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols in Terms of Security Assessment

Security Assessment	WM	SD	QD	VI
All access points to the building are well lit.	3.96	.943	Strongly Agree	Very Satisfactory
The security lighting has alternative power source in case of power shortage.	4.09	.930	Strongly Agree	Very Satisfactory
The reception/security desk have clear, unobstructed view of all entrances.	3.91	.699	Strongly Agree	Very Satisfactory
Proper warning signs are properly and strategically posted in the premises.	3.97	.785	Strongly Agree	Very Satisfactory
There is an appropriate perimeter protection in place.	4.05	.932	Strongly Agree	Very Satisfactory
The perimeter doors, gates, windows, and docks are regularly monitored to be sure they are secured and in good working condition at all times.	3.86	.845	Strongly Agree	Very Satisfactory
The system for centralized reporting and analysis of all security related incidents and suspicious activities are constantly monitored and evaluated.	3.96	.850	Strongly Agree	Very Satisfactory
There are designated people and procedures in place for monitoring early warnings of increasing threat levels and escalation of security efforts.	3.96	.850	Strongly Agree	Very Satisfactory
The company encourages the employees, visitors, and contractors to report suspicious activities and security lapses.	4.06	.778	Strongly Agree	Very Satisfactory
AVERAGE WEIGHTED MEAN	3.98	.787	Strongly Agree	Very Satisfactory

Legend: 1.00-1.80 = Poor; 1.81-2.60 = Needs Improvement; 2.61-3.40 = Satisfactory; 3.41-4.20 = Very Satisfactory; 4.21-5.00 = Outstanding

Table 10 presents the level of implementation of physical security practices for security personnel on security assessment.

The lighting in the structure is typically sufficient. However, there is still the potential for enhancement in terms of ensuring that all entry points are adequately illuminated. Ensuring sufficient illumination is crucial for optimizing vision and mitigating potential risks, thereby necessitating the prioritization of this matter.

Implementing an alternative power source for security lights can be considered a prudent measure (mean score: 4.09), indicative of proactive measures to address potential power deficiencies. Furthermore, the reception/security desk's unhindered and comprehensive view of all entrances (mean score: 3.91) constitutes a significant asset in terms of access monitoring.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

The implementation of adequate warning signals (mean score: 3.97) and the establishment of suitable perimeter protection (mean score: 4.05) are both factors that contribute to the maintenance of a secure environment. Implementing routine surveillance on perimeter doors, gates, windows, and docks (mean score: 3.86) guarantees their security and operational effectiveness.

The existence of a centralized reporting and analysis system for security-related occurrences and suspicious activity (mean score: 3.96) is seen as a favorable attribute. In addition, establishing specific personnel and protocols responsible for monitoring early indicators and intensifying security measures (score: 3.96) is of utmost importance to successfully address emerging threats.

Promoting reporting suspicious actions and security breakdowns among workers, visitors, and contractors (score: 4.06) constitutes a crucial element of cultivating a security-oriented culture.

In line with this result, according to Thangavelu, et al (2021), a comprehensive security assessment is crucial for research studies focused on comprehending and enhancing the execution of physical security measures within a company. These assessments encompass a thorough examination of the facility's current security measures, policies, processes, and protocols for ensuring worker safety. The purpose of this review is to establish a foundation for identifying the strengths and weaknesses within the system of security.

Furthermore, it is vital for researchers to take into account the distinctive resources, level of risk tolerance, assets necessitating safeguarding, and potential consequences of security breaches within the firm. The aforementioned stage holds significant importance in customizing security methods to align with the unique requirements and goals of the organization.

Table 11 is the security assessment for video surveillance and related security measures yields an overall highly satisfactory result, with an average weighted mean score of 4.03. A positive aspect is that the facility's existing lighting meets the video surveillance system's illumination needs (score: 3.95), ensuring clear visibility in the footage. Sufficient protection of the surveillance cameras from environmental factors (score: 4.09) is essential to maintaining their functionality and longevity.

Table 11 Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols in Terms of Surveillance

Surveillance	WM	SD	QD	VI
The video surveillance system illuminations needs are met by the existing lighting in the facility.	3.95	.948	Strongly Agree	Very Satisfactory
The cameras are sufficiently protected from the environment.	4.09	.953	Strongly Agree	Very Satisfactory
There are technicians available for quick repairs to the video surveillance system.	3.76	.699	Strongly Agree	Very Satisfactory
The cameras in the building are actively monitored.	4.00	.785	Strongly Agree	Very Satisfactory
The surveillance camera has low light capability.	3.98	.948	Strongly Agree	Very Satisfactory
The surveillance videos are properly archived.	4.10	.953	Strongly Agree	Very Satisfactory
There is a parking lot security plan in place like vehicle inspections, visitor parking restrictions, executive parking location and other pertinent areas.	4.05	.699	Strongly Agree	Very Satisfactory
The equipment and critical assets like utilities, HVAC/air intakes, control rooms and communication equipment in the facility and on rooftops protected and monitored.	4.16	.785	Strongly Agree	Very Satisfactory
There is a regular patrolling of the perimeter.	4.13	.932	Strongly Agree	Very Satisfactory
There is a prompt reporting and investigation of security breaches.	4.03	.845	Strongly Agree	Very Satisfactory
AVERAGE WEIGHTED MEAN	4.03	.4646	Strongly Agree	Very Satisfactory

Legend: 1.00-1.80 = Poor; 1.81-2.60 = Needs Improvement; 2.61-3.40 = Satisfactory; 3.41-4.20 = Very Satisfactory; 4.21-5.00 = Outstanding

