UNIVERSITY OF TURKU

Implementation of ISO Frameworks to Risk Management in IPv6 Security

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

John Emmanuel Opuda

Supervisors:

Petri Sainio

Seppo Virtanen

May 2023

UNIVERSITY OF TURKU

Master of Science in Technology Thesis Department of Computing, Faculty of Technology University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: John Emmanuel Opuda
Title: Implementation of ISO frameworks to Risk Management in IPv6 security
Number of pages: 79 pages, 12 appendix pages
Date: May 2023

The Internet of Things is a technology wave sweeping across various industries and sectors. It promises to improve productivity and efficiency by providing new services and data to users. However, the full potential of this technology is still not realized due to the transition to IPv6 as a backbone. Despite the security assurances that IPv6 provides, privacy and concerns about the Internet of Things remain. This is why it is important that organizations thoroughly understand the protocol and its migration to ensure that they are equipped to take advantage of its many benefits. Due to the lack of available IPv4 addresses, organizations are in an uncertain situation when it comes to implementing IoT technologies.

The other aim are to fill in the gaps left by the ISO to identify and classify the risks that are not yet apparent. The thesis seeks to establish and implement the use of ISO to manage risks.It will also help to align security efforts with organizational goals. The proposed solution is evaluated through a survey that is designed to gather feedback from various levels of security and risk management professionals. The suggested modifications are also included in the study.

A survey on the implementation of ISO frameworks to risk management in IPv6 was conducted and with results as shown in random sampling technique that was used for conducting the research a total of 75 questionnaires shared online, 50 respondents returned responses online through emails and social media platforms. The result of the analysis show that system admin has the highest pooling 26% of all the overall participants, followed by network admin with 20%, then cybersecurity specialists with 16%. 14% of the respondents were network architects while senior management and risk management professional were 4% and 2% respectively.Majority of the respondents agreed that risk treatment enhances the risk management performance of IPv6 network resulting from proper selection and implementation of correct risk prevention strategies.

Keywords: IPv6 Security, Internet of Things, Risk Management and ISO

Acknowledgement

I would like to express my gratitude to all those who made it a point to motivate me to finish this project. I would also like to thank the risk management and security professionals who took time from their hectic schedules to help me complete the survey, especially from TurkuSec meetings.

Table of contents

List of figures

List of tables

Abbreviations and acronyms

ACID	Atomicity, Consistency, Isolation, Durability
ACL	Access Control List
BCP	Business Continuity Plan
BS	British Standard
BYOD	Bring your own Device
CIO/CTO	Chief Information/Technology Officer
CISO	Chief Information Security Officer
CMM	Capability Maturity Model
CoAP	Constrained Application Protocol
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
DAD	Duplicate Address Detection
DNSSec	Domain Naming System Security
DTLS	Datagram Transport Layer Security
ERM	Enterprise Risk Management
FERMA	Federation of European Risk Management Associations
GRC	Governance, Risk and Compliance
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPsec	Internet Protocol security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISO	International Organization for Standardization
KPI	Key Performance Indicators
LLN	Low power and Lossy Networks
MCR	Minimum Capital Requirement
MIP	Mobile Internet Protocol
MTU	Maximum Transmission Unit
NDP	Neighbor Discovery Protocol

NIST	National Institute of Standards and Technology
OCEG	Open Compliance and Ethics Group
OWASP	Open Web Application Security Project
ROI	Return on Investment
RPL	IPv6 Routing Protocol for Low-power and Lossy Networks
SCR	Solvency Capital Requirement
SeND	Secure Neighbor Discovery
SLA	Service Level Agreement
SLAAC	Stateless Address Auto-configuration
SSL	Secure Sockets Layer
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WBAN	Wireless Body Area Network

1 Introduction

1.1 Introduction to the research topic

The tremendous growth and usage of Internet over the past years has caused the versions of the Internet protocol to advance. For example, IPv4 is a 32-bit addressing standard is depleted, enforcing IETF to establish a new design of the Internet protocol version 6 (IPv6) in the 1990s (Supriyanto,2014). IPv6 is the establishment for future connectivity designed and established with much higher addressing storage to accommodate more connectivity and simplicity to users. One of the major new functions of IPv6 is to address auto configurations of more unique hosts through the Neighbour Discovery Protocol (NDP).

Internet connectivity based on the Internet of Things has grown to the point that everything in human possession, including watches, cars, and hospital facilities, among all work environments, can use it. Every single connection of these multiple devices requires its IP address. The insufficiency of addresses posed a significant threat to the communication of devices over the Internet. This results from a shortage in address space, an outcome of multiple device connectivity. A case in point is the digitization and automation of smart devices, such as washing machines, air conditioners, and televisions, among others in smart homes, which can be connected through IoT as such require an independent IP address to perform remotely based on the connectivity to the Internet (Dey,2016) - IPv4 cannot support such projections.

It was estimated that Internet connections reached 56.4% by 2012 (Internet Society, 2022). To better understand the depletion of IPv4, we see that its structure consists of 32 bits of address space equivalent to 4.3 billion Internet addresses, much smaller than Internet connectivity and users (Internet Society,2022).

As a solution to IP address depletion, researchers proposed a new IP protocol with a larger address space thus IPv6 that operates on a 128-bit address space and holds millions of IP addresses per millimetre square of earth's surface (Savolainen,2013). The IPv6 is equipped with other merits like improved network layer security, packet-forwarding efficiency, and quality of service capabilities; IPv6 has established itself as the most dominant Internet protocol used as it gives significant support to multiple addresses.

With the establishment of IPv6, it is clear that IoT devices are set off the roof and will increase drastically from this transition. However, the certainty of IPv4 address exhaustion is the primary

cause of the outcome (Al-Khafaji,2018). Over the years, this has called for IoT infrastructure to adopt the new norm of transition to IPv6. Besides, increasing IoT devices and connectivity increases security risks and privacy concerns.

Computers and usage were unfamiliar in the past because technology had not evolved. Moreover, the enormous prices to purchase computers and information with sensitive information were only exposed to a specific number of people, which seemed a threat. Hence, the objective was to trust the system to deny access to unauthorized users, as protecting physical computers was the principal security focus. However, as computers became less expensive and usage increased, we experienced a shift in the protection of computers to the safety of information in the computers (Samonas, 2014)

1.2 CIA (Confidentiality, Integrity and Availability)

The CIA model (Confidentiality, Integrity and Availability) establishes three significant roles in information security.Confidentiality encompasses setting privacy in data information, including people, devices and processes that permit and restrict access to sensitive information and deny access to authorized users.

The integrity calls for data safety including data in transition, process, and storage, to ensure that data and information cannot be modified or changed from their original form intentionally or maliciously. For example once a bank account digit has been changed or altered it changes the whole account and reads differently.

Availability guarantees that with all the cybersecurity mechanisms in place handling both hardware and software, people, and processes. Availability implies that information should always be available for access by authorized users. Information should be accessible at any time of need indicating that the system should have the tolerance to disaster recovery by increasing availability through zones that establish recovery and backup (Lo, 2017).

The objectives of cybersecurity are also focused on using AAA (Authentication, Authorisation, and Accounting) Authentication means proving that you are who you say you are, thus proving identity. Authentication requires proof like passwords or a key. However the combination of all these factors comprises multifactor authentication.

Authorization refers to providing accurate access that matches stored passwords or fingerprints based on the authentication approach. Authorization also manages the level of access per user. Various users' roles have different authorized access rights.

Accounting, which keeps track of what users are doing as they log into the system, is significant for forensic purposes as it provides digital evidence (Tech Target, 2023).

Consequently the project will establish the shortcomings in the system development life cycle in IoT devices, increasing the risk based on the transition to IPv6. The project will also look at the current security techniques proposed to establish privacy and security in technology and information security thus risk assortment frameworks.

1.3 Justification of the research topic

The rise of the Internet of Things and information technology has led to the evolution of new policies that govern the operations of businesses and society. As a result this thesis analyses the risks and opportunities associated with transitioning from the IPv4 to the IPv6 protocol.

Hence it will investigate the various vulnerabilities related to the network configuration of IPv4 and IPv6. It will also focus on identifying gaps in the security and migration processes. The study's main objective is to view the vulnerability landscape and identify potential solutions comprehensively.

1.4 Research significance

This study is relevant in implementing ISO frameworks for Risk management in IPv6 to create a likelihood of enhancing performance and achieving objectives for an organization. This improves identifying opportunities and threats and establishes the proper allocation of resources to handle related risks. However, it is significant to note that ISO frameworks are not a priority for certification purposes but act as a guide for internal and external audit programme. Organizations can evaluate risk management practices with internationally recognized benchmarks, providing strong principles for effective management and corporate governance.

1.5 Purpose of the study

The study aims to develop a proactive management strategy to minimize the risks associated with implementing IoT in the enterprise. The strategy will involve implementing various measures to maintain the system’s security. Implementing ISO frameworks has raised a bar for network perimeter security by minimizing the risks associated with technology. Effective risk management should occur from the project's inception to the maintenance and production stage.

1.6 Scope of the study

The scope of the study is mainly focused on establishing mechanisms that will enhance the security of IoT devices based on risk management in IPv6. This survey was focused on Information technology Infrastructure with an emphasis on the security of networks in general thus, this thesis mainly elaborated on the implementation of ISO frameworks to enforce proper security mechanisms against risks.

1.7 Research problem/ problem statement

Many organizations employ best practices and methods supported by an enterprise risk management framework to manage information technology risk. Despite these efforts security breaches occur in many organisations as the threat landscape has exponentially grown. Known or unknown there are new avenues for attackers and malicious individuals to exploit vulnerabilities in poor configurations of IPv6 and careless implementation of IoT. These are well accounted for in the work of Santa (2015).

1.8 Research aim and objective

1.8.1 Aim

This thesis aims to provide senior management, information technology and risk management teams and professionals with a preemptive approach to lower the risk of acceptable levels enhancing organisations to migrate to IPv6 and keep ahead of the IoT innovation wave while aligning these efforts with strategic objectives.

1.8.2 Research objectives

1. The objectives of this study can be seen below:
2. To assess the implementation of ISO risk management frameworks.
3. To enforce security measures in all phases of IoT
4. To formulate and develop a strategy to ensure compliance and governance
5. To conduct a survey on the implementation of ISO frameworks to risk management in IPv6

1.9 Research problem and questions

The research focuses on formulating and establishing strategies to enforce vigilance atop all the compliance best practices and risk management frameworks.

The research is conducted through a combination of qualitative and quantitative methods, which are complemented by the design science approach. The seven guidelines of the design science method are utilised for better outcomes. Open-ended interviews are also used for data collection. Various materials are included in the study such as books articles and websites and the results of the study revealed several factors that complement the implementation of the ISO framework to assess risk management in IPv6.

I. From the business perspective, how will IoT devices be used securely without creating loopholes for security risks?

II. On a scale of 1 to 10 how satisfied are you with IoT governance and Compliance? Would you evaluate room for improvement?

III. What are the major principles of implementing ISO frameworks to IPv6, and what are some challenges?

1.10 The research assumptions and limitations

In the study, the following assumptions were made, it was assumed that.

i. The participants in the study freely provided the researcher with ratings of significance regarding professional education competencies.

ii. The respondents based their ratings objectively on the importance of professional education competencies.

On the other hand, the study's limitations illustrated that the purposive sampling procedure indicated that the investigation is limited to ISO framework Implementation to risk management in IPv6.

1.11 Chapterization

Chapter one introduces the topic. It also details the justification of the report topic and the research significance. Additionally, it presents the purposes of the study and the research problem/problem statement. Furthermore, the research aim and objectives are stated in this chapter. The chapter also outlines the research questions and the research assumptions and limitations. The second chapter of the thesis provides an overview of the target system, which is IPv6, as it is compared with IPv4. The security and merits of this technology are discussed.

The third chapter provides an overview of the design specifications for the IoT, which will help generate ideas for a suitable solution. It also explores the various risks and security issues associated with the technology.

The fourth chapter of the thesis explores the various frameworks that are used to manage the risks associated with IoT. It also provides a framework for developing effective strategies to address these issues.

The fifth chapter explores the methodology used in conducting the research, including the research design, data collection method and analysis, among others.

The sixth chapter discusses the proposed IPv6 and the various processes required to prevent attacks and threats. It also provides a framework allowing users to perform surveys that can affect the current frameworks.

The concluding chapter of the thesis, the seventh chapter, summaries the project, with suggestions for the future and limitations set based on the research.

2 Description of internet protocol version 6

2.1 IPv6 overview

IPv4 became dominantly a used in the early days till today its being used despite being published in 1981 (Wu, 2012). The lesser competence exposed by IPv4 made it is clear that connectivity became challenging with the increasing number of users.It is defined that at least each host must have access to an interface on the network and uniquely noticed through a globally unique IP address. As a result the IP addresses were mostly consumed up basing on high volumes of connectivity and in the long run no more additions could be possible to the network. Research identifies that IPv4 has a limit of about 4 billion (4,000,000,000) unique addresses (Ibhaze,2020).The exhaustion of the 4,000,000,000 addresses can be said to be based on the growth of users and the lack of means to allocate address blocks during the distribution (Huston,2013). Thus, some clusters were allocated more than needed mostly in Europe and the United States. However, in reality IPv4 supports less than 250 million uniquely addressed nodes. With this shortage and demerit came IPv6 which represents significant availability and connectivity access based on a wider growth of the Internet till today. The introduction of IPv6 didn't mean the end for IPv4 as of today IPv4 still functions

In summary, IPv6 was a remarkable invention and the best opportunity for IETF to build a protocol. Nonetheless, the challenge related to the address space was merit to establishing IPv6 by IETF, thus, a more considerable extent to the development (Feldner, 2018).

2.2 IPv4 to IPv6

2.2.1 Merits of IPv6

IPv6 was established as a result of shortcomings from IPv4. Accordingly, the Internet Task force (IETF) developed a new suitable IPv6 to solve the error and weaknesses of IPv4. Consequently in June 2012 IPv6 was officially rolled out and many organisations started using it (Korusuz, 2012).

2.2.2 Sufficient IP address

With a lot of address space ISPs have more than enough IP addresses allocated to all dependants. As a result, every IP address has a unique identifying address. However despite the availability of a firewall, NAT was established as a technique to address shortages (Davies, 2012). As mentioned earlier, IPv4 was a 32-bit address, and the transition to IPv6 bit was a great milestone in the history of Ips and connectivity. Moreover, the substantial address opened to about 4.29 billion addresses

which were impossible with IPv4(Davies, 2012). Today, at least each individual can connect more than two devices to the Internet simultaneously. All devices connected have a unique Ip address and an address only identifies each device. This shows the sufficient Ip address space and storage used today, which was not the case with IPv4. Nevertheless it is significant to note that the difference in address and prefix notation is shown by 16-bit hexadecimal blocks hence

2001:0cb6:0000:0000:0101: a3ef: fe1e:5349

The comparison with IPv4 can also be seen based on the inter-domain routing the prefix identifier is based on the subnet and prefix length utilized at the end of the address post a slash.

2001: da8:1200: :/40

2.2.3 Business-to-business connectivity

Business-to-business connectivity requires unique unlimited connectivity shown and identified within NAT thus enhancing performance and reliability (Chelius, 2005).

2.2.4 Auto-configuration

To understand better, it is expedient to examine IPv4 addressing. Addresses are connected to devices automatically with a DHCP server. As a result more device connectivity becomes extremely expensive to manage and addresses running out. When it comes to IPv6 as it comes with SLAAC functions that enable devices to establish an IP address based on the network established by the router and host device (Villalba,2011). On the other hand, the MAC address is a randomized number that requires no DHCP server as a result management and network are much more simplified than in Version 4.

The auto-configuration for IPv6 can be categorised into two Stateful Auto-Configuration and Stateless Auto-Configuration. Stateful Auto Configuration calls for human interaction with DHCPv6 during the installation. The DHCPv6 stores a list of nodes and clusters with configuration information. It performs state information maintenance to enable the server to understand the time stamp for each address and when to reassign based on availability (Villalba, 2011). On the other hand, Stateless Auto-Configuration is based on small-scale organisations and individuals thus each host has an address identified from the form of content transmitted by the router and uses the IEEE EUI-64 standard to establish a network identity for the address. Despite the state of address identity

the nodes must verify the potential of an address to a local link through a neighbour solicitation message to the intended address. Moreover once the nodes pick up any response it understands that the address is in use already and therefore establish another (Morabito, 2017).