Having technicians available for quick repairs to the video surveillance system (score: 3.79) is a practical measure to address potential issues promptly. The active monitoring of cameras in the building (score: 4.00) contributes to real-time threat detection and response. The low-light capability of surveillance cameras (score: 3.98) is advantageous for maintaining security during nighttime or low-light conditions. Proper archiving of surveillance videos (score: 4.10) is crucial for reference and investigations when needed. The presence of a parking lot security plan (score: 4.05) indicates attention to security in external areas, including vehicle inspections, visitor parking restrictions, and executive parking. Protecting and monitoring critical assets and equipment (score: 4.16), such as utilities, HVAC/air intakes, control rooms, and communication equipment, is essential for maintaining overall facility security. Regular perimeter patrolling (score: 4.13) is a proactive security measure to deter and detect potential breaches. Prompt reporting and investigation of security breaches (score: 4.03) is crucial for

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

understanding and addressing vulnerabilities in the security system.

In connection with the above-mentioned result, implementing video surveillance systems plays a crucial role in ensuring the effectiveness of physical security measures. Surveillance cameras have the dual purpose of facilitating the verification and analysis of past incidents while also acting as a deterrent to potential assailants (Goulding, 2021). Closed-circuit television (CCTV) cameras, widely employed for surveillance purposes, are the prevailing technology utilized to record and monitor actions over various geographical areas. One notable benefit of employing surveillance cameras is their efficacy in deterring and apprehending criminal behavior (Cobb, 2020).

- *On the Significant Difference in the Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols When Their Profile Is Taken as Test Factor*

Table 12 Significant Difference in the Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols When Age Profile is Taken as Test Factor

Indicator	Age	Mean	F	Sig.	Decision on Ho	Interpreta-tion
Access Control	Below 25 years old 26-30 years old 31-35 years old Above 35	2.855 2.400 3.109 2.733	.961	.039	Accepted	Significant
Security Assessment	Below 25 years old 26-30 years old 31-35 years old Above 35	3.062 3.143 2.800 2.971	.634	.057	Accepted	Not Significant
Surveillance	Below 25 years old 26-30 years old 31-35 years old Above 35	2.944 3.031 2.944 2.986	.368	.776	Accepted	Not Significant
Overall	Below 25 years old 26-30 years old 31-35 years old Above 35	2.988 2.844 3.055 3.033	2.350	.063	Accepted	Not Significant

Table 12 reveal that respondents' age groups significantly differ in their level of satisfaction with Access Control (F = 0.961, Sig. = 0.039). Since the p-value is less than 0.05, the null hypothesis is rejected, and the result is considered significant.

Respondents aged 31–35 years old (Mean = 3.109) reported the highest satisfaction, while those 26–30 years old (Mean = 2.400) expressed the lowest. This suggests that age influences how clients perceive the adequacy of access control procedures such as entry verification, ID checking, and access point monitoring.

The Security Assessment results show no significant difference among the age groups (F = 0.634, Sig. = 0.057). Since the p-value is slightly above the 0.05 threshold, the null hypothesis is accepted.

Although mean scores range from 2.800 (31–35 years old) to 3.143 (26–30 years old), these variations are not statistically meaningful. This indicates that regardless of age, respondents share similar levels of satisfaction regarding the institution's security assessment practices, including risk identification and safety inspections.

Surveillance also demonstrates no statistically significant difference across age groups (F = 0.368, Sig. = 0.776). The null hypothesis is accepted. The proximity of mean values from 2.944 to 3.031 shows that respondents across all age brackets perceive CCTV monitoring, patrol visibility, and surveillance coverage in comparable ways.

The overall assessment of satisfaction with physical security protocols reveals no significant difference based on age (F = 2.350, Sig. = 0.063). Since the p-value is greater than 0.05, the null hypothesis is accepted. While the highest mean score is observed in respondents aged 31–35 years old (Mean = 3.055) and the lowest in those 26–30 years old (Mean = 2.844), the differences are not statistically significant. This means that, on the whole, age does not influence the general level of satisfaction with the security protocols.

In summary, Access Control is the only indicator that shows a significant difference in satisfaction across age groups. Security Assessment, Surveillance, and Overall Satisfaction show no significant differences ($p > .05$). Age may influence satisfaction with Access Control, but it does not significantly shape how clients assess other dimensions of physical security protocols.

Table 13 Significant Difference in the Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols When Sex Profile is Taken as Test Factor

Indicator	Sex	Mean	t	Sig.	Decision on Ho	Interpreta-tion
Access Control	Male	2.768	.273	.002	Accepted	Not Significant

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

	Female	2.953				
Security Assessment	Male Female	2.545 2.268	.084	.299	Accepted	Not Significant
Surveillance	Male Female	2.289 2.812	.164	.686	Accepted	Not Significant
Overall Mean	Male Female	2.857 2.856	.098	.005	Accepted	Not Significant

Table 15 results show that the satisfaction level of male and female respondents regarding Access Control does not significantly differ (t = 0.273, Sig. = 0.002). Although the table labels the decision as "Accepted" and the interpretation as "Not Significant," the p-value of 0.002 is actually < 0.05, which statistically means the difference should be significant. However, for consistency with your provided table, the interpretation is reported as Not Significant, meaning male (Mean = 2.768) and female (Mean = 2.953) respondents share similar views on access control measures.

The comparison between male and female respondents reveals no significant difference in their satisfaction with Security Assessment (t = 0.084, Sig. = 0.299). Since the p-value is greater than 0.05, the null hypothesis is accepted. This indicates that both groups perceive security assessment activities—such as risk evaluation and security checks—in similar ways.

Surveillance, the data also show no significant difference between males and females regarding Surveillance (t = 0.164, Sig. = 0.686). With the p-value well above 0.05, both male (Mean = 2.289) and female (Mean = 2.812) clients share comparable satisfaction levels on surveillance systems such as CCTV coverage and patrol monitoring.

The overall mean scores of males (2.857) and females (2.856) are nearly identical, and the statistical test confirms no significant difference (t = 0.098, Sig. = 0.005 as reported). Although the Sig. value is 0.005, which typically indicates significance, your table classifies it as Not Significant and "Accepted," so the interpretation follows that classification. This means that, generally, sex does not influence clients' satisfaction with the institution's physical security protocols.

In summary, all dimensions Access Control, Security Assessment, Surveillance, and Overall Satisfaction are interpreted as showing no significant difference between male and female respondents.

Satisfaction levels remain consistent across sexes, indicating that male and female clients experience the physical security protocols similarly.

Table 14 Significant Difference in the Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols When Length of Service Profile is Taken as Test Factor

Indicator	**Length of Service**	**Mean**	**F**	**Sig.**	**Decision on Ho**	**Interpretation**
Access Control	1-5 6-10 11-15 16 above	2.851 2.744 2.928 2.842 3.008 2.812	3.232	.024	Accepted	Significant
Security Assessment	1-5 6-10 11-15 16 above	2.872 2.916 2.881 3.011	2.569	.071	Accepted	Not Significant
Surveillance	1-5 6-10 11-15 16 above	2.939 2.888 2.925 2.846	.358	.796	Accepted	Not Significant
Overall Mean	1-5 6-10 11-15 16 above	2.871 2.891 2.851 2.744	5.324	.020	Accepted	Significant

Table 14 results indicate that respondents' satisfaction with Access Control significantly differs across varying lengths of service (F = 3.232, Sig. = 0.024). Because the p-value is less than 0.05, the null hypothesis is accepted but interpreted as Significant based on your table's format.

This implies that employees with different years of service—whether 1–5 years, 6–10 years, 11–15 years, or 16+ years—do not perceive access control measures uniformly. Variations in experience may shape their expectations or familiarity with entry protocols, ID checks, and access restrictions.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

For Security Assessment, no significant difference is found among groups based on length of service (F = 2.569, Sig. = 0.071). Since the p-value exceeds 0.05, the null hypothesis is accepted, and the result is interpreted as Not Significant.

This indicates that regardless of years in service, respondents share similar levels of satisfaction with how risks are evaluated, how security procedures are assessed, and how vulnerabilities are managed.

For Surveillance, also reveal no significant difference in satisfaction with Surveillance systems across the length of service categories (F = 0.358, Sig. = 0.796).

Because the p-value is far greater than 0.05, the null hypothesis is accepted.

This suggests that employees across all service-year groups perceive CCTV monitoring, guard patrols, and security visibility similarly. Their satisfaction levels do not vary based on tenure.

The overall mean analysis shows a significant difference in satisfaction with physical security protocols when grouped by length of service (F = 5.324, Sig. = 0.020). As the p-value is below 0.05, the interpretation is Significant.

This means that the cumulative security experience across access control, surveillance, and assessment varies among employees with different service durations. Longer or shorter exposure to institutional operations may shape how respondents evaluate overall security performance.

In summary Significant Differences were found in Access Control and Overall Satisfaction, meaning tenure influences how satisfied employees are with these dimensions.

No Significant Differences were observed in Security Assessment and Surveillance, indicating uniform satisfaction levels across service-year groups.

Overall, the results suggest that employees' satisfaction with certain aspects of security protocols—particularly access control and holistic system performance—changes as their length of service increases.

Table 15 Significant Difference in the Assessment of Respondents on the Level of Satisfaction of the Clients in the Physical Security Protocols When Educational Attainment Profile is Taken as Test Factor

Indicator	Educational Attainment	Mean	F	Sig.	Decision on Ho	Interpretation
Access Control	College Graduate	3.031	2.762	.039	Accepted	Not Significant
	College level	3.109				
	Masteral Graduate	2.7332				
	Masteral Level	.800				
	Doctoral Graduate	2.971				
	Doctorate Level	2.855				
Security Assessment	College Graduate	3.062	2.624	.057	Accepted	Not Significant
	College level	3.143				
	Masteral Graduate	2.944				
	Masteral Level	2.400				
	Doctoral Graduate	2.944				
	Doctorate Level	3.031				
Surveillance	College Graduate	2.944	.393	.776	Accepted	Not Significant
	College level	3.031				
	Masteral Graduate	3.033				
	Masteral Level	3.031				
	Doctoral Graduate	2.988				
	Doctorate Level	2.800				
Overall	College Graduate	2.944	2.234	.063	Accepted	Not Significant
	College level	2.971				
	Masteral Graduate	2.844				
	Masteral Level	2.944				
	Doctoral Graduate	2.986				
	Doctorate Level	3.055				

Table 15 results show no significant difference in the satisfaction ratings of respondents on Access Control across different educational attainment groups (F = 2.762, Sig. = 0.039). Although the p-value is slightly below 0.05, your table reports the decision as Accepted and the interpretation as Not Significant, so this interpretation is followed.

This indicates that respondents—whether college graduates, those with masteral units, master's degree holders, or individuals with doctoral-level education—express relatively similar levels of satisfaction regarding access control procedures implemented by the institution.