2.2.5 Deletion of network address translation tables for local devices

Previously NAT tables were implemented in IPv4 routers to create addresses to local and private simply because addresses in IPv4 could not be used for public Internet (Morabito, 2017). Hence NAT was also used to implement a slower usage and exhaustion of addresses exposing and connecting multiple devices to one global IP address. As a result this is a major factor in the slow adoption of IPv6 (Elmore,2008). Nonetheless establishing IPv6 has eliminated the use of NAT tables by using end-to-endpoint connectivity enhancing internal devices to connect directly with the outside world (Oliveira, 2011). The reverse is applicable simplifying routing efficiency and costs (Oliveira, 2011).

2.2.6 Enhanced mobility

From MIPv4, network entities were introduced where HM is responsible for MN reachability while on the Internet and within the same identified domain and safe of the mobility information. Conversely the foreign domain assigns a temporary address to the MN as information comes in and CN the mobile host keeps static and mobile nodes in communication with MN (Nikander, 2010). However as a result of IP address depletion IPv6 comes in proxy Mobile IPv6 and the major purpose is to ensure that all mobility-related signalling messages are enhanced between mobile nodes (Leu, 2015) and HA host-based protocols that maintain all hosts within a mobile network accessible through a permanent address.

2.2.7 Simplified header formats

Among the many deficiencies of IPv4 was the complexity of the headers. Consequently, its continuity would have led to establishing a bottleneck corresponding to the depletion of addresses. Research shows that the IPv4 header comprises 10 fields; hence, the two 32-bit address fields and the option field bring the header to the correct value length (Morton, 1997). Without the option field empty, the IPv4 header is 20 bytes long, illustrating that the IPv6 header with 80 bytes was inapplicable. IPv6 introduced a mechanism that combines headers; hence IPv6 consists of 6 fields and the two 128-byte addresses basically for origin and destination without option fields

“The simplest IPv6 header is still only 40 bytes long- or double the size of the IPv4 header without options even though the two addresses it incorporates are four times the size of the IPv4 header.” (Morton, 1997)

2.2.8 Improved support for options and extensions

IPv4 defines clustered opinions to the root header. However IPv6 contains options in extension headers that are only used when needed and, as a result, enable faster packet processing. This is facilitated by the definitions of six extension headers, including routing, Mobile IPv6 level of service, and security (Hagen, 2006).

Some misconceptions about IPv6 can often be judged from the above-mentioned advantages. Below are some of the misconceptions affecting the adoption of IPv6 adoption.The background of IPv6 exposes a risk to current IP infrastructure including networks and services. To clarify it is significant to understand that the major objective of IPv6 establishment was to bring about integration mechanisms that let both protocols co-exist. As a result, one can implement both IPv6 and IPv4 independently and in the long run the co-existence establishes a dominance of IPv6 (Hagen, 2006).

The assumption is that IPv6 is non-competent in performance compared to IPv4. However IPv6 has been implemented in most routers and operating systems for over 10 years and has been tested (Fred et al.2015). Among other mechanisms is under the Moonv6 operated by the US Department of Defence basically to perform tests for IPv6 among establishing mobility and security as seen among the advantages (Marsan, 2006). Accordingly the tests performed at Moonv6 prove that IPv6 has a strong foundation for stability and performance.

The costs of running IPv6 are expensive. Therefore it is certain that costs get higher in maintaining IPv6 than IPv4 thus new networks find IPv6 support in current network infrastructure as high and expensive (Waddington, 2002). Regardless it is significant to note that to a larger extent all newer things are established incur. The introduction of IPv6 to an organisation calls for sensitization of users, and IT staff, integration processes and yet all are to be performed at the cost of an expert.

The moment that stage is passed the costs related to IPv6 get cheaper to manage and maintain. Nevertheless IPv4 networks are complex especially with new technology trends such as video conferencing increasing layers of complexity. NAT has established more mechanisms and solutions to enable cost management which cannot be enforced in today’s world of IoT. Consequently IPv6 proves more cost-effective than IPv4 in the long run.

With the establishment of stateless autoconfiguration, users cannot control and monitor network access. It is important to note that administrators will have a level of control based on choice despite the stateless autoconfiguration. DHCPv6 is shown as RFC 3315 which can support two operation nodes, thus stateful and stateless (Bound et al.2003). Stateful mode is more familiar with IPv4 in which the DHCP client sends a request for an IP address and configurations from the server. Stateless mode on DHCPv6 operates by requesting a configuration. Subsequently the server will obtain the IPv6 address and the configurations of IPv6 networks use DHCPv6 for address assigning which operates as a security feature hence authentication.

ISP offers no IPv6 services so we cannot use it. Nonetheless it is not to the ISP to transition you to an IPv6 network but rather the need to connect to the global IPv6 Internet through a transition mechanism and adopt IPv6 over IPv4 infrastructure (Singalar, 2018).

Lastly the concept that we have enough IPv4 addresses does not need IPv6 and having enough IPv4 addresses requires no immediate upgrade. However it is wise to avoid problems before they happen. Prevention is better than quire. Ignoring IPv6 for the existence of IPv4 assumes complete isolation of the network from the rest of the world which is not the case. In addition the organisation's growth means more devices and address storage are required. From history it is known that IPv6 adoption has existed in Asia for longer than in the United States, which means that despite the existence of IPv4 address storage, incorporation with other organisations from Asia for example is a huge obstacle for business operation and efficiency (Nikolina, 2022)

2.3 IPv6 risks and security measures

Given the similarities between the attack vectors used against the previous generation of Internet protocol and the new generation, many risks remain (DeNardis, 2006). Among the risks involved include the following;

- The introduction of rogue devices into their networks: These can be devices not authorized by the network owner, such as a router,wireless access points, a switch, or a computer. Implementing a device authentication framework such as IPsec to minimize this issue can help prevent unauthorized access (Javaid, 2018).
- Sniffing Attack: A typical sniffing attack is carried out by capturing the traffic in transit, allowing the attacker to access the sensitive information the network is trying to collect (Anu, 2017). By implementing an IPsec implementation, this can be done away with.

- Denial of service attack: This type of attack can be described as a malicious attack on a network structure to cause the server's unavailability. The attacks are usually caused by sending millions of requests to the server with the objective of slow performance flooding traffic to the sever invalid data and requests with invalid spoofed IP addresses (Elleithy, 2005)

- Man-in-the-middle attack: Keeping data in motion secure and private is a huge threat caused by this type of attack as they are performed remotely with fake addresses. Similarly with communication comes the problem of man-in-the-middle attacks, which affects the security network and the involvement of intruders (Maurizio Aiello,2014). However encryption has been established to control and prevent man-in-the-middle attacks. Various forms of encryption are available today including asymmetric cryptography.

- The application layer attacks: These kinds of attacks occur by exploiting loopholes in protocol implementation and designs and secrecy in the definition that targets given applications to individuals (Tripathi, 2021).As a measurement of encounters it is significant for the cyber world to prepare DDoS response plans. Therefore incident response plans and mechanisms and ensuring continuous business growth improved network security thus entanglement of smart firewalls and honeypots and established server redundancy.

Hence IPv6 comes with various risks related to the Internet and its usage however a well-established security and incident response layout should be established.

2.3.1 Protocol security

Adopting the IPv6 security protocol has established a threat based on the protocol itself. Prior to IPv6, IPv4 had no protocol threats. This is because the IPv6 protocol headers and protocol behaviour design differ entirely from IPv4.

2.3.2 Fragmentation attacks

Fragmentation attacks occur due to IP datagrams being compressed to smaller packets sent across the network and later re-established as the original datagrams based on communications hence the attack. Among the newly established features of IPv6 are improved headers which have been added to offer support as backup thus positioned between the IPv6 header and upper-layer header (Atlasis, 2012). This implies that packet fragmentation can eliminate firewall rules and principles. Consequently the fragment offset value sets the offset to the next packet and overwriting data and TCP for the first packet (Teq-faq, 2023). In summary when a large number of small packets are sent,

they result in overload, which causes buffering directly to the targeted system, leading to denial-of-service attacks. Cryptographic techniques like IDS and temporary node private addresses are recommended to solve fragmentation attacks.

2.3.3 Routing headers

IPv6 routing headers are called to process routing headers, and the characteristic of the header routing poses a risk to the security of IPv6 as it grants access to intruders to send packets to mostly publicly accessible addresses using a foreign routing header. In return, the host sends the packet to the destination address.

2.3.4 ICMPv6 Misuse

The concepts of neighbour discovery and path maximum transmission unit depend on ICMPv6 notification. Similarly it permits failed incidents to be cast back to the multicast addresses. The security loophole exists, and the attackers take this opportunity to exploit it by sending false packets to the multicast address resulting in various responses to the victim (Jong Hyuk Park and Hsiao-Hwa Chen, 2009). This attack can be controlled by denying responses to messages sent to multicast addresses (Durda, 2009).

2.3.5 Mobile IPv6 attacks

MIPv6 is an IP-layer protocol that enhances mobility performance in all layers. However with the Internet structure that lacks trust between users the security of mobile IPv6 is equally at risk since Mobile IPv6 architecture is based on the general operation of IPv6 including configurations of NDP (Nikander, 2004). BU messages payload packets and prefix discovery may cause the threats (Aura, 2006). As a result research has shown that BU is used to establish location (Aura, 2006). In the long run, mobile IPv6 attacks can result in connection hijacking, where malicious codes are published by sending false messages and assume origin from the outside network creating that connection, further enabling attackers to monitor connections prior to hijacking. Figure 1 illustrates connection hijacking because of mobile IPv6 attacks.

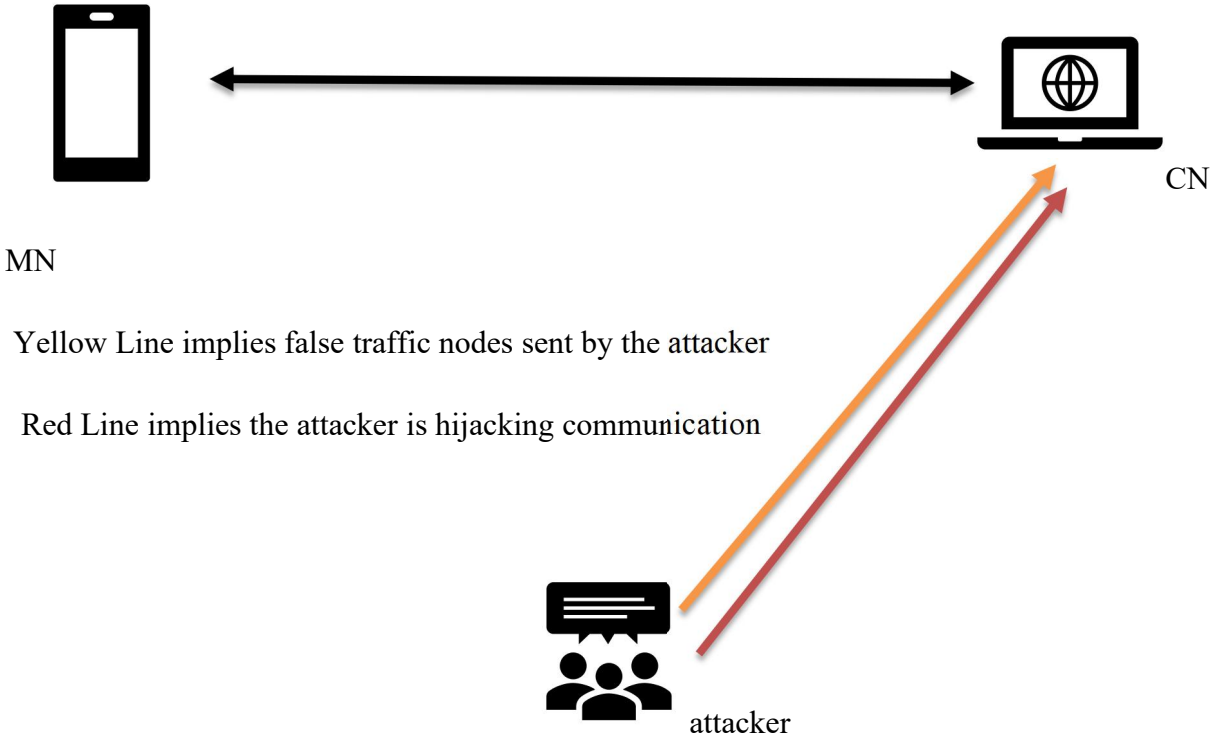

Figure 1 Connection hijacking (MN, Mobile node),(CN, Corresponding Node).

2.3.6 Address auto-configuration and NDP attacks

The IPv6 Neighbour Discovery Protocol NDP is used for auto-configurations by connecting systems to local links and accessing a network prefix node.

NDP messages are unencrypted, which exposes stateless address auto-configuration to attacks like spoofing.

2.3.7 IPv6 protocol stack attacks

As the number of networks using IPv6 continues to grow, it will become more likely that malicious individuals will try to take advantage of this new technology. There are still many bugs that are not yet discovered in the code that will be used in the networks as we transition to IPv6 (Barker, 2013)

2.4 Security deployment

2.4.1 Management of IPsec and security key

As the number of networks using IPv6 continues to grow, it will become more likely that malicious individuals will try to take advantage of this new technology. Many bugs are still not yet discovered

in the code that will be used in the networks as we transition to IPv6. IKE facilitates the process of establishing an IPsec key. Multiple configuration options can make it difficult to negotiate the parameters needed to secure the traffic flow in an IPv6 network. Hence both nodes must have the options to support secure end-to-end communication (Cho, 2004).

2.4.2 Dual-stack

Both IPv6 and IPv4 can coexist on the same networks and devices. In this case the devices should only be configured in one of three states thus IPv4 only, IPv6 only, or both. All configuration options including those for DNS and DHCP are available in the three states. A dual-stack network can help smooth the transition from IPv4 to IPv6 by allowing applications to run seamlessly. It does not require the use of tunnelling or protocol translation. The cost of running dual-stack networks is typically higher than running one protocol (Aravind and Padmavathi,2015). In addition to the management costs the complexity of the migration process also comes with training and additional hardware required to support the load. Most small enterprises require a complete migration to IPv6 on a scale-out basis.

Many devices and operating systems ready to go by default with IPv6 are vulnerable to exploitation by attackers. This is because the security policies for the new protocol are not well-defined and implemented. An attacker can take advantage of this vulnerability by sending out a router frame that will allow them to access the target network's resources. After the DAD procedure is performed the attacker can collect all the network details. If the users and administrators are not aware of the security policies for IPv6 before its migrated they can easily open their networks to threats. To prevent this the security policies must be adequately enforced. One simple way to prevent this issue is by implementing a personal IPv6 firewall on hosts (Aravind and Padmavathi, 2015).

2.4.3 Security transitioning

Due to the incompatibility of Internet Protocol version 6 (IPv6) and Internet Protocol version 4 (IPv4) IT departments must develop strategies to transition their networks. This process can be carried out step by step. Even though your ISP is still using IPv4 it is still possible to migrate to IPv6 while they are still running. There are various ways to make the migration happen and each organization should develop a strategy that fits its requirements.

2.4.4 Tunneling

The term tunnelling refers to the process of moving traffic between an IPv4 network and an IPv6 network. This is ideal if your ISP still uses the older protocol version and you have legacy equipment. It involves moving the IPv6 packets from one network island to another. Various mechanisms can be used to perform this, such as the Teredo, 6to4, and ISATAP (Zagar, 2007).

An attacker can control the traffic route between an IPv4 network and an IPv6 network through a tunnel sniffing technique. They can also perform man-in-the-middle attacks by spoofing the source and destination addresses of the packets. If an endpoint accepts the IPv4 packets without verifying they are from the correct address, the hacker can send all IPv6 traffic on the network. This method can lead to a denial-of-service operation as the attacker can send spoofed packets to a potential victim without receiving a response (Zagar, 2007). Tunneling administrators should enforce rules similar to those for IPv4 to prevent unauthorized network access. One of the most effective ways to do this is by implementing a Unicast reverse path forwarding solution. This method blocks traffic that's sent and received from a spoofed IP address. It can also prevent the encapsulation of 6to4 packets. Another effective method to prevent unauthorized access to a network is by implementing an IPsec tunnel. This method adds a variety of authentication,confidentiality and integrity mechanisms to the communication (Abdallah, 2018)

2.4.5 Translation mechanisms

NATPT is a process used in networks to map private IPv4 addresses to the Internet-facing address of the public IPv4. Translation in IPv4 has contributed to the reduction of the address space and it is a contributing factor to the laziness of many enterprises when it comes to adopting IPv6 since it allows only the nodes that are IPv6 to communicate with each other. As a transition mechanism, it is now being used to allow nodes that are only IPv4 to communicate with those already IPv6 by translating packets into IPv6 using a translation gateway (Armitage, 2002). One of the biggest issues that NATPT faces is its end-to-end IPsec breakdown. Because of the security advantages of IPsec, it is not possible to create a tunnel between the nodes that are only IPv6 and the ones that are only IPv4. All traffic must be unencrypted and transparent to ensure that the ALG performs its duty. When this happens, all DNS Security packets' signatures are invalidated, rendering them unusable.