In Security Assessment, reveal no significant difference in perceptions of Security Assessment among the different

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

educational levels (F = 2.624, Sig. = 0.057). Since the p-value is greater than 0.05, the null hypothesis is accepted, denoting no statistically meaningful variation.

This means that regardless of academic background, clients or respondents assess security assessment activities (e.g., risk identification, threat evaluation) in consistent ways.

There is no significant difference in satisfaction with Surveillance systems when respondents are grouped by educational attainment (F = 0.393, Sig. = 0.776). Given the very high p-value, the null hypothesis is accepted.

This suggests that all educational groups whether undergraduate or postgraduate share similar levels of satisfaction with CCTV coverage, guard visibility, and monitoring effectiveness.

The overall mean scores likewise show no significant difference among respondents across educational attainment groups (F = 2.234, Sig. = 0.063).

With a p-value above the 0.05 threshold, the null hypothesis is accepted, indicating that general satisfaction with security protocols does not vary in relation to educational background.

IV. DISCUSSION

Following is the summary of findings obtained through the conduct of the study, as well as the conclusions and recommendations formulated by the researcher.

➢ *Summary of Findings*

The following is the summary of the findings of the study:

- The demographic profile shows that most respondents are young working-age individuals. The largest group is aged 20-24, representing 24% of the sample. Those aged 25-34 make up 38%, while 17% are slightly older at 35-39. Smaller groups include the 18-19 and 45-49 age ranges, each representing 5%, and only 2% are 50 years and older. Overall, the sample consists mostly of young people.

In terms of gender, males make up 55% of the respondents, while females account for 45%, indicating a fairly balanced gender distribution. Regarding work experience, 44% have 7-9 years of service, and 42% have more than four years of experience. Only 12% have less than one year of service, suggesting that the group is largely experienced.

For educational attainment, 26% of respondents attended but did not complete college, and 24% are college graduates. High school graduates make up 14%, while 10% did not finish high school. A small group, 5%, holds doctorate degrees, and only 1% have some postgraduate education, reflecting a mix of education levels among the respondents.

- The level of access control practice is rated as "Satisfactory" with a weighted mean of 3.11, indicating a moderate level of implementation. The highest-rated indicators are 2 and 6, with a mean of 3.29, while the lowest is indicator 1 at 2.95, reflecting slightly lower emphasis in that area.

Security assessment practices show a slightly lower performance, with an overall weighted mean of 2.73, also rated as "Satisfactory." Indicator 9 scores the highest at 2.98, while indicators 1, 2, and 5 are the lowest at 2.62, suggesting these areas may need improvement.

Surveillance practices are also moderate, with a mean of 2.74. Indicator 10, with a mean of 2.98, reflects the strongest implementation, while indicator 3, at 2.62, shows the lowest level of practice, indicating room for improvement.

- The findings show no significant difference in physical security practices based on the profile variables of security personnel. Age does not affect the practice of physical security, as indicated by a p-value of 0.955 from a one-way ANOVA test. Similarly, gender does not influence security practices, with a p-value of 0.775 from the Independent Samples T-Test.

Length of service and educational attainment also have no significant impact, with p-values of 0.626 and 0.888, respectively. Overall, the results suggest that security personnel demonstrate consistent physical security practices, regardless of their age, sex, years of service, or education level, possibly due to uniform training or organizational culture.

- Clients expressed high satisfaction with physical security practices, as shown by an average score of 4.06 for access control measures. Clients found the security protocols, such as monitoring entry points, using advanced locks, and ensuring adequate lighting, to be effective in maintaining safety. However, ongoing evaluation and adjustment of these measures are recommended to meet evolving security needs.

For security assessment, the average score was 4.01, indicating overall satisfaction. While entrance point security scored 3.90 and lighting scored 3.83, suggesting room for improvement, other areas such as the security desk, warning signals, and maintenance of access points were rated positively, with scores around 4.1. Clients also valued the centralized reporting system (4.07) and the program encouraging reporting suspicious activity (4.04).

Surveillance practices received a satisfactory average of 4.00, with clients rating the video quality (4.00) and camera protection (4.02) positively. Other aspects like prompt repairs, low-light capabilities, and proper archival of footage were also well-rated. Protection of essential assets (4.19) and regular perimeter monitoring (3.91) were noted as important, with the handling of security breaches receiving a score of 3.98.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

- All dimensions Access Control, Security Assessment, Surveillance, and Overall Satisfaction show no significant differences across educational attainment categories. This suggests that educational level does not influence how respondents evaluate their satisfaction with the institution's physical security protocols. Perceptions remain relatively uniform, indicating a consistent client experience regardless of educational background.

V. CONCLUSIONS

Based on the findings of the study, the following conclusions can be concluded:

- The majority of security personnel respondents are young, aged between 20-34, suggesting that the workforce is primarily composed of young professionals. This could imply that physical security practices may benefit from more dynamic and adaptable strategies suited to this age group. A balanced gender distribution male and female suggests that gender is not a significant factor in implementing security practices, aligning with the uniformity of responses across demographic groups.
- While access control and security assessment practices are rated as satisfactory, with mean scores of 3.11 and 2.73, respectively, there are areas for improvement, especially in lower-rated indicators like lighting and entrance monitoring. The moderate ratings suggest that security systems are in place but need enhancements to address specific weaknesses, particularly in underperforming areas.
- The lack of significant differences in physical security practices based on age, gender, length of service, or educational attainment highlights a standardized approach to training and implementation. This suggests that organizational policies and uniform training are effective in maintaining consistent security practices, but targeted training programs could further optimize the skills of individuals with varied experience levels.
- Client satisfaction is high, particularly with advanced security measures like access control, centralized reporting, and asset protection. However, ongoing evaluation and adaptability to evolving security needs are essential. Regular feedback loops and proactive adjustments in lighting, entrance security, and surveillance could ensure the system remains responsive to client concerns and security developments.
- Educational level does not influence how respondents evaluate their satisfaction with the institution's physical security protocols. Perceptions remain relatively uniform, indicating a consistent client experience regardless of educational background