In addition, NATPT can expose the hosts to attacks by depleting the pool of addresses in the server which can be done through spoofed packets. As a result various mechanisms can be used to prevent the depletion of the pool such as using an IP source guard. This can be done by implementing rate

limiting on the gateway device and strict anti-spoof rules (Srisuresh, 2001). By depleting the server's pool of addresses using spoofed requests NATPT exposes hosts to DOS attacks. It can also overwhelm the ALG with requests that need inspection. To prevent this and to counter the attacks caused by denial of service, a technique known as rate limiting can be utilized on the gateway device.

2.5 Prevention mechanisms

2.5.1 Firewalls and intrusion detection in IPv6 network

Similar to how they are in IPv4, firewalls are essential in an IPv6 network. They can block traffic from external and internal networks but they can also be used to restrict access to specific network portions. Since the header of IPv6 is different from that of IPv4 firewalls should have separate rules for it. Various types of firewalls can be used to protect an IPv6 network and filter different types of traffic.

Multicast and site-local addresses at the perimeter are required to address the risks of unauthorized access and manipulation of the network. They should also be utilized to block services and prevent spoofed traffic. In addition event management logs should be stored for analysis to identify malicious activity (Bhatt, 2014). In addition to blocking and preventing unauthorized access an IDS is also required to monitor the network's activities and identify potential threats. This type of system is usually a software or hardware device used to analyse the events happening in the network. To perform its function an IDS should be able to recognize the different types of packets sent and received by the network (Depren, 2005).

Contrary to popular belief, the next generation of Internet protocol, IPv6, is less secure than its predecessor IPv4. Although it is more secure in some cases it is less secure in others. As a result it is still important that the various devices and functionalities used to implement the new network are designed to secure and enforce best practices. Due to the relatively new nature of the technology there is a shortage of experienced and trained individuals who can properly defend and deploy IPv6 networks (Caicedo, 2009).

3 Internet of things

3.1 IoT overview

The Internet was first created during the late 1960s to early 1970s. During this period, various technological advancements have allowed organizations to improve efficiency and reach out to customers more effectively. Some of these include the development of e-commerce and the ability to customize products (Porter, 2001).The Internet has many advantages but it also has disadvantages such as allowing malicious individuals to carry out their illegal activities online. Despite the various advantages of the Internet enterprise management professionals have to asses the risks and impact and respond accordingly and as a result more organizations have adopted internet continue to reap its benefits. The Internet of Things is a technological revolution expected to have a huge impact on how we live and work. It involves the creation of a network of devices and embedded computing hardware.

The Internet of Things concept goes beyond traditional computers and the connection of various devices such as cars, buildings, and light fixtures. Like the Internet, there are still risks associated with this new technology.

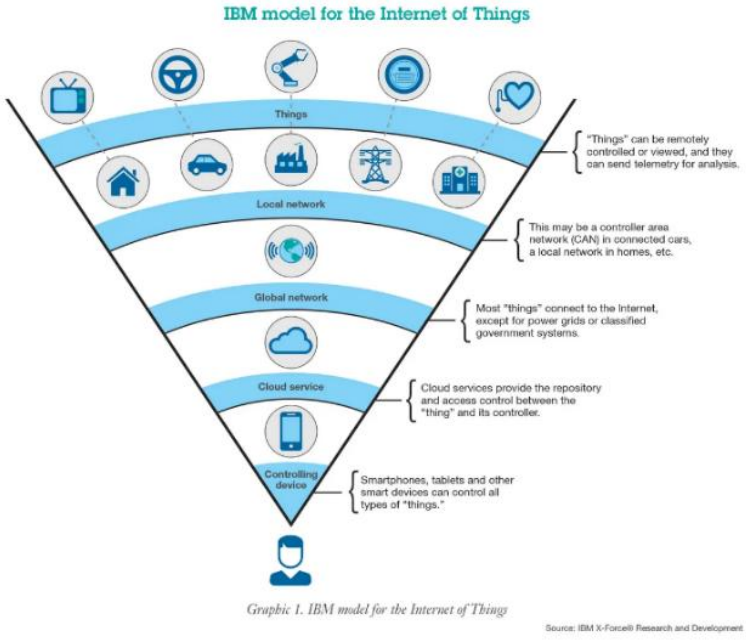

Image 1 IBM model for Internet of things (Porter, 2001)

The concept of the Internet of Things was first proposed in 2005 by the ITU. In 2008, it was suggested that the networks of sensors would eventually become ubiquitous. The IoT features

various communication protocols such as 4G LTE, RFID and Zigbee. Ideally a single protocol would allow for a unified and easy-to-use application platform while simplifying appliance development. The development of IoT applications is expected to benefit from the availability of IPv6 (Suresh, 2014). The Internet of Things (IoT) is a new dimension in the telecommunications industry that brings forth a new level of connectivity. It allows objects to talk to each other and with people at any time. This new dimension has the potential to improve the efficiency and quality of various businesses.

3.2 Propositioning and Values

A system consisting of animals machines and objects has a unique identification and computing power to transmit data over a network. Since computers rely on humans to generate information, humans' limited accuracy and attention span make data capture difficult (Hudson, 2017). The rise of the Internet of Things (IoT) has created new opportunities for organizations to collect and use machine-generated data to improve efficiency and reduce waste. Some of these include the military public safety retail stores transportation and agriculture. Collecting and using IoT data has tremendous value for businesses as it allows them to make more informed decisions. Due to the increasing need for timely information companies have started investing in data analytics.

With the help of data analytics, companies can make more informed decisions and improve their efficiency. This can be done through various operations, such as supply chain management and production planning (Uslu, 2019). The ability to monitor a person's health or a certain appliance from their smart phone is just one of the many benefits of the Internet of Things. Due to the vast number of innovations that are related to the IoT it is not feasible for any company to develop an end-to-end solution (Alli and Alhasaan, 2022).

3.3 IoT architecture

Even before we knew the term Internet of Things, we already knew how to associate it with various objects and technologies. Some of these include bar codes RFID tags and infrared sensors. The IoT is a functional and growing network that can be divided into three following different entities;

3.3.1 Network infrastructure and gateways

Most Internet of Things (IoT) devices currently not designed to connect to the Internet are not equipped with the necessary hardware to operate properly. This is why gateways are necessary. They allow devices to establish interoperability between their networks and the Internet. Besides

providing a secure and easy-to-use environment, gateways also help prevent unauthorized access to their data (Do, 2019).

The IETF has created the Mobile IPv6 standard, which provides a node with a feature to maintain connectivity while travelling. The protocol is designed to be transmitted over low-power wireless LANs (6loWPAN). The end-to-end wireless protocols used for transmitting information between nodes make IPv6 an ideal communication standard for the Internet of Things (IoT). The backbone of the ecosystem is composed of routers, switches, repeaters, and other equipment involved in the network's communication.

3.3.2 Remote application and cloud infrastructure

Instead of buying expensive server farms organizations are now adopting cheaper cloud computing solutions to store and process the data generated by their IoT devices. These solutions act as an out-of-the-box repository that can handle the big data the devices collect.

The application layer is the top of the cloud computing stack where the data collected by the devices is then processed and presented to the relevant individuals through various channels. This includes web servers mobile devices and desktop applications.

3.3.3 Sensing things

Things are devices or objects currently being used in various industries or households. These can collect and interpret current information or send it to other intelligent systems for processing or analysis. The characteristics of an IoT device should be reliable secure easy to maintain and safe. These are some of the factors that are considered when it comes to choosing an appropriate type of device. Besides being able to operate efficiently in remote locations IoT devices also need to be energy efficient. An 8-bit system-on-a-chip (SoC) controller is the smallest type of device. An example of this is an Arduino board.32-bit chips from Atheros and ARM support various features such as OpenWRT a miniature version of Linux (Laghari, 2021)

64-bit and 32-bit hardware platforms are also available that can run various operating systems such as Linux. Examples include the Raspberry Pi and the open-source project known as the Beagle-bone. The various phases of an IoT device's life cycle are known as bootstrapping operational and maintenance. The first stage involves establishing a secure and trust relationship between the device and the network. Maintenance involves regularly updating and adding new features to the device's software and applications. This period usually lasts until the device's end of life. IoT devices' design

ensures that they constantly interact with the environment they're being used in. They need to meet certain real-time constraints to respond to events. These devices can be hybrid systems with analogue and digital components (Singh, 2020).

When connecting to the outside world, IoT devices' use internet protocols and The different technologies have unique advantages in terms of power consumption, range and bandwidth. Figure 2 shows IoT architecture that involves a network that is responsible for connectivity and converting information into data analysis from sensors. Platforms include firewalls under the Gateway layer with a main role of filtering traffic and lastly the device like computer, smartphones and house, cars that are connected to both networks and platforms for performance, devices are at a wide range the those listed above are just a few among the many.

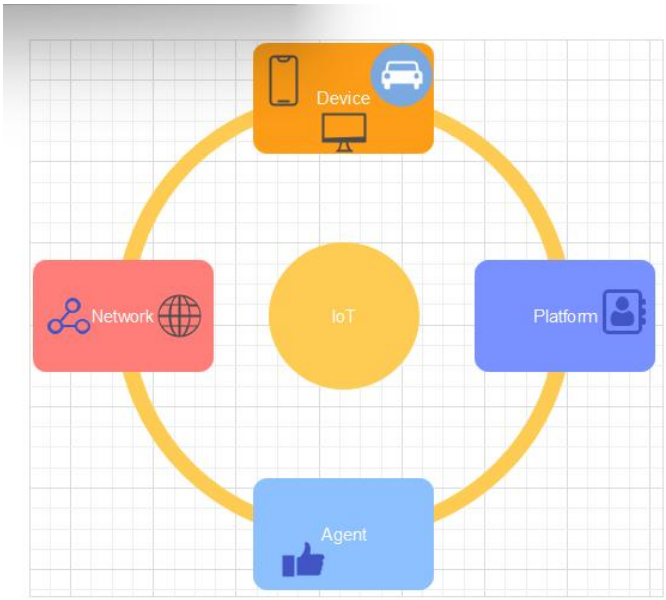

Figure 2 IoT System and architecture

3.4 Insecurity of IoT

The availability and authenticity of data is the most critical aspect of an organization's operations. It can be hard to make informed decisions without the proper security measures. The Internet of Things (IoT) is the primary source for all the data that an organization collects, but most devices are not built to provide the necessary security (Barcena, 2015).

Various organizations can take advantage of the IoT threat landscape such as stealing data from a competitor orchestrating corporate espionage or even launching attacks on an enterprise. The

situation's complexity and the risks associated with IoT should be acknowledged and analysed to provide a comprehensive view of the potential consequences for businesses.

3.5 Functionality risks

When securing the networks of embedded Internet of Things devices, they must have a triple-A authentication mechanism. This includes having the necessary personnel authorized to access and configure the devices. These three-factor authentication mechanisms help ensure that the devices are secure. They also keep track of the user's activities and provide accountability not available in other systems. These implementations can be embedded in devices if the security is thoroughly woven into the development cycle (Lee, 2020).

Unfortunately, implementing an authentication system in IoT devices can be very challenging due to the number of keys required to be distributed. This can lead to various issues, such as man-in-the-middle attacks.

Although the requirements for securing the data from IoT devices are usually met by encryption, many of the technologies used for this security do not support strong enough levels of encryption. Also, rogue devices can be used without the knowledge of network administrators and system engineers. These risks can lead to the unauthorized access and storage of data.

3.5.1 Technical risk

The security challenges associated with the Internet of Things (IoT) are numerous. While they are not as vulnerable to attacks as traditional IT infrastructure, they face various threats. The increasing number of linked devices and the lack of transparency around their administrative oversights make it difficult to manage the security risks associated with IoT. One of the most common vulnerabilities that criminals can exploit is the vulnerability in a wireless baby monitor. In 2009, hackers accessed the device and taunted the parents using it (Scheifer, 2015).

Dealing with compromised systems can be very time-consuming and challenging. Implementing a software upgrade is one of the most common steps to address these issues. However, this method can be very time consuming and difficult to implement on mobile devices due to their users' preference for postponing updates. In 2009, Chrysler was forced to issue a recall after hackers accessed its digital systems. Toyota also had to recall millions of cars due to various issues (Ahsan, 2013). The cost of these incidents can be substantial. Besides implementing a software upgrade, it is also important that personnel and administrators have the necessary tools and resources to respond

to these types of incidents. One of the most effective ways to address these issues is by establishing a security management framework to monitor and prevent data leakage (Brass, 2021).

3.6 Business risk

3.6.1 Cyber-attacks with financial prospects

One of the world's largest medical device companies is St. Jude Medical. Its stock price took a nosedive after MedSec, specializing in medical devices, discovered multiple product vulnerabilities. The company decided not to inform SJM about the security issues, opting to negotiate with a short seller activist, Muddy Waters. After gaining access to SJM's internal networks, Muddy Waters proceeded to launch attacks against the company's products. These actions resulted in a major stock price loss. The rise of IoT insecurity has highlighted how vulnerable organizations are to attacks (Tomaiko, 2021).

3.6.2 Privacy of data

The concept of privacy is a fundamental part of the information era. In this context, the Internet of Things (IoT) allows users to monitor the activities of their female hygiene products through an app. This type of invasiveness raises questions about the privacy of individuals. What happens if a device is compromised and the owner's data is collected? Do they have the necessary safeguards in place to protect this information? This is just one example of the many questions that arise when it comes to protecting the privacy of individuals using the Internet of Things (Rosas, 2019).

To protect users' privacy, legislation must be enacted to prevent unauthorized access and use of their data. The Health Insurance Portability & Accountability Act of 1996 (HIPAA) (ACT, 1996) is one of the most important laws that can protect patient information's confidentiality. Other important laws that can help protect the privacy of individuals include the Electronic Communications Privacy Act and the Children's Online Protection Act. However, if these regulations are not enforced across the network hackers can still take advantage of them. For instance, if a CAT scan device is on the same network as a thermostat,it can still comply with HIPAA regulations even if it is not.

3.6.3 Sovereignty of data

The concept of the sovereignty of data refers to the idea that the data collected on a server farm is subject to the laws in the country where it is stored. However, enforcing privacy laws is the most

important concern when protecting the data. Due to the rise of the Internet of Things (IoT) and the increasing number of governments implementing regulations regarding data storage it is now more important than ever that the data collected by a cloud provider is kept in the country where the customer is located. However, this is still not always possible due to unreliable information (Amoore, 2018).

3.6.4 Data fidelity

The concept of cognitive hacking refers to a cyber-attack that aims to alter a person's or machine's observed behaviour in response to a given situation. This can be done through the manipulation of data that is collected from a machine or human. Data can be manipulated to be partially true or completely true, but in an irrelevant or misleading context. The rise of the Internet of Things (IoT) has raised the issue of how senior management can rely on the data collected by devices to make informed decisions. This is because the data collected by these devices can be manipulated by malicious actors (Jung, 2014).

3.7 Oasis initiative: MQTT

The goal of the not-for-profit organization Oasis is to provide a framework for developing and consolidating open standards related to the interoperability of products using the Generalized Markup Language (GML). Since its inception, the organization has expanded its scope and standardized the messaging transport protocol known as MQTT. This simple and lightweight protocol is designed for low-bandwidth, high-latency devices commonly used in the IoT. The protocol provides a variety of capabilities for establishing and managing client-server relationships, such as naming and authentication. Although it does not provide encryption, it can be used to address the issue of confidentiality by implementing SSL. This is currently being supported by the Amazon Web Services IoT platform (Firdous, 2017).

3.7.1 ITU Internet of things GSI

In 2016, two recommendations were approved by the ITU to establish a global standard for the Internet of Things (IoT). These recommendations aimed to create a unified framework for developing IoT applications (Kafle, 2016). By implementing these recommendations the ITU was able to help service providers establish and use IoT services in their networks. The research initiative also laid the foundations for a new study group focused on developing applications for smart cities. The ITU released a series of technical reports in support of these recommendations.

These reports cover various aspects of security and management for the IoT. One of these is a draft report that aims to provide a comprehensive analysis of the security capabilities needed to protect the safety of the IoT.

3.7.2 IEEE

IEEE released the 802.15.4 standard in 2011 for low-rate wireless networks (WPAN). This communication protocol is used for various IoT devices, such as those from 6loWPAN and Zigbee. It features a layered architecture that allows for higher-layer services. It also protects from man-in-middle attacks. The IEEE has been developing a standard for addressing and sequencing the media access control (MAC) sub-layers. This standard will be used in various applications that require high precision ranging (IEEE, 2016).