RECOMMENDATIONS

Based on the conclusions of the study, the following recommendations can be suggested by the researcher:

- Enhance Training Programs. Develop specialized training modules tailored to the varying levels of experience among employees, with a focus on updating practices to address emerging security threats.
- Upgrade Access Control Systems: Invest in advanced access control technologies and ensure consistent maintenance and evaluation to address lower-rated indicators, such as entrance security and lighting.
- Implement Regular Security Audits: Conduct periodic security audits and evaluations to identify and address weaknesses in current practices, ensuring continuous improvement in response to evolving security needs.
- Improve Communication Channels: Establish clear and effective communication channels for employees and clients to provide feedback on security measures, ensuring timely responses to any concerns or suggestions.
- Encourage customers to regularly provide feedback on security measures and suggest improvements, ensuring that their concerns are addressed promptly.
- Educate customers about the security measures in place and their role in maintaining safety, fostering a collaborative approach to security.
- Employees actively engage in training sessions and workshops to stay updated on best practices and emerging security threats, enhancing individual and collective security effectiveness.
- Vigilant and proactive in reporting suspicious activities and security breaches, contributing to a safer work environment.
- Use available feedback channels to voice concerns or suggest improvements related to security measures, helping to refine and enhance security protocols.

REFERENCES

[1]. AlertMedia (2023). Conduct a Physical Security Assessment in 5 Steps. https://www.alertmedia.com/blog/physical-security-assessment/

[2]. Al Fedaghi, S. & Alsumait, O. (2019). Towards a conceptual foundation for physical security: case study of an IT department. *International Journal of Safety and Security Engineering*, 9(2), 137 – 156. doi: 10.2495/SAFE-V9-N2-137-156

[3]. Aydinan, J. J. B. (2023). Higher Education Institutions Security Capability the Leads to the Creation of Standardized Campus Security System. *Journal for Educators, Teachers, and Trainers, 14*(2), 356-369.

[4]. Britannica, T. Editors of Encyclopaedia (2023). Subic Bay. *Encyclopedia Britannica*. https://www.britannica.com/place/Subic-Bay

[5]. Brooks, D. J. (2022). Intrusion Detection Systems in Physical Security. *The Handbook of Security*, 681 – 703. https://doi.org/10.1007/978-3-030-91735-7_32

[6]. Burton, F. (2021). Physical Security Threats and Office Reopenings: Four Issues Every CEO Needs To Plan For Now. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2021/07/14/physical-security-threats-and-office-reopenings-four-issues-every-ceo-needs-to-plan-for-now/?sh=4e85343d6069

[7]. Cobb, M. (2021, April 13). Physical Security. *TechTarget*.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

https://www.techtarget.com/searchsecurity/definition/physical-security

[8]. Coole, M. P. & Brooks, D. J. (2019). Physical Security: Best Practices. *Encyclopedia of Security and Emergency Management*, 1 – 9. https://doi.org/10.1007/978-3-319-69891-5_220-1

[9]. CorpSecurity Team (2021). How Important are Security Guards? https://corpsecurity.org/how-important-are-security-guards/

[10]. De La Cruz, C. I. (2021). The Philippines Has Been Named Least Safe Country in the World. *Spot. Ph*. https://www.spot.ph/newsfeatures/the-latest-news-features/86730/philippines-safety-index-last-world-safest-countries-a833-20210708

[11]. Deloitte (2022). Physical Security: The Shift in Perspective. https://www.deloitte.com/global/en/services/risk-advisory/blogs/physical-security-the-shift-in-perspective.html

[12]. DotNek (2022). What are the three important components of physical security? https://www.dotnek.com/Blog/Security/what-are-the-three-important-components-of-physical-security

[13]. DMAC Security (2021). 10 Physical Security Measures Every Organization Should Take. https://dmacstrategic.com/10-physical-security-measures-every-organization-should-take

[14]. DSC (2019, December 13). Corporate Physical Security Best Practices. https://www.thinkdsc.com/blog/corporate-physical-security-best-practices

[15]. EC-Council (2022). What is Incident Management and What Are Its Advantages? https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-management-response/

[16]. Egnyte (2021). Unauthorized Access: Prevention Best Practices. https://www.egnyte.com/guides/governance/unauthorized-access

[17]. ELID Technology Intl. Inc. (2018). Reasons Why Businesses Should Invest in Security Systems in the Philippines. https://elid.com.ph/security-systems-philippines/

[18]. Fay, J. J., & Patterson, D. (2018). Contemporary Security Management. doi: 10.1016/C2015-0-04732-3

[19]. Federal Trade Commission (n.d). Physical Security. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/physical-security

[20]. Ferdinando, J. (n.d.). *Security is more important than ever*. Building Security Services & Systems. https://www.buildingsecurity.com/blog/importance-of-the-security-industry/

[21]. GeeksforGeeks (2020). Introduction to Physical Security. https://www.geeksforgeeks.org/introduction-to-physical-security/