The proposed protocols for securing the communication between nodes in the wireless sensor networks and Internet hosts are shown in Table 2. The Sizzle architecture uses the SSL protocol to establish a gateway that can terminate connections. Unfortunately, implementing this protocol does not ensure end-to-end safety since it requires a gateway to translate the SSL message on the Internet to a specific sensor network protocol. SNAIL uses a lightweight version of SSL instead. Although the SSL protocol is generally used for secure communication, it requires an end-to-end solution to implement it. The Sizzle and SNAIL implementations use the Elliptic Curve digital signature algorithm for authentication and key exchange (IEEE, 2012).

	SSNAIL	Sizzle	ContikiSec
Authentication	ECDSA	ECDSA	CMAC
Key exchange	ECDH	ECDH	
Key size	160	160	128
Data Encryption	RC4	RC4	AES
Hashing	MD5 SHA1	MD5 SHA1	CMAC
Access control		Gateway	
Network operation	SSL	SSL	Link-layer
Gateway Usage	No	Yes	No
End-to-end Security	Yes (SSL)	Yes (SSL)	No

Table 1Advocated security for high-layer WSN.

In addition to the SSL protocol, IEEE released the 802.15.6 standard for low-power wireless networks designed for human presence. This standard is built on the recommendations of medical professionals to ensure that the safety of the users is maintained. The WBAN is a high-quality wireless network that supports both the security and quality of service standards (IEEE, 2012).

3.8 IETF Initiative

3.8.1 RFC 4919 and RFC 4944

The IETF's proposed standards for transmitting Internet Protocol packets over sensor networks made it easier to implement the technology. The standards provide information about the various steps involved in transmitting packets over the networks of IEEE 802.15.4 and 802.15.6 (Tjensvold, 2007).

Although the security features of the networks already in use by IEEE are not changed, the various standards related to this area have been updated to address users' security concerns. Some of these include the implementation of trust models and the threat landscape.

3.8.2 RFC 6550 RPL

Lossy and low-power networks are defined as networks characterized by the constraints of their endpoints and routers regarding their processing power and memory. Meanwhile, the RPL is a framework that addresses these issues. It features three security bootstrapping options that can be utilized to implement effective security measures (Brandt, 2012).

When other security measures are implemented, such as link layer security, the RPL can use an unsupervised mode to send messages without a security section.

The preinstalled mode provides integrity and confidentiality, which is ideal for sending and receiving messages. A node must have a key to join the RPL network as a router or host.

The authenticated mode provides a level of confidentiality and integrity that is ideal for sending and receiving messages on the RPL network. It requires a second key that can be used to join the network as a router.

These are also useful when the IoT devices are not from the same manufacturer. They can help ensure that the security parameters are transferred between the nodes.

3.8.3 RFC 7252 CoAP

The lack of resources in the TCP-based HTTP protocol is considered a major issue when implementing IoT networks. A better alternative is the CoAP a client-server protocol designed to provide a low-cost and simple way to transfer messages between applications. It is ideal for networks characterized by constraints (Shelby, 2014).

3.8.4 RFC 6347 DTLS

The DTLS protocol is a secure transport layer that protects messages and datagrams from eavesdropping and other attacks. It works with various server applications, including CoAP.

3.8.5 Global standard 1

The development of the bar code led to the establishment of Global Standard 1 on the standardization of coding methods. This standardization aims to provide a common language for businesses and organizations to share information about their physical entities.

3.8.6 Electronic product code

A physical object can be identified by using an electronic identification system known as an EPC. The GS1 standard version 2.0 added various security features to protect consumers' privacy. These include using tags to combat counterfeiting and anti-theft systems (Brock, 2001).

3.8.7 ONS standard

The Object Name Service was first released in December 2012 and officially ratified in January 2013. Like the Domain Name System, ONS handles routing, identification, and object naming requests. It relies on the DNS to process requests and handles requests in different regions and countries (Mockapetris, 1988)

3.8.8 Observations

The dynamics of mobility and the risks associated with device security are some factors that affect the risk landscape. In addition to physical security, we also need to consider the various aspects of device management. For instance, how do we ensure that users are aware of their privacy and manage the multiple vulnerabilities in their devices? One of the most critical factors that affect the

security of the Internet of Things is the limited resources available to the devices. This is because the lack of memory, processing power, and energy consumption can prevent the design of end-to-end solutions to provide secure and resilient connectivity. Even the existing solutions that are designed to address these issues need to be interoperable.

Businesses should be assured that their IoT manufacturers have the necessary security measures in place when developing their products. Unfortunately, many people responsible for the design and implementation of the Internet of Things do not consider the security of their devices when it comes to their work. Even though the chapter covers the various initiatives aimed at improving the security of the IoT, the speed at which it becomes prevalent still exceeds those of cyber security.

4 Risk management specifications

4.1 Overview

Over the years, organizations have adopted various strategies to manage their uncertainty. The ability to handle unforeseen events has become a critical part of their operations. Risk management is an essential part of any organization's strategy whether it is a start-up or a multinational corporation.

The failure to manage risk can lead to catastrophic events such as the 2008 global economic recession. As the rise of technology and the increasing number of people using the Internet of Things have raised concerns about privacy and security, risk management should be considered a core component of any organization's operations (Lee, 2020).

The concept of risk refers to the potential damage or loss caused by a given threat to an organization or its assets. Assets are often considered valuable to an organization, but they may not always be tangible. Another term that should be considered is vulnerability an external or internal weakness an organization can fall victim to.

This should not be confused with the role of risk governance which is the responsibility of the board of directors and the executive management. It is the alignment of the risk strategy with the organization's objectives.

Risk and probability are also used to describe the likelihood of an event and the impact it will cause. Risk is typically calculated based on the impact and probability of the occurrence.

$$\text{Risk} = \text{Probability X Impact}$$

As organizations try to realize the value of their information technology investments they face increasing risks associated with the projects. This is why all the departments must be aware of the risks involved in the project. Despite the increasing number of initiatives related to technology the success rate of these projects is not good. According to an analysis of over 50 IT projects over half fail to achieve their goals (Benaroch, 2002). The reasons for this are various such as the lack of skilled personnel, inadequate resources and scope creep. The uncertainty surrounding the Internet of Things also contributes to this failure rate.

Another common reason for the failure rate is the lack of proper project management techniques. This can be attributed to the improper use of risk-averse principles. The project should be considered as a whole to determine the appropriate link between the project's goals and the company's strategic objectives. A structured process or charter is necessary to manage the risks associated with a project. This process should help the various departments identify the appropriate ways to approach these risks. According to RISK, an enterprise risk management strategy should involve a multi-disciplinary approach (Lam, 2017).

A strategic business discipline aims to support an organization's overall goals by managing the multiple risks it faces.

The increasing number of technology-related initiatives has made information technology a core component of an organization's overall risk management strategy. In most cases, an organisation's other risks are related to the technology risk.

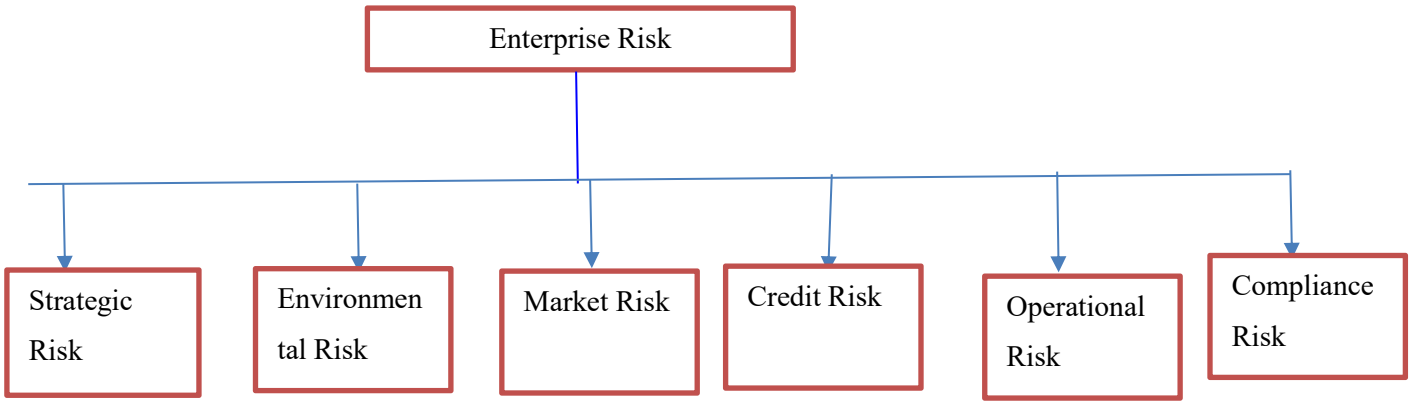

Figure 3 Enterprise risk

Due to the increasing importance of information systems, all aspects of risk are placed at the organisation's centre. This means that the management of risk is a continuous process. It should be aligned with the business objectives to improve the project's success rate. Figure 6 illustrates the various stages of risk management.

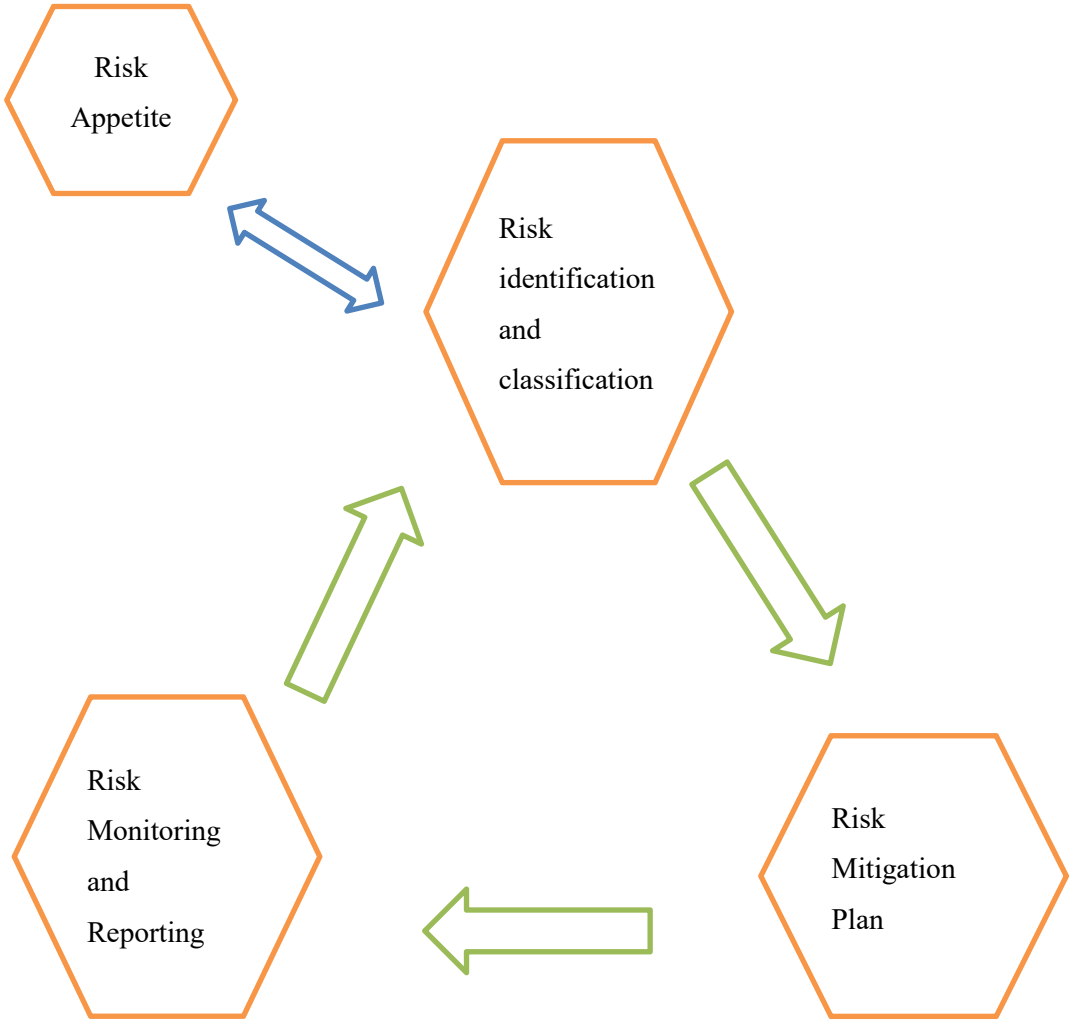

Figure 4 Risk management life cycle

4.2 Risk appetite

The concept of risk appetite is a framework that describes the various aspects of risk an organization has to manage. It is usually defined by the company's objective to absorb the loss and the culture of the Organisation (Barfield, 2007). Hence, it is the ability of an organization to absorb and manage risks. It refers to the level of risk it is willing to take to pursue its goals and values. An organisation's executive management and board of directors are responsible for determining the appropriate amount of risk that the organization is willing to take (Barfield, 2007). On the other hand, risk tolerance is the deviation an organization is willing to accept to pursue its value-creation goals. This concept takes into account the broad idea of being averse to risk. For instance a project

may overshoot its budget by 10% or get delayed by 15 percent. A risk map can help illustrate the various levels of risk that an organization is willing to take in pursuit of its goals (Colletaz, 2013).

4.2.1 Risk Identification and classification

Without first identifying an organisation's assets, it is impossible to identify potential risks. These are categorized according to their value depending on the business units and departments they belong to. The first step in identifying an organization's assets is to identify the various components that make up its operations. These include the people, hardware, software, and documents used to run its business. The classification process is usually carried out according to the different factors that affect an organisation's operations (Xenidis, 2005).

After identifying the assets, an organization conducts a risk analysis to identify the various risks it could face. This process can help identify the appropriate steps to minimize the impact of these risks. One of the most critical factors an organization should consider is the development of effective data sources that can support its decision-making process. The risk analysis results can then be stored in various tools, such as a risk register or a risk map. The profile can then be used to identify the areas of the organization that are most critical to its operations. The BIA is a process designed to help the senior management make informed decisions. The goal of the BIA is to provide a comprehensive view of the impact of a system or process outage on an organization's operations. It also allows the management to identify the appropriate steps to restore resources (Radanliev, 2019).

4.2.2 Risk mitigation plan

Although risk management can eliminate a certain amount of risk, it cannot eliminate all of it. Even with the various controls and foresight that are in place, residual risks can still be encountered after the treatments have been completed (Lehmann, 1990). This is why it is important to consider multiple approaches to managing the identified risk. Organizations can avoid risk by choosing not to carry out the process or venture that creates the risk scenario. This is done based on the senior management team's risk tolerance and appetite. An organisation has multiple options if it decides to take on a venture with known risks. Control is used to manage the situation to limit the impact and frequency of a risk. This approach can be used in various modes, such as preventive, detective, and recovery. It can be layered over other processes and equipment to provide optimal protection (Hamelmaan, 2008).

The various controls an organization has to implement are important for ensuring its transactions are reliably processed. These include the availability of atomicity, consistency, and isolation. Having the right controls can help prevent them from experiencing issues affecting the organisation's operations. One of the most important factors an organization should consider when implementing these controls is the cost-benefit analysis. One of the most common steps an organization can take when implementing risk management is transferring the burden of the risk to a third party. This type of approach can be done with insurance companies or outsourcing the services of a third party.

Although outsourcing or insurance services can be considered part of an organization's risk management strategy, it is still important to consider the cost-benefit analysis before proceeding. The senior management team and the board of directors are responsible for managing the risks. The concept of accepting risk refers to the recognition of a risk by an organization but not the resources to address it. In most cases, a threat's impact or probability of success is low. Although there may be a high likelihood of occurrence, the level of risk appetite of an organization can also be high depending on its goals and objectives. For instance, a pharmaceutical company's risk appetite is high when developing new drugs. On the other hand, a banking institution's risk appetite is low.

4.2.3 Monitoring and reporting

The continuous monitoring and assessment of the adequacy and functionality of risk controls is a part of the continuous process of building a resilient security framework. This process involves reporting back to the management when the conditions warrant. Reducing risk to a level below the organization's appetite can be done by establishing controls. This can be done through the use of various forms of reports, such as penetration testing and audit reports. These reports can help the management and the board of directors identify and evaluate the risks and assets of the company. They can also help the senior management make informed decisions (Parameswari, 2019).

4.3 Risk management frameworks

Many organizations utilize frameworks to manage their risk. These are usually categorized into one or two types and follow a risk assessment cycle. They can be adjusted to accommodate changes in the business. The best practice is to carry out risk assessments every three years. This allows for flexibility and security (Themsen, 2018). These standards aim to help organizations implement effective risk management techniques. They can be used in various industries and are designed to help organizations identify and manage their risks. In addition to being used for internal purposes,

government agencies can use these frameworks to establish regulations and guidelines. A framework is a means by which organizations can easily view and implement international standards and guidelines designed to help them manage their risk. These guidelines are often updated to reflect the changes the information systems environment brings. Aside from meeting their goals, frameworks also help organizations comply with regulations.

4.3.1 ISO 31000:2009 Risk management – practices and guidelines

The ISO is a non-profit organization coordinating the efforts of over 150 national standards bodies to develop international standards. These bodies are responsible for providing solutions and knowledge to various challenges through their shared expertise and knowledge. Some of the standards that are commonly used include BS ISO 31000. Although ISO 31000 is not focused on a single industry or sector, it has a framework and eleven characteristic principles that can be used to describe the various aspects of risk management. This standard aims to broaden the scope of risk management by emphasizing proactive competencies. The goal of ISO 31000 is to align the various aspects of an organization's risk management strategy with international standards (Dali, 2012). This will give them a complete view of their risk portfolio and help them make informed decisions. Although the standards do not eliminate the need for traditional risk management, they do provide a framework that can help organizations drive efficiency. The emphasis is placed on the decision-making process and the actions taken to identify and manage the identified risks. With ISO 31000, organizations can measure the effectiveness of their risk management applications. This helps them determine the value of their decisions and improve their efficiency. Furthermore, 31000 emphasizes using widely-accepted strategies to manage risk (Gjerdum, 2009). This can create a risk-averse environment. Instead of focusing on an event, ISO 31000 emphasizes how risk management can affect an organization's goals. It goes beyond being a compliance-based function and provides a framework that enables organizations to make informed decisions.

4.3.2 OCEG “Red book” 3.0 2015 GRC Capability model

The objective of the OCEG is to provide a framework for addressing the various challenges that organizations face in today's rapid emergence and evolution of new risks and requirements. Through its Principled Performance approach, the organization aims to help companies manage their risk and compliance effectively (Mitchell, 2017). Many organizations have failed to effectively manage their risk and compliance programs due to factors such as poor governance, lack of visibility, and duplication of functions.

The lack of control over the cost of implementing and managing risk and compliance programs has led to less productivity within the organizations. The OCEG's Principled Performance approach aims to provide a framework that combines the various aspects of risk and compliance management to achieve effective performance. The concept of principled performance involves an organization's various departments and functions, which are aligned and contribute to the business's success, for example, banks (Ahmadalinejad, 2015). It also establishes a culture where these entities work together seamlessly to achieve the organization's goals. The various departments and functions of an organization must contribute to the collection of data to improve the efficiency of the business. This can be done using effective technology and aligning the core functions with the requirements of the business. The Principled Performance approach also considers the various factors that affect the organization's operations, such as the social mores and the law. Hence, the continuous improvement process of the GRC Capability model is designed to help organizations achieve principled performance. It involves the use of various integrated capabilities such as;

The process of discovery is a step that involves identifying the requirements of an organization to achieve its goals. Additionally, it entails conducting an in-depth analysis of the various factors that influence an organization’s operations and culture. However, the alignment of the various requirements of an organization is also a step that involves identifying the strategies and objectives that will help achieve its goals. This process can be carried out through the board of directors' direction. Furthermore, the performance of an organization is determined by addressing its obligations and opportunities while developing effective strategies and procedures to manage threats.

The goal of this review is to identify the effectiveness of the various controls and actions of the organization in improving the designs and ensuring that they are aligned with the company's strategic objectives. It also seeks to improve the capabilities of the team. As a result, it explores the following critical factors:

An organisation's Human Resource Management (HR) department is responsible for identifying its employees' various roles and responsibilities. The planning and design of the organization's new strategies are carried out while considering the various factors that affect the organisation's efficiency. Continuous assessment is also performed to evaluate the effectiveness of the plans (Lengnick-Hall, 2003).

On the other hand, a good governance and risk management (GRC) strategy aims to achieve principled performance by developing a high-level commitment to the process and allocating

resources to support the concept. This can be done through the development of plans and designs that are based on the capabilities model. The various responsibilities of the organization's governing authority, such as the CEO, the CIO, the CFO, and the other managers, are assigned to different groups and individuals (Kleffner, 2003).

4.3.3 NIST 2014 Cyber security framework

The US Department of Commerce established the NIST in 1901 to promote industrial competitiveness and innovation. It is a national laboratory that develops standards and advances measurement science to improve the quality of life and economic security (Greer, 2014). The National Institute for Standards and Technology collaborated with industry experts to develop a framework to help organizations manage cyber security risks. The framework was built based on various standards and practices and designed to be both technically neutral and flexible (The White House, 2012).

The framework aims to provide a common language for describing and managing the various aspects of cyber security risk. It also helps organizations identify and prioritize activities to reduce risk exposure. Thus, it features three main components: the Core, the Implementation Tiers, and the Framework Profiles. The three sections reinforce the connection between the various activities and business drivers involved in cyber security risk (Szykman, 1998). The Framework Core is designed to provide a comprehensive view of the various aspects of cyber security risk. As a result, it includes practical examples and activities that can help organizations identify and implement effective strategies. It also helps organizations communicate the goals and procedures related to their cyber security efforts. The framework's core includes various elements, such as functions, categories, and informative references.

The framework functions help organizations identify, protect, detect, respond, and recover. These activities can help them manage their cyber security risk and improve their efficiency. It also allows them to develop resilient plans and improve their response to incidents.

These functions are aligned with the current methods used for incident management. They can also help organizations show the impact of their cyber security investments. The categories included in the framework are those focused on specific areas, such as asset management and detection processes (Shen, 2014).

The categories in the framework are designed to provide specific details about the activities performed in managerial and technical risk areas. The categories within the framework are also

designed to help organizations achieve their goals and improve their efficiency. They are sub-categorized and supported by informative references commonly used in the infrastructure sectors. The Implementation Tiers provide an overview of the various aspects of cyber security risk that an organization must face. This is because they help identify and implement effective strategies. This framework has four levels: Partial, Risk Informed, Repeatable, and Adaptive. The Implementation Tiers provide an overview of the various aspects of cyber security risk an organisation faces. They help identify and implement effective strategies. Additionally, they are categorized into four categories based on the threat environment, business goals, legal requirements, and implementation practices. The Framework Profile is designed to align the various categories and functions with the requirements of an organization. Hence, it helps develop a roadmap clearly showing the organization's priorities when managing its cyber security risk. It also helps in communicating the risks to the public. Meanwhile, the framework's Target and Current Profile sections provide an overview of the different aspects of cyber security risk an organisation faces. Therefore, they help identify and implement effective strategies. The former summarizes the current state of the security risk, and the latter indicates the necessary steps to achieve the goals.

4.3.4 COSO: 2004 Enterprise risk management for integrated frameworks

The COSO framework is widely used and regarded as one of the most effective tools for improving and controlling organisations' internal control systems. It was developed to help organizations achieve their goals and objectives by giving them a stronger grip on their activities. Rather than replacing the existing internal control framework, the COSO Integrated Framework aims to expand its scope. As a result, it provides a more comprehensive and holistic approach to managing risk. This ensures organizations have a more effective and efficient internal control process (Hiles, 2012).

The four categories of the COSO framework are strategic, operations, compliance, and reporting. They help organizations achieve their goals and objectives by separating the expectations of different groups from those of the organization. For instance, the objectives of the strategic category are aligned with the organization's mission and are often focused on achieving high-level goals. On the other hand, the operations category's goals are linked to the effective use of resources (Bowling, 2005).

The reporting category is composed of requirements related to reports' reliability. The last section of the framework is called Compliance, which aims to help organizations achieve their goals and objectives by ensuring that they follow the regulations and laws of their operating environment. The integrated framework ensures that an organisation's various goals and objectives are achievable

even if they are not fully under the organisation's control. For instance, an organisation's operations and strategic objectives are not always under the control of the management. The Enterprise Risk Management division of the COSO framework can monitor and help the board and the management with the organisation's progress toward its goals.

The eight components of the COSO framework are designed to help management effectively carry out their duties and responsibilities. They are used in evaluating and mapping enterprise risk management (Chapman, 2004).

- The internal environment component of the COSO framework is composed of the various aspects of an organization's risk management strategy and procedures. It includes the expectations of its employees, the management, and the public about the organization's risk appetite.
- The goal-setting process of an organization is also carried out through the integrated framework. It ensures that the chosen objectives are aligned with the company's mission and are in line with the organisation's risk appetite.
- Events that can affect an organization's set goals should be identified and classified into internal and external categories. These should be categorized into opportunities and risks.
- A risk assessment is also carried out to identify and analyze an organisation's potential risks. It can help the management determine the appropriate steps to minimize these risks' impact.
- The management also responds to a risk to align the organization's risk appetite with its goals and objectives. As a result, it can either accept, minimize, or share the risk.

The procedures and policies designed to effectively implement the risk responses should be available to the entire organization.

Communication and information: This is also ensured by the management, as it allows the various parties within the organization to effectively carry out their responsibilities. This can be done through the capture and dissemination of the necessary information.

The continuous monitoring of an organization's risk management is also carried out through the regular evaluation and implementation of its policies and procedures.

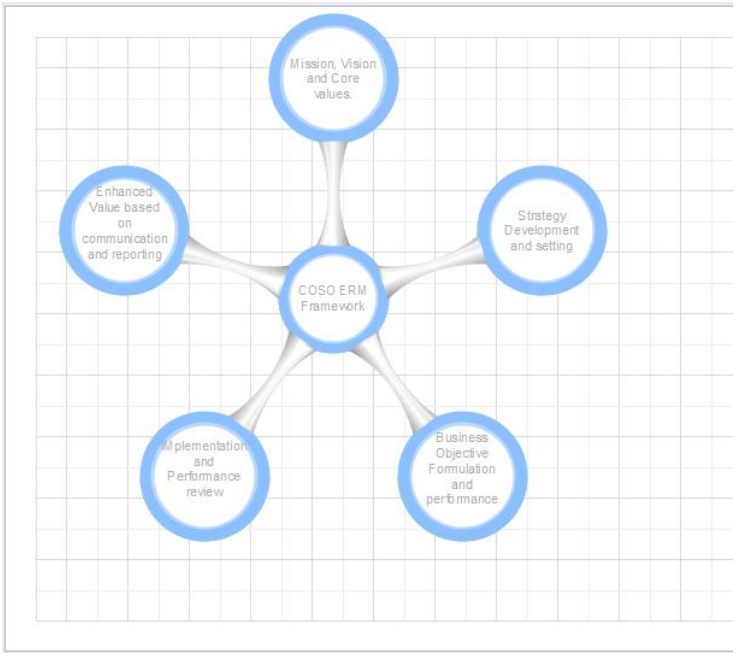

Figure 5 COSO enterprise risk management

The COSO's integrated framework for enterprise risk management (ERM) provides a framework that enables the management of multiple components. These include establishing a culture of risk, developing a risk appetite, and identifying the ideal people. It also involves conducting business analysis and setting goals. This process aims to enhance the organisation's performance by developing and implementing effective response capabilities and portfolio views. In addition, the review and implementation of risk assessments are also carried out to improve the management of the risks. Finally, the continuous improvement of the communication and reporting framework is made to enhance the effectiveness of the organization.

4.3.5 FERMA: 2002 Risk management standard

As the role of risk management shifted from being focused on the financial to the strategic and corporate governance aspects, the FERMA has been working to support this evolution. The formation of FERMA brought together various national associations from various European countries. With the increasing number of members, the organization has been working to promote and coordinate dialogue between them to improve the quality of their risk management practices.

In 2002, the FERMA developed a standard that aims to standardize the approach to risk management across Europe. Consequently it provides a framework for identifying and managing risks and implementing procedures and control (Henriksen, 2006). The standard provides a

framework for analyzing and managing risks, comprising opportunities and threats to goals. These are part of an organization's overall strategy and are usually handled optimally. The standard provides a simple framework for identifying and managing risks. Additionally, it allows organizations to classify the various risks into their respective effects and probability of occurrence. Thus, this allows them to perform business impact analyses to determine the appropriate treatment for these threats. The procedures and controls that are part of the standard should be designed to effectively and efficiently address the organisation's various requirements. They should also be carried out in a way that complies with regulations and mandates. One of the most important factors that the FERMA standard provides is the establishment of a monitoring process designed to ensure that the procedures and controls follow the policies.

4.3.6 Liquidity: 2012 Risk management for insurance

The liquidity framework is a new standard that will be implemented by insurance companies operating in the European Union from November 1, 2012 (Doff, 2008). Hence, it aims to improve the regulation of the insurance industry by implementing a risk-based system and an integrated approach to assessing and managing the risks associated with the business. The liquidity framework provides a broad framework for risk management (Doff, 2008). It also requires insurance companies to establish procedures and controls to manage their risk. Finally it requires them to develop a capital requirement that is proportionate to the level of assets and liabilities that they have.

The Financial Services Authority has defined economic principles to measure the various assets and liabilities of Solvency II. The first pillar of this framework is focused on regulating quantitative requirements. The Solvency II framework has two capital requirements that are designed to ensure that insurance companies have the necessary capital to meet their obligations. The first is the minimum capital requirement, which is the amount they should hold to cover their liabilities. The second pillar of liquidity is the framework's requirements for the supervision and governance of insurance companies. These requirements are designed to create a framework for effective coordination between the different authorities in the European Union. The framework also provides a set of principles for the development of internal control systems and risk management procedures. These include the establishment of a risk management quality framework and the development of effective senior management criteria. The third pillar of the framework is focused on developing rules designed to enhance the transparency and disclosure of information related to the operations of insurance companies (Doff, 2008). The liquidity framework has three layers of defence designed to protect an insurance company from various risks. These include the establishment of effective risk

management procedures and controls the development of risk oversight and the implementation of risk assurance. The first layer of defence is the establishment of risk management procedures and controls. The chief risk officers carry out this process. The second layer of defence is the development of risk oversight. The audit committee carries out this process. The third layer of defence is the implementation of risk assurance. This process ensures that the company's compliance activities are carried out.

4.4 Observations

A standard or framework is often used as a basis for governments and organizations to develop their best practices in various areas. For instance, implementing risk frameworks and standards is a process focused on developing effective risk management techniques. Implementing a risk strategy and governance framework is also beneficial for ensuring that an organization follows the proper regulations (de Oliveira, 2017). Best practice controls are typically established based on guidelines and regulations developed through collaboration over time. They can then be improved upon and expanded to include new procedures. However, they cannot always evolve with the changes in the environment due to how they are designed. To ensure that their best practices apply to different situations, organizations must identify the changes they need to make. When a government or an organization makes a mandatory requirement in an approved contract then standards become more regulated. This can bring about various aspects of compliance such as implementing regulations and establishing effective risk management policies and if an organization uses the proper regulations security can still be compromised due to the lack of consistency and the continuous testing of the procedures. Proper certification for best practices and compliance with regulations is also beneficial for ensuring the procedures are followed properly. It can help prevent complacency and ensure the organisation follows the correct security measures.

The ISO 31000 standard focuses on the effectiveness of risk management in improving the performance of an organization. It does not provide adequate assurance that the procedures are being followed properly and that the organization follows the correct regulations. This is a significant issue since implementing IoT security requires establishing effective controls designed to identify and prevent threats (de Oliveira, 2017).

The approach taken by OCEG emphasizes the importance of incorporating various aspects of risk management into a single framework. Unfortunately, this approach limits the scope of risk management and prevents the organization from properly identifying and mitigating the risks associated with the IoT (Henriksen, 2006).The development of the NIST Framework, a

comprehensive security standard, is expected to provide a better framework for addressing the various aspects of risk. It is designed to help organizations manage their security by focusing on their systems' detection and response capabilities. Although experts have criticized the release of the NIST Framework version 1.0 for its lack of focus on implementing effective measures to protect critical infrastructure, it is still beneficial to have a framework that focuses on an organisation's detection and response capabilities.

The FERMA standard and the COSO Framework do not provide a comprehensive framework for addressing the root cause analysis of risk. This is a significant issue since implementing the regulations related to establishing effective measures to protect critical infrastructure requires the proper management of risk. Although the standards and frameworks discussed in this chapter provide a good baseline, most security breaches are not detected by an organization's internal processes. Instead, third parties usually detect them (Chapman, 2004). The average time it takes for an organization to discover a security breach and the time it takes to resolve the issue is over 140 days globally and almost 500 days in the Middle East, Africa, and Europe regions. These are alarming statistics that show the need for better risk management standards. Even though numerous security vulnerabilities have been identified in the Internet of Things (IoT), it can take an organization a while to patch them. For instance, the patch for the St. Jude Medical devices was partially released in January 2017 after it was first discovered in August 2016 (Bacon, 2015).