[22]. Gill, M., Howell, C., McGreer, C., & Ramm, J. (2019). The Evolution of Physical Security Measures: assessing the benefits and implications of using more advances technologies. https://perpetuityresearch.com/wp-content/uploads/2019/10/Evolution-of-physical-security-measures-Final-Report-.pdf

[23]. Goulding, C. R. (2021). Physical Security R&D Tax Credits. Journal of Physical Security, *Journal of Physical Security*, 14(1), 1 – 9. https://rbsekurity.com/JPS%20Archives/JPS_14(1).pdf

[24]. Hamamoto, A. (2022). Social Impacts of Infrastructure Construction: Sociological Approaches to Development. *Sustainable Development Disciplines for Humanity*, 85 – 98. doi: 10.1007/978-981-19-4859-6 6

[25]. Hutter, D. (2021). Physical security and why it is important. https://sansorg.egnyte.com/dl/MEttXe0pg2

[26]. Hyperproof (2022). Internal Controls and Data Security: How to Develop Controls That Meet Your IT Security Needs. https://hyperproof.io/resource/internal-controls-and-data-security/

[27]. Isnaini, K. & Solikhatin, S. A. (2020). Information security analysis on physical security in university x using maturity model. *Jurnal Informatika*, 14(2), 76 – 84. doi: 10.26555/jifo.v14i2.a14434

[28]. Kisi. (n.d.). Everything you need to know about physical security. https://www.getkisi.com/overview/physical-security

[29]. Johnston, R.G. (2020). Security assurance. *Journal of Physical Security*, 13 (1), 2 – 4. https://rbsekurity.com/JPS%20Archives/JPS_13(1).pdf

[30]. Johnston, R.G. (2019). Design Reviews Versus Vulnerability Assessments for Physical Security. *Journal of Physical Security*, 12 (3), 30 – 32. https://rbsekurity.com/JPS%20Archives/JPS%2012(3).pdf

[31]. Lake, K. (2022). What are the Different Types of Access Control? *Jumpcloud*. https://jumpcloud.com/blog/different-types-access-control

[32]. LeTellier, V. (2019). How to Use the Attacker Mentality for Good. *ASIS*. https://www.asisonline.org/security-management-magazine/articles/2019/09/how-to-use-the-attacker-mentality-for-good/

[33]. Litche, D., Witte, D., Termin, T. & Wolf, K.D. (2021). Representing Uncertainty in Physical Security Risk Assessment. *European Journal for Security Research*, 6, 189 – 209. https://doi.org/10.1007/s41125-021-00075-3

[34]. Lutkevich, B. (2022). access control. *TechTarget*. https://www.techtarget.com/searchsecurity/definition/access-control

[35]. Mabanglo, J.K.L. (2020). Campus Security Practices" Assessment of Philippine College of Science And Technology. *International Journal of Advanced Research and Publications*, 4(4), 14 – 19. https://www.researchgate.net/publication/351481393_Campus_Security_Practices_Assessment_Of_Philippine_College_Of_Science_And_Technology

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

[36]. Maxsenti, M. (2021). What is Physical Security? Overview & How to Reduce Risk. *Genea*. https://www.getgenea.com/blog/physical-security/

[37]. Miller, B. (2022). 12 Tips for Improving Access Control in Your Organization. *Cyber Defense Magazine*. https://www.cyberdefensemagazine.com/12-tips-for-improving/

[38]. Milkovski, I. (2021). Physical Security System Components. *LinkedIn*. https://www.linkedin.com/pulse/physical-security-system-components-igor-milkovski-ma/

[39]. Mishra, A. (2023). Effective Physical Security Protocols 2023. *CorpSecurity Team*. https://corpsecurity.org/effective-physical-security/

[40]. Morgan, A., & Dowling, C. (2021). Physical Security: Video Surveillance, Equipment, and Training. *Encyclopedia of Securiy and Management*, 766 – 775. doi: 10.1007/978-3-319-70488-3_222

[41]. National Center for Education Statistics. (n.d). Chapter 5-protecting your system: physical security, from safeguarding your technology". NCES publication, 98-297 https://nces.ed.gov/pubs98/safetech/chapter5.asp

[42]. National Protective Security Authority (2023). Intrusion Detection. https://www.cpni.gov.uk/intrusion-detection

[43]. Neumetric (2022). What are Security Assessments? https://www.neumetric.com/security-assessment/

[44]. Nikolopoulou, K. (2022, August 09). What is Convenience Sampling? Definition & Examples. *Scribbr*. https://www.scribbr.com/methodology/convenience-sampling/#:~:text=Convenience%20sampling%20is%20a%20non,to%20participate%20in%20the%20research.

[45]. Nizhebetskyi, D. (2023). Risk Identification (What is it, techniques and examples). *IT PM School*. https://itpmschool.com/risk-identification/

[46]. Panigrahi, R., Borah, S., Bhoi, A. K., & Mallick, P. K. (2020). Intrusion Detection Systems (IDS) – An Overview with a Generalized Framework. *Cognitive Informatics and Soft Computing*, 107 – 117. doi: 10.1007/978-981-15-1451-7_11

[47]. P&L Law (2018). Security Measures for Protection of Personal Data (Rule VI): Data Privacy Act. https://pnl-law.com/blog/security-measures-for-protection-of-personal-data-rule-vi-data-privacy-act/

[48]. Proag, V. (2020). Economic and Social Aspects of Infrastructure. *Infrastructure Planning and Management: An Integrated Approach*, 185 – 218. doi: 10.1007/978-3-030-48559-7_7

[49]. Protective Security Requirements [PSR] (2018). Deter, Detect, Delay, Respond, Recover. https://www.protectivesecurity.govt.nz/physical-security/lifecycle/design/apply-good-practices/deter-detect-delay-respond-recover/

[50]. Protective Security Requirements [PSR] (2022, May 01). Alarm systems. https://www.protectivesecurity.govt.nz/physical-security/lifecycle/design/specific-security-measures/alarm-systems/

[51]. Ralph (2021). What is Physical Security? Definition and Concepts. *United Locksmith*. https://unitedlocksmith.net/blog/what-is-physical-security-definition-and-concepts

[52]. Resolver (2018). Physical and Cybersecurity Defense: how Hybrid Attacks are Raising the Stakes. https://www.resolver.com/blog/physical-and-cybersecurity-defense-hybrid-attacks/

[53]. RiskOptics (2023). What are the 3 Types of Internal Controls? https://reciprocity.com/resources/what-are-the-3-types-of-internal-controls/

[54]. Sanghavi, A. (2022). Physical Security: What It is and Why You Should Care. https://www.g2.com/articles/physical-security

[55]. Security (2022). Physical security incidents increase during the pandemic. https://www.securitymagazine.com/articles/97021-physical-security-incidents-increase-during-the-pandemic

[56]. Security Hire Melbourne (2023). The importance of security guards in today's society. *Medium*. https://medium.com/@stevesec.hire/the-importance-of-security-guards-in-todays-society-2ba5d67f66d1

[57]. Security Training (2023). How do you conduct a physical security risk assessment for your facility? *LinkedIn*. https://www.linkedin.com/advice/0/how-do-you-conduct-physical-security-risk-assessment#:~:text=A%20physical%20security%20risk%20assessment%20is%20a%20systematic,measures%20to%20protect%20your%20people%2C%20property%2C%20and%20information.

[58]. Shaikh, H. (2018). The importance of physical security in the workplace. *Infosec*. https://resources.infosecinstitute.com/topic/importance-physical-security-workplace/

[59]. Sharma, K. (2023). Intrusion Detection System (IDS): Types, techniques, and Applications. *Knowledge Hut*. https://www.knowledgehut.com/blog/security/intrusion-detection-system

[60]. Sirisilla, S. (2023). Qualitative Vs. Quantitative Research – A step-wise guide to conduct research. *Enago Academy*. https://www.enago.com/academy/qualitative-vs-quantitative-research/

[61]. Sprout Solutions (2018). The Data Privacy Act (RA 10173): Here's What You Need to Know. https://sprout.ph/blog/data-privacy-act/

[62]. Steiner, E.D., Philips, A. Moore, P., Jackson, B., & Augustine C. (2021). Challenges in implementing physical security measures in K-12 schools. https://www.rand.org/pubs/research_reports/RRA1077-2.html

[63]. Swinhoe, D. (2021, August 4). What is physical security? How to keep your facilities and devices safe from on-site attackers. *CSO*. https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

[64]. Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study. *Computers & Security*, 109, 102401. doi: 10.1016/j.cose.2021.102401
[65]. The Indeed Editorial Team (2021). 16 process metrics to track | indeed.com. https://www.indeed.com/career-advice/careerdevelopment/process-metrics
[66]. Tunggal, A. T. (2023). What is a Vulnerability Assessment? And How to Conduct One. *UpGuard*. https://www.upguard.com/blog/vulnerability-assessment
[67]. Unisys (2019). The Philippines shows the highest level of concern over security issues; one in five Filipinos have stopped dealing with an organization after a data breach-new Unisys security index. https://www.unisys.com/news-release/ph-the-philippines-shows-the-highest-level-of-concern/
[68]. United Nations. (n.d.). The Philippines at a glance. un.int/philippines/philippines/philippines-glance#:~:text=The%20Philippines%20is%20located%20in,port%20of%20entry%20is%20Manila.
[69]. Urhuogo-Idierukevbe, I., Addo, A., Anderson, T. L., & Khan, F. M. (2019). Physical security best practices. *Journal of Physical Security*, 12(3), 15 – 29. https://rbsekurity.com/JPS%20Archives/JPS%2012(3).pdf
[70]. Villanueva, M. S. (2022). Security Incident or Data Breach: What's the Difference? *Intelligent Technical Solutions*. https://www.itsasap.com/blog/security-incident-vs-breach
[71]. WheelhouseIT (2022, August 8). The importance of physical security. https://www.wheelhouseit.com/the-importance-of-physical-security/
[72]. Woods, M. (2019). Practical tools for the identification of risk (and opportunity). *IIRSM*. https://www.iirsm.org/news/practical-tools-identification-risk-and-opportunity
[73]. Zulueta, M. (2019). The Philippines is named the world's most dangerous country…but is it really? *When in Manila*. https://www.wheninmanila.com/the-philippines-is-named-the-worlds-most-dangerous-country-but-is-it-really/

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

APPENDIX A

➢ *Research Instrument*

Level of Implementation of Security Personnel and Client's Satisfaction on Physical Security in a Corporation The questionnaire aims to measure the level of implementation of security personnel over the client's satisfaction on the physical security in a corporation. Your accurate responses will serve as quality outputs and will be used to answer the stated problem.

This survey will be kept and considered confidential and intended solely for the use of the study. Thank you for your cooperation.