5 Methodology

5.1 Overview

Research methodology deals with the empirical study of how research work is conducted. It discusses a scholar's step-by-step processes for studying a research problem and its logic. Furthermore, the methodology allows for a detailed understanding of how the study was done under different headings. Here, the methodology is premised on the research design model known as the research onion by Saunders and Tosey (2015). Each of the stages in the model serves as a guide for this section.

5.2 Research design

The research onion methodology is adopted in this study. It is a model developed by Saunders and Tosey (2015). It outlines the critical stages involved in research methodology. The steps are shown in the figure below.

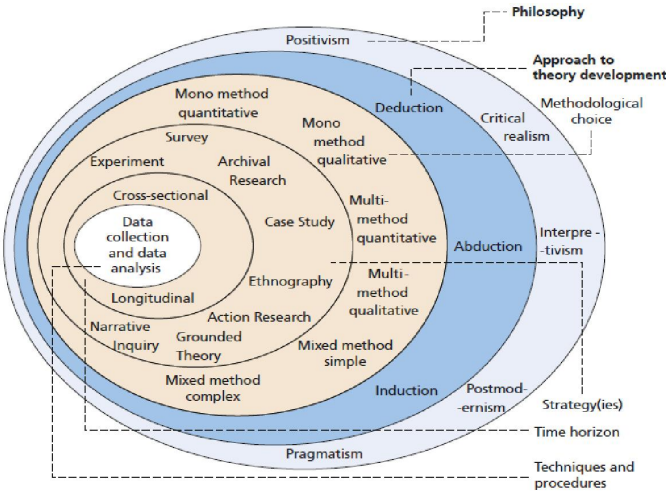

Figure 6: The research onion (Saunders and Tosey, 2015)

The first layer of the research onion is the research philosophy, followed by the research approach, strategy, research method or choice, time horizon, population and sampling, data collection method, and analysis. Each of these layers is discussed.

5.2.1 Research philosophy

The research philosophy is an approach whereby assumptions are created to justify the research executed (Flick, 2011). Therefore, philosophy in research is a belief system and assumption on

knowledge development. There are four main research philosophies in research. They are interpretivism, positivism, pragmatism, and realism.

According to Chowdhury (2014), interpretivism is a belief that the social world is subjectively interpreted. It is premised on the principle that researchers are essential based on their input in observing the social world. Thus, the researcher's interest is critical when a study is premised on interpretivism.

Positivism is a set of beliefs in which the social world can only be understood objectively. Thus, a researcher engaging in this kind must be objective in his approach, reduce personal bias, and work with an independent and open mindset. Furthermore, Ryan (2018) believes that this philosophy is premised on empirical findings and that factual knowledge is gained only through sense experience.

Pragmatism is another type of research philosophy premised on the assumption that researchers must use methodological and philosophical approaches best suited to a specific research problem (Tashakkori, Abbas, and Teddille, 1998).

Realism has to do with an idea hinged on the independence of reality from the human perspective (Dean et al., 2006). Based on this, realism assumes that a scientific approach is needed in knowledge development

This study adopted positivism's argument because it focused on collecting and confirming the Implementation of ISO frameworks to risk management in IPv6 through a questionnaire survey. To a large extent, the study identifies with the demand of positivism philosophy and addresses it, and quantitatively analyses the order using the SPSS analytical tool.

5.2.2 Research approach

The philosophy adopted determines the research approach chosen for a particular study (Saunders, Lewis, and Thornhill, 2009). There are two major types of approaches in research. They are deductive and inductive approaches. Gabriel (2021) posits that any study that is deductive in its approach would test an existing theory. At the same time, inductive research, rather than testing a current theory, would generate a new view from the data collected. Also, in deductive research, conclusions are drawn based on the past evidence obtained and the data obtained on the model. In contrast, the business model is new in the inductive study, as there is always little or insufficient previous research evidence or data about the business model. However, this report adopted the

deductive approach because the literature sources are available. Also, there is a need for a limited time-frame to complete the study.

5.2.3 Research strategy

According to Saunders et al. (2009), strategy in research is the general plan of action for answering the research question posed. It is chosen based on the research questions and objectives of the study, the extent of the existing knowledge on the subject matter, and the available time and resources, including the philosophical underpinnings of the researcher. The most common research strategy is action research, case study, experiment, and survey. This study adopted a survey. A survey is a generally adopted method, allowing ample access to more participants. Due to the availability of websites and other online places, such as social media, where surveys are quickly and cheaply distributed, survey responses are now easily organized (Open Learn, 2020).

5.2.4 Research method

This is the procedure used in the collection and analysis of data. There are three types of methods or choices in research. Research methods could be mono, mixed, and multi. This method can as well be quantitative and qualitative. Mono-research is when either a qualitative or quantitative approach is used in research. Also, the mixed method is when both qualitative and quantitative methods are used. Multi-research takes place when two qualitative or quantitative studies are done simultaneously. It is worth noting that the approach adopted depends on the knowledge type a researcher intends to develop.

According to Scribbr (2020), the quantitative method deals with numerical data, which can be statistically analyzed to test the relationship between dependent and independent variables. The qualitative method, on the other hand, is a method that deals with non-numerical data. This is the data that cannot be counted or quantified. It is mainly analyzed thematically to interpret the underlying trends in the data (Leedy, 1993). This report used qualitative and quantitative methods because an open-ended questionnaire collects information on implementing ISO frameworks to risk management in IPv6. This makes the study a mixed-choice study, and it is crucial to the achievement of the objective of this study. The data was analyzed using SPSS analytical tools (Winberg, 2002).

However, there are other types: exploratory or conclusive and descriptive or casual. Exploratory research deals with investigating problems that are not clearly defined. It is done to have a deeper

knowledge of a research problem and its context instead of understanding its solution (Rudestam and Newton, 2007). Researchers use it to have a deeper knowledge of the studied problem to form a more concise research problem before being effectively investigated. According to Voxco (2021), the exploratory research method can be categorized into two, that is, primary research methods and secondary research methods. The primary research method is where data is obtained directly from the subject of investigation (Rudestam and Newton, 2007). This may be a group of persons or an individual. Surveys, interviews, observation, and focus groups are common primary research methods (David and Sutton, 2004). On the other hand, secondary research methods are used in collecting data from existing resources about the investigation. Online sources, case studies, research papers, and literature, among others, are common secondary research methods (Voxco, 2021).

Conclusive research is a type of research design used in collecting data that may be used to draw conclusions or make informed decisions (Blaxter et al., 2006). The obtained data is usually quantitative and has distinct numbers. Based on this, conclusive research depends on using structured techniques, like surveys with close-ended questions. This method helps the researcher confirm or disprove a hypothesis (Voxco, 2021). There are two types, namely descriptive research and causal research. The Descriptive is used in answering the question of ‘what’, ‘when’, ‘where’, and ‘how’ instead of ‘why’ (Sweetnam, 2000). It is a form of research that describes a population, phenomenon, and situation. Causal research, on the other hand, is used in investigating the cause-and-effect relationship between variables (Voxco, 2021).

5.2.5 Time horizon

Molina-Castillo and Munuera-Aleman (2009) refer to the time horizon part of the research onion as a fixed period in the future where certain processes are presumed to come to an end. There are two types of time horizons in a research study. They are longitudinal and cross-sectional studies. In a longitudinal research study, there is a continuous measure to follow certain people over an extended time (Elias, 2021). Also, data are collected prospectively (Al-Zeferiti and Mohammed, 2015). However, a cross-sectional study involves the researcher simultaneously measuring the participants’ outcomes and exposure (Setia, 2016). Also, the data is collected in a cross-sectional study retrospectively to extract pertinent data helpful in answering the research questions posed. Also, because of the time constraint, the cross-sectional approach collects data within a short time frame to complete the study (Setia, 2016). The cross-sectional time horizon is relevant and thus adopted for this study compared to the longitudinal time horizon. The longitudinal time horizon is not time-

saving, and adequate research information required for the research study may not be obtained due to the researcher's limited time to complete this study.

5.3 Conceptual framework

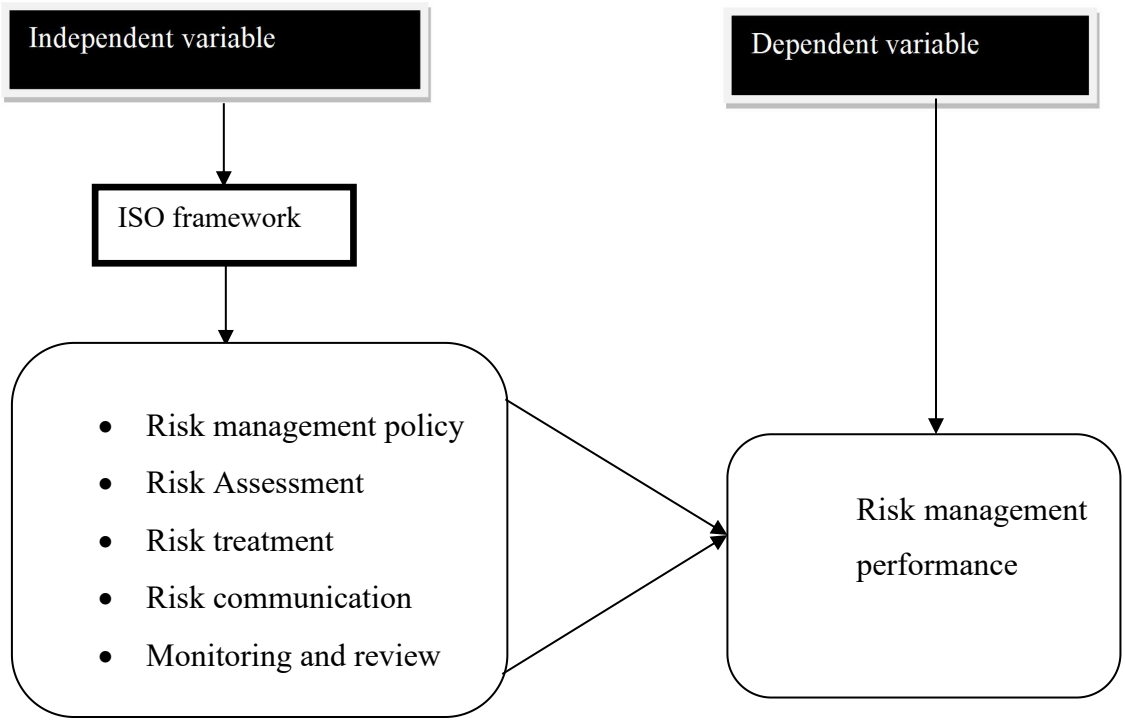

Figure 7 Independent and dependent variables

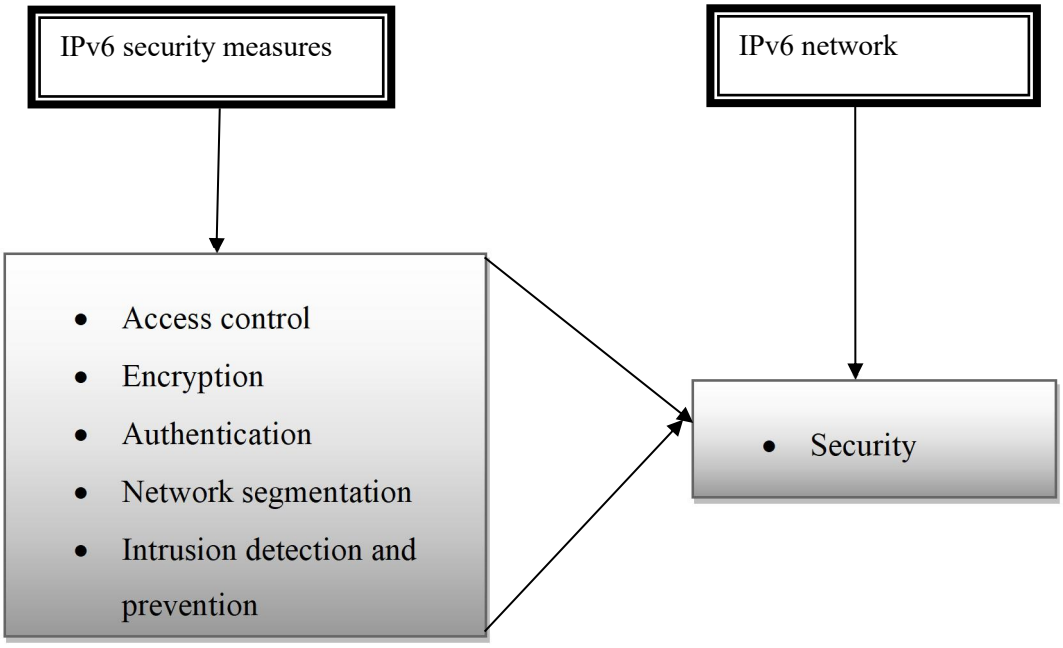

Figure 8 IPv6 networks and security measures

Risk management policy: This is a tool used in identifying and responding to risks to reduce their impact (Sarokin, 2020)

Risk assessment: This is the overall method of identifying, assessing, and controlling threats to digital assets, including the data stored on servers or public cloud service and digital information in transit (N-able, 2023)

Risk treatment: This entails identifying digital assets, reviewing their existing security measures, and executing a solution to either continue with what works or mitigate security risks that may make the digital asset vulnerable to attacks (Rapid7, 2023)

Risk communication: This happens when information relevant information on cybersecurity risks and issues is shared (Board, 2022)

Monitoring and review: This overseeing the risk management activities to ensure it is effective over time (Cooper et al., 2014)

Access control: This is a data security process that allows organizations to manage who has the authority to access digital and information assets and resources (Kim and Solomon, 2013)

Encryption: This transmits digital data to the cloud and computer system. Since modern algorithms have replaced the outdated data encryption standard, the algorithm guards information security by authenticating the origin of any message (Pachgharge, 2019).

Authentication: This is the security procedure in which identity is verified and recognized as the same as the person claims to be (Sen and Mehtab, 2020)

Network segmentation: This is a security technique in which a network is divided into smaller, distinct sub-networks that allows network teams to compartmentalize the sub-networks and enhance security control and services to each sub-network (Fabig and Haasper, 2018)

5.4 Hypothesis testing

H10: Risk management policy has no impact on the risk management performance of the ISO framework.

H11: Risk management policy has an impact on the risk management performance of the ISO framework.

H20: Risk assessment has no impact on the risk management performance of the ISO framework.

H21: Risk assessment has an impact on the risk management performance of the ISO framework.

H30: Risk treatment has no impact on the risk management performance of the ISO framework.

H31: Risk treatment has an impact on the risk management performance of the ISO framework.

H40: Risk communication has no impact on the risk management performance of the ISO framework.

H41: Risk communication has an impact on the risk management performance of the ISO framework.

H50: Monitoring and review have no impact on the risk management performance of the ISO framework.

H51: Monitoring and review have an impact on the risk management performance of the ISO framework.

H60: Access control does not enhance the security performance of the IPv6 network.

H61: Access control enhances the security performance of the IPv6 network.

H70: Encryption does not enhance the security performance of the IPv6 network.

H71: Encryption enhances the security performance of the IPv6 network.

H80: Authentication does not enhance the security performance of the IPv6 network.

H81: Authentication enhances the security performance of the IPv6 network.

H90: Network segmentation does not enhance the security performance of the IPv6 network.

H91: Network segmentation enhances the security performance of the IPv6 network.

H100: Intrusion detection and prevention do not enhance the security performance of the IPv6 network.

H101: Intrusion detection and prevention enhance the security performance of the IPv6 network.

5.5 Population and sampling

5.5.1 Target population

A target population is a set of people who have a specialized set of characteristics. They are the large set of people in the world to which the research outcome is generalized. They can also be referred to as the study population if they are the subset available for the study (Banerjee and Chaudhury, 2010). The target population for this study was the individuals involved in designing and implementing an organisation's security and risk management policies and procedures.

5.5.2 Sample frame

This is the list of members of the population of interest from which a probability sample is chosen. This does not always include all the target population members (Rukmana, 2014). For instance, if a study were to survey residents who use smartphones in a certain neighborhood as the sample frame, the non-smartphone device users would not be included (Rukmana, 2014). In the same vein, the current research's target population was the individuals involved in designing and implementing an organization's security and risk management policies and procedures. However, out of this were senior management, network architects, security analysts, network administrators, system administrators, cybersecurity specialists, risk management professionals, and auditors, who served as the sample frame for this work.

5.5.3 Sample size

A sample is an arm of a fully defined population. It is the number of participants or observations included in the research. The number is usually represented by n. The sample size influences the

estimates' precision and the power to draw informed conclusions in the study (Faber and Fonseca, 2014). The sample size for this study was 75.

5.5.4 Sampling technique

Sampling techniques can be categorized into random sampling and non-random or purposive sampling. The non-random or purposive, or non-probability sampling technique is a method that uses non-random criteria such as the availability, the proximity of location, or professional knowledge of individuals you want to study to have a specific answer to research questions (Nikolopoulou, 2022). Non-random sampling is mainly used when the target population parameters are unknown or possible to identify one after the other. There are certain limitations to this technique. It includes the target population that may be hard to identify. Also, statistical inferences like confidence intervals and significance tests may not be easily estimated from a non-random sample (Banerjee and Chaudhury, 2010). Also, it is worth noting that this technique is at a higher risk of biases (Nikolopoulou, 2022). There are different types of non-random sampling techniques; they include convenience sampling, quota sampling, self-selection sampling, snowball sampling, and purposive or judgmental sampling (Nikolopoulou, 2022).

- Convenience sampling: This is determined by the researcher’s convenience (Nikolopoulou, 2022).
- Quota sampling: A predetermined number or proportion of units known as the quota is selected (Indrayan, 2008).
- Self-selection sampling: This is also called volunteer sampling and depends on the participants' voluntary agreement to be part of the study (Banerjee et al., 2007).
- Snowball sampling: This is used when the population intended for studying is not easy to reach. Or a situation with no existing database or other sampling frames to help (Nikolopoulou, 2022).
- Purpose: This is a blanket term for a series of sampling techniques that select participants deliberately due to their qualities, which will help the research work (Banerjee et al., 2007).

The sampling method that allows a sample to have an equal likelihood of being included in a study sample at random is known as the random sampling technique (Banerjee and Chaudhury, 2010). Random sampling is the basis of all good sampling techniques as it does not allow any method to be selected based on volunteering or the choice of people who may cooperate with the research (Indrayan, 2008). In other words, compared to other approaches, it does not use a biased technique

for responses collected from target population sizes. It is impossible to study the whole population; thus, scholars rely on sampling to have a clear aspect of the whole population for observation. The system must not bias the class chosen to represent the whole target population group (Banerjee and Chaudhury, 2010). Random sampling techniques are of different types. They are simple random sampling, systematic sampling, and stratified random sampling (Nikolopoulou, 2022).

Stratified sampling divides the target population into sub-populations or strata based on their differences. It allows for more concise conclusions by ensuring that each stratum is well-represented in the sample (McCombes, 2023). A cluster is the opposite of stratified, as it deals with the group of each stratum or subgroup based on their similarities.

Systematic sampling: Here, every member of the population is listed with randomly generated numbers, as individuals are selected at regular intervals (McCombes, 2023)

Simple random sampling involves sample selection from a set of targeted groups out of a bigger population group. Each individual and element of the group can be chosen by chance due to the similar opportunities they all share to be among the sample selection. It is the most suitable random sampling when it concerns the entire population from which the sample is selected as homogenous (Nikolopoulou, 2022). The advantage of simple random sampling is the relative ease of utilization and the exact representation it garners. It is distinct from the rest because it comes easily in mining samples out of an enormous population. It does not need to cut the bigger population to a sizeable sub-population from the bigger group (McCombes, 2023).

This study adopted simple random sampling in designing and implementing an organization's security and risk management policies and procedures. As a result, senior management, network architects, security analysts, network administrators, system administrators, cybersecurity specialists, risk management professionals, and auditors were randomly selected to represent the large population.

5.6 Data collection method

There are two types of data in research, primary and secondary data. According to Library (2019), primary data is freshly collected for a particular purpose, while secondary data is existing data collected in previous studies. Primary data is collected using surveys, focus groups, and interviews. This study used a survey technique, as such questionnaire was used. A questionnaire is a research instrument with a set of questions formulated by the researcher to collect survey participants' responses to test the study’s objective (Library, 2019). A well-structured questionnaire allows

respondents to provide a comprehensive response and allows for more information sharing as participants can express their views. A questionnaire was framed to obtain responses from participants on general quantitative data related to implementing ISO frameworks to risk management in IPv6 security. There are two types of questionnaires, structured and unstructured. Structured is a formal standardized or quantitative questionnaire, and it was deployed in this work to collect quantitative data from the participants (Nikolopoulou, 2022). On the other hand, an unstructured questionnaire is an exploratory or qualitative questionnaire deployed to collect qualitative data (McCombes, 2023). Secondary data was collected from different secondary sources, such as journal articles from online databases, websites, and blogs. The extracted data was used to prosecute different sections of literature reviews.

5.7 Data analysis tools

The quantitative data collected through the survey were analyzed using the SPSS analytical (Statistical Package for Social Science) tool. It is used to carry out a quantitative analysis. It is a complete statistical package developed on the interface of identifying an icon, pointing to it, and clicking on it. Lots of researchers have used it in the past to conduct quantitative analysis. It was developed to accept, read, and write data from other databases, packages, and spreadsheets. Users put the data into the package while the variables viewed are clicked. This allows the user to customize his work due to the data type, under the heading, such as missing the name, column, type, width, align and measure, decimals, and label. The headings' significance allows users to input the data into different classes. It is usually used in many social science research studies where there is a need for large statistical data analysis involving chi-test, cross-tabulation, f-test, and t-test, among others. The analysis menu can also be found on the application.

5.8 Data presentation tools

Data presentation is important in statistics and research because it helps researchers' study and explain their findings thoroughly. Therefore, data presentation is the process of using different graphical formats to present visual representations of the relationship between two or more sets of data to help draw an informed decision (Vendatu, 2023). Different forms of presentation tools are available in research, and they are textual, tabular, and diagrammatic. The diagrammatic have different types that can be used in research; they include pie charts, bar charts (simple bar diagrams and multiple bar diagrams), histograms, line charts, heat maps, column charts, box plots, and map data graphs, among others (ATH, 2023).

6 Data analysis and presentation

6.1 Overview

Two types of data were collected during this research. Quantitative data and qualitative. The survey was distributed to the respondents who were random selected. A total of 75 questionnaires were shared online after the informed consent of the respondents have been sought. 50 respondents returned their responses via the same platform through which it was distributed such as email, social media, among others. The quantitative data was analysed using Excel and SPSS and qualitative data was analysed using thematic analytical techniques.

6.2 Demographic information

6.2.1 Percentage of survey respondents

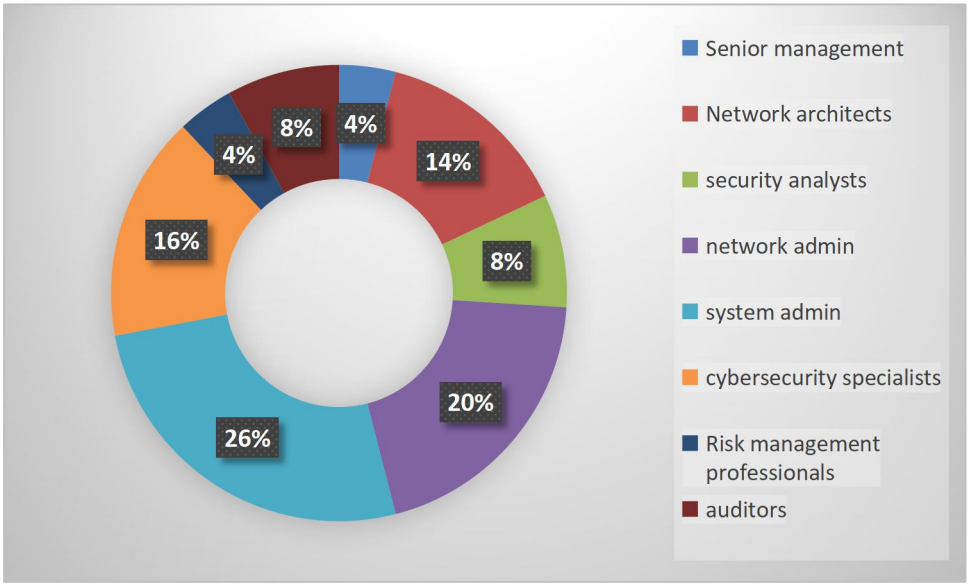

Figure 9: Positions

The result of the analysis shows that among the survey participants, system admin was the highest pooling 26% of the overall participants, followed by network admin, who were 20%, then the cybersecurity specialists, who were 16%. Also, 14% of the respondents were network architects, network architects, while senior management and risk management professional were 4% respectively. Also, the respondents who were auditors and security analysts were 8% respectively.

6.2.2 Gender

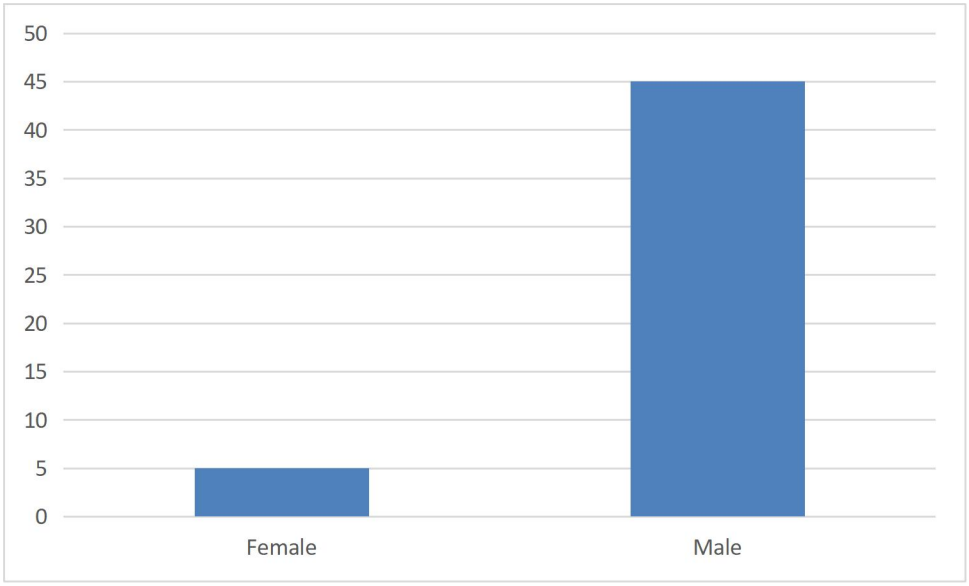

Figure 10: Gender

The figure above shows the representation of the gender of the survey participants. Females were 5 in numbers, while males were 45. This shows that there were more males participants than females.

6.2.3 Educational qualification

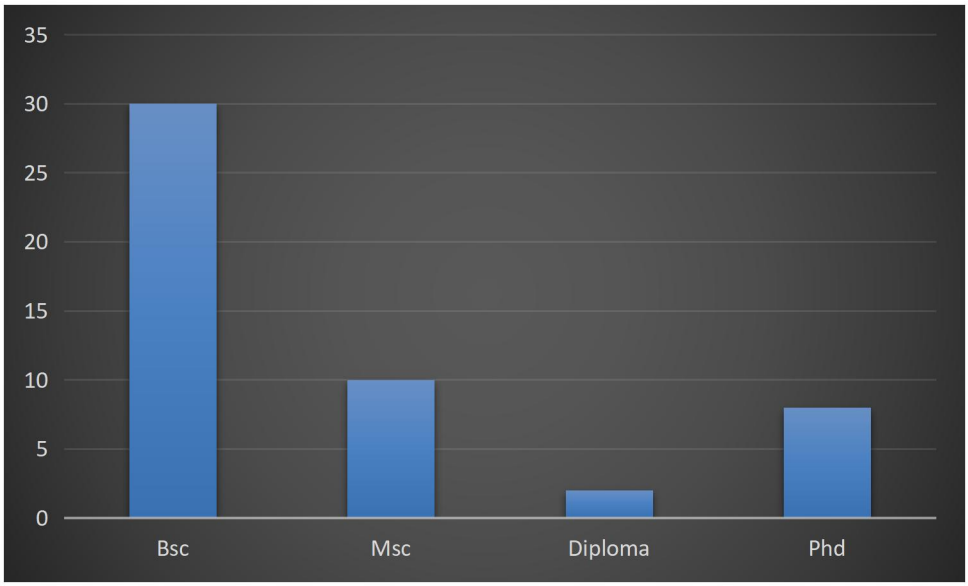

Figure 11: Educational qualification

The above figure is the educational qualification of the respondents. 30 people held BSc qualification, followed by those who held MSc, then PhD holders who were 8 in numbers and the

remaining 2 were diploma holders. The BSc holders were more than other respondents of different educational qualifications.

6.2.4 Years of experience

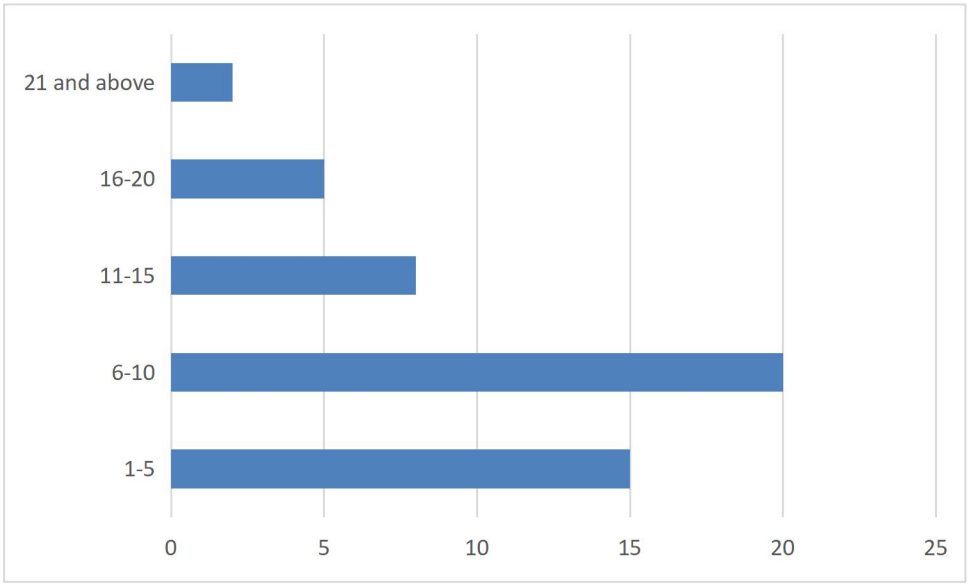

Figure 12: Years of experience

The years of experience of the respondents is presented in the above figure. Respondents who had 21 years and above experience were 2, those with 16-20 years' experience were 5, those with 11-15 years' experience were 8, also, those with 6-10 years' experience were 20 and respondents with 1-5 years' experience were 15. Those whose experience period fell between 6-10 years were more than the other groups.

6.3 General information

6.3.1 Risk management policy

Organisations should not have a risk management policy because it is unnecessary for ISO framework risk performance.

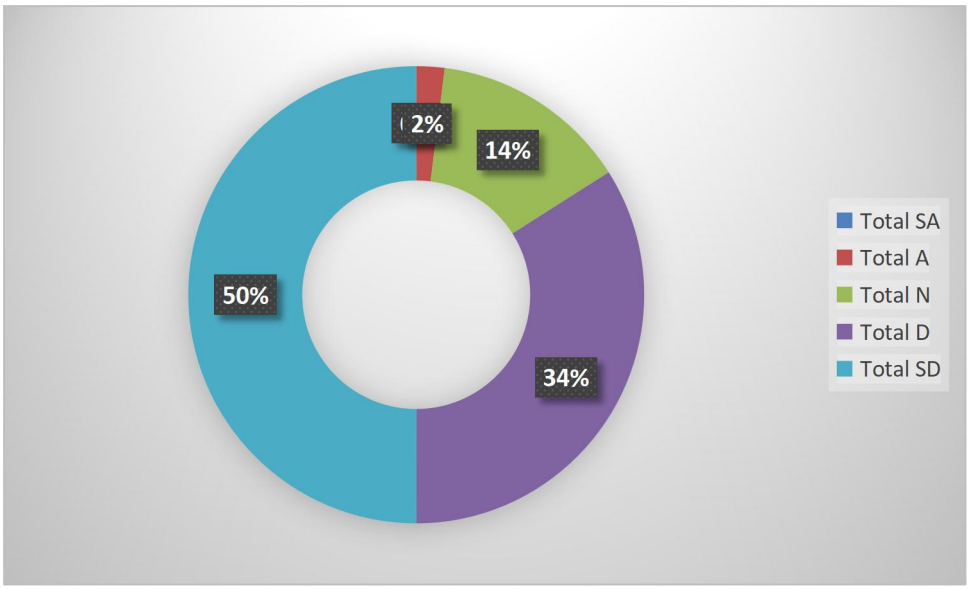

Figure 13: Risk management policy for organisations.

The figure above presents the response of the participants on the statement "organisations should not have a risk management policy because it is unnecessary for ISO framework risk performance" 50% strongly disagreed, 34% disagreed, 14% were neutral and 2% agreed. This shows that 84% believe that organisation should have a risk management policy because it is necessary for ISO framework risk performance. Thus, risk management policy is necessary requirement for ISO framework risk performance.