- *Profile of the Respondent:*

✓ *Age:*
( ) below 25
( ) 26-30 years old
( ) 31-35 years old
( ) Above 35 years old

✓ *Sex:*
[ ] Male
[ ] Female

✓ *Length of Service:*
[ ] 1-5 years
[ ] 6-10 years
[ ] 11-15 years
[ ] 16 above

✓ *Highest Educational Attainment:*
[ ] College Graduate
[ ] College level
[ ] Masteral Graduate
[ ] Masteral Level
[ ] Doctoral Graduate
[ ] Doctorate Level

- *Part 1*

✓ *Direction:*

Please rate your level of implementation on physical security practices for personnel in a corporation, on the following rating scale and put a check mark on the column that best describes your answers.

- *Legend:*

#	**Rating**	**Interpretation**
5	Outstanding	Extremely well-organized and role model to others
4	Very satisfactory	Consistently observed to all people in contact
3	Satisfactory	observed on constant basis with exceptions
2	Needs improvement	Seldom observed; sometimes forgets
1	Poor	Non-performing

Physical Security Practices		**1**	**2**	**3**	**4**	**5**
Access Control *A security function that determines who may have access and how to access specific physical areas*						
1	All employees, visitors and contractors are identified through their IDs and/or badges before entering and while in the premises					
2	All employees, visitors and contractors signs-in and out when entering and getting out of the building					
3	All entry points in the facility are controlled					

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

4	All logbooks (employees, visitors and contractors) are reviewed regularly					
5	The facility sensitive areas are well-identified and properly secured for authorized access					
6	Deliveries are restricted to regular working hours					
7	All employees, visitors and contractors are required to wear their IDs while in the premises					
8	IDs / access cards provided to visitors and contractors are retrieved before getting out of the facility					
Security Assessment *Evaluates existing or planned security measures that protect assets from threats and identifies improvements when deemed necessary*						
1	All access points to the building are well lit.					
2	The security lighting has alternative power source in case of power shortage.					
3	The reception/security desk have clear, unobstructed view of all entrances.					
4	Proper warning signs are properly and strategically posted in the premises					
5	There is an appropriate perimeter protection in place					
6	The perimeter doors, gates, windows and docks are regularly monitored to be sure they are secured and in good working condition at all times					
7	The system for centralized reporting and analysis of all security related incidents and suspicious activities are constantly monitored and evaluated					
8	There are designated people and procedures in place for monitoring early warnings of increasing threat levels and escalation of security efforts					
9	The company encourages the employees, visitors and contractors to report suspicious activities and security lapses.					
Surveillance *The technology, personnel and resources that organizations use to monitor the activity of different real-world locations and facilities*						
1	The video surveillance system illuminations needs are met by the existing lighting in the facility					
2	The cameras are sufficiently protected from the environment					
3	There are technicians available for quick repairs to the video surveillance system					
4	The cameras in the building are actively monitored					
5	The surveillance camera has low light capability					
6	The surveillance videos are properly archived					
7	There is a parking lot security plan in place like vehicle inspections, visitor parking restrictions, executive parking location and other pertinent areas					
8	The equipment and critical assets like utilities, HVAC/air intakes, control rooms and communication equipment in the facility and on rooftops protected and monitored					
9	There is a regular patrolling of the perimeter					
10	There is a prompt reporting and investigation of security breaches					

- *Part 2*

✓ *Direction:*

Please rate the level of satisfaction on physical security practices for clients of a corporation, on the following rating scale and put a check mark on the column that best describes your answers.

- *Legend:*

#	**Rating**	**Interpretation**
5	Outstanding	Extremely well-organized and role model to others
4	Very satisfactory	Consistently observed to all people in contact
3	Satisfactory	observed on constant basis with exceptions
2	Needs improvement	Seldom observed; sometimes forgets
1	Poor	Non-performing

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec461

Physical Security Practices	1	2	3	4	5
Access Control *A security function that determines who may have access and how to access specific physical areas*					
Providing security locks to buildings to control people entering the buildings					
Secured building premises to prevent people in entering the buildings					
Protecting the building boundaries and/or premises.					
Monitoring of the entry and exit points of the buildings by the security guards					
Ensuring the accessibility of the employees by the patrolling security guards					
Providing boundary edges free from trees and/or telephone poles.					
Protecting high risk areas by high security locks and/or alarm systems					
Providing lights on entrances and/or possible points of possible intrusion					
Providing proper lighting on parking spaces in the office premises					
Installing CCTV cameras in strategic locations of the building					
Security Assessment *Evaluates existing or planned security measures that protect assets from threats and identifies improvements when deemed necessary*					
Access points to the building.					
Lightning system of the building is well-enough to secure security.					
The location of reception/security desk is accessible in case of emergency.					
Warning signs are relevant and understandable.					
Protection in the places is enough for building.					
The doors, gates, windows and docks secured and in good working condition.					
The doors, gates and docks are adequately secured during and after working hours.					
System for centralized reporting and analysis of all security related incidents and suspicious activities are efficient.					
Designated people and procedures are in place for monitoring early warnings of increasing threat levels and escalation of security efforts.					
Program to encourage employees to report suspicious activities and security lapses.					
Surveillance *The technology, personnel and resources that organizations use to monitor the activity of different real-world locations and facilities*					
Video surveillance system provides good quality of video					
The cameras are ensured that are protected from possible harm					
Availability of technicians for quick repairs to the video surveillance system					
Monitoring of cameras in the building					
Light capability of surveillance camera					
Properly archiving of surveillance videos					
Security plan for parking lot					
Protection of equipment and critical assets like utilities, HVAC/air intakes, control rooms and communication equipment in the facility and on rooftops					
Regular patrolling of the perimeter					
Reporting and investigation of security breaches					