6.3.2 Implementation of effective risk assessment.

This becomes significant as it facilitates Organisation with the ability to narrow the surface areas of security threats and attacks, through contentious vulnerability check.

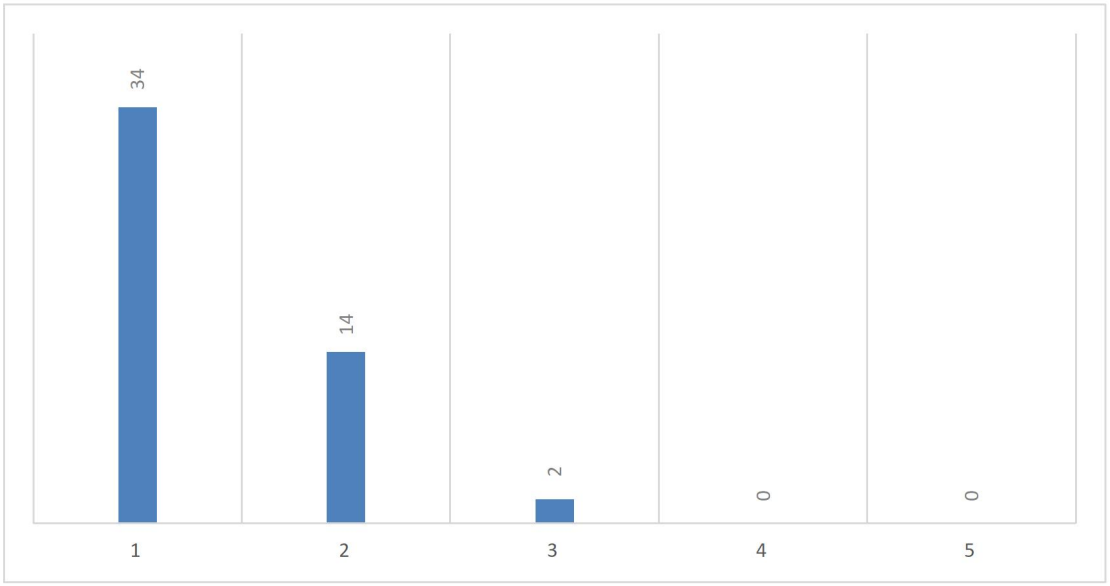

Figure 14: Implementation of effective risk assessment

34 respondents strongly agreed that the implementation of effective risk assessment can help an organisation prepare against security threats. Also, 14 of them agreed, while 2 respondents were neutral. This therefore implies that 48 people were positively disposed to the statement, thus, the effective implementation of risk assessment can guard against security threats.

6.3.3 Risk treatment.

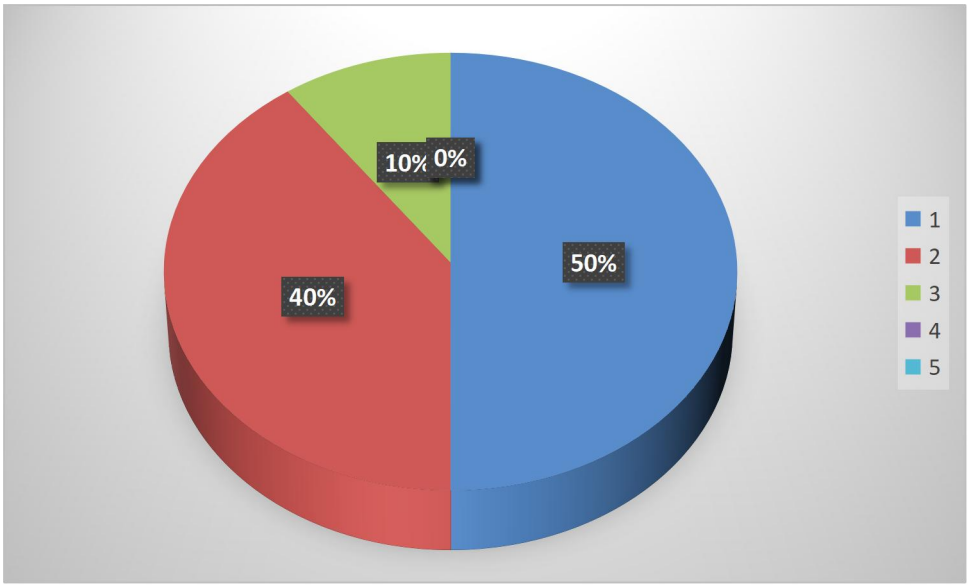

Figure 15: Risk treatment

59% of the respondents strongly agreed with the statement that risk treatment reduces the likelihood of incidences of security vulnerabilities. Also, 40% agreed to the statement, while 10% of the respondents remained neutral to the statement. This therefore implies that 90% of the respondents were positively disposed to the statement, which then means that risk treatment can reduce the likelihood of security vulnerabilities incidences.

6.3.4 Effective risk communication.

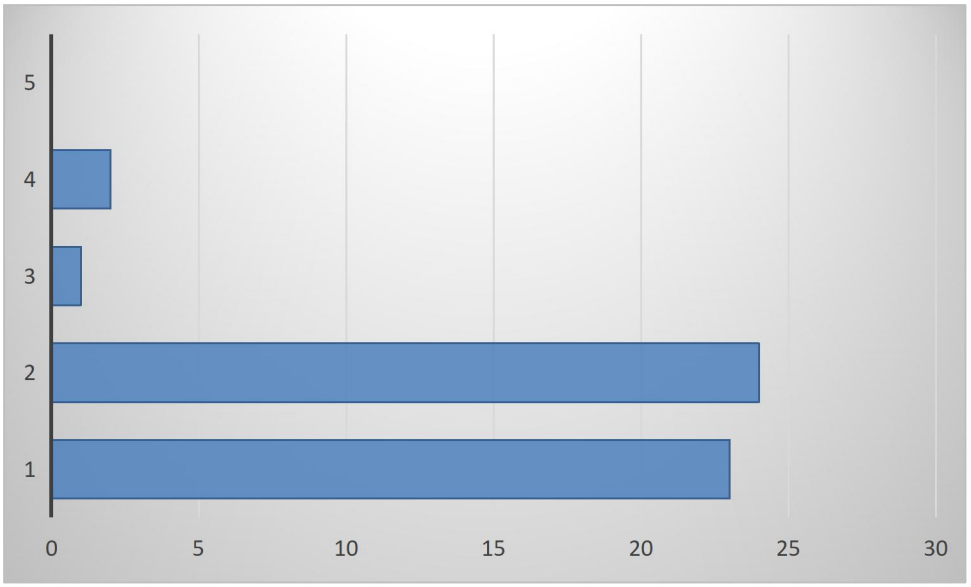

Figure 16: Effective risk communication

2 respondents disagreed with the statement that effective risk communication helps raise awareness about the potential risks and promote a security culture. Also, only one respondent took a neutral position to the statement. However, 24 and 23 respondents agreed and strongly agreed respectively to the statement. Therefore, since 47 respondents in total were in agreement with the statement, it therefore implies that effective risk communications can truly help to raise awareness on the potential risks and promote a security culture.

6.3.5 Monitoring and reviewing processes.

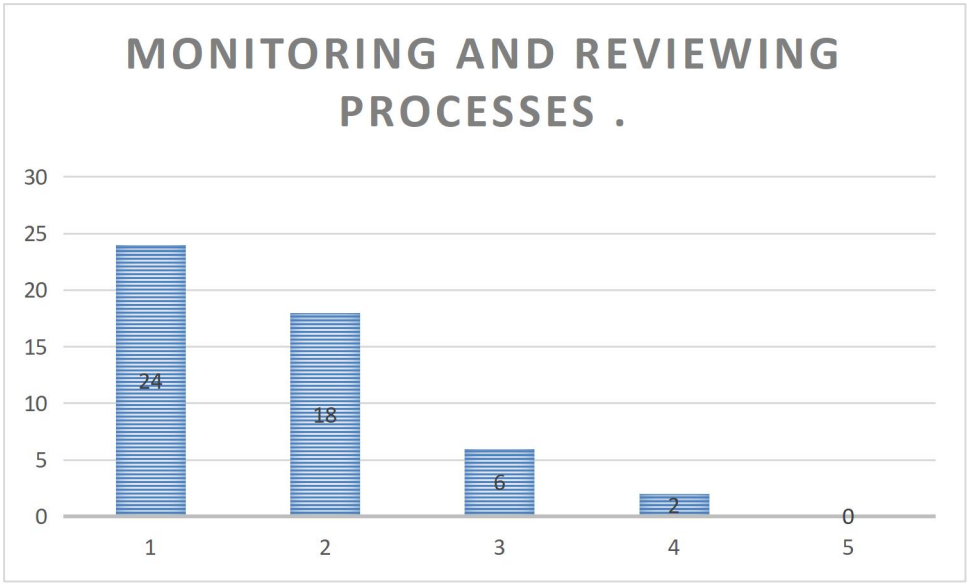

Figure 17 Monitoring and reviewing processes

On the statement about monitoring and reviewing processes helping in resilience against threats and helps ISO framework stay updated and effective, 24 respondents were strongly in agreement, while 18 other respondents agreed, 6 persons were neutral on the statement, while 2 individuals disagreed. Since 42 persons agreed with the statement out of 50 persons, it then implies that monitoring and reviewing processes can help maintain resilience against security threats and helps ISO framework stay updated and effective.

6.3.6 Access control.

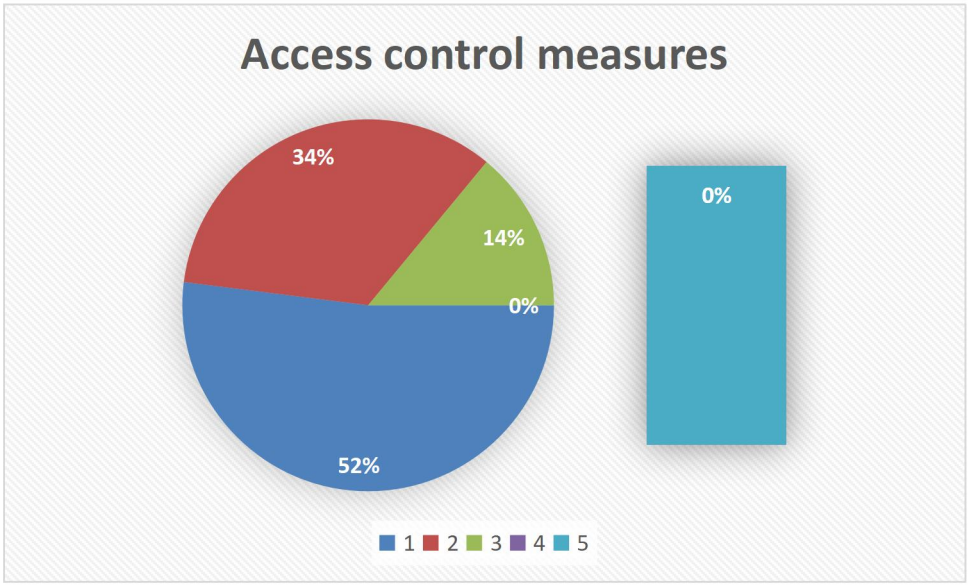

Figure 18 Access control measures

On whether the access control measure can enhance network performance, especially through processing overhead and latency, if implemented with network traffic. The figure above shows that 52% of the respondents strongly agreed, while 34% agreed, 14% were neutral. Thus, since the 86% of the respondents agreed with the statement, then it implies that access control can truly enhance network performance, especially through processing overhead and latency, if implemented with network traffic

6.3.7 Optimization of hardware and software.

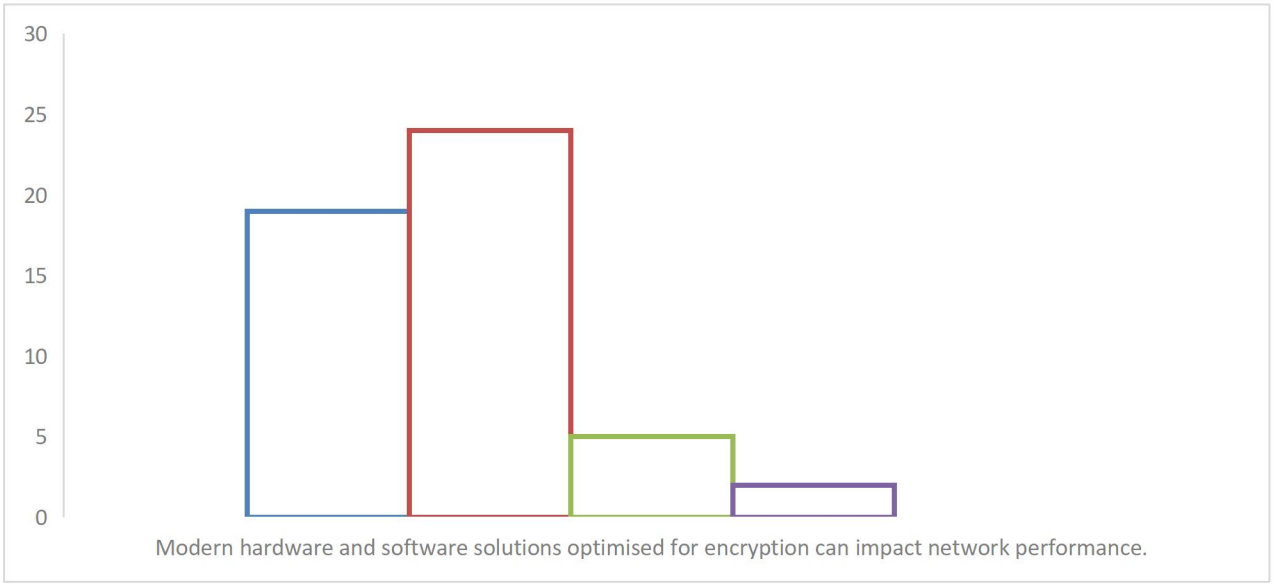

Figure 19 Optimization of hardware and software for encryption

The statement of if modern hardware and software solutions optimised for encryption can impact network performance. It was found that 19 respondents strongly agreed, while another 24 agreed. However, 5 respondents chose to be neutral with the statement, while 2 individuals disagreed with the statement. Since the 43 people agreed with the statement, as against the few who disagreed and were neutral, then indeed modern hardware and software solution optimised for encryption can impact network performance.

6.3.8 Authentication.

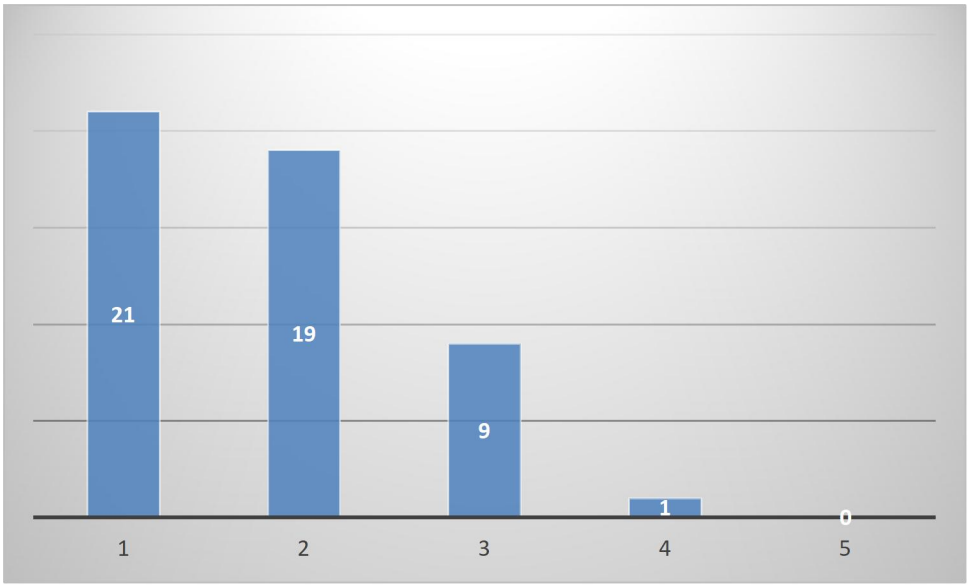

Figure 20: Authentication.

On the statement of whether an authentication can enhance network performance through additional processing and bandwidth for identity verification, it was found that 21 respondents strongly agreed to the statement, while 19 agreed. Also, 9 individuals were neutral to the statement and only one respondent disagreed. Therefore, since the 40 out of 50 respondents agreed with the statement, it therefore implies that authentication can truly enhance network performance through additional processing and bandwidth for identity verification.

6.3.9 Network segmentation.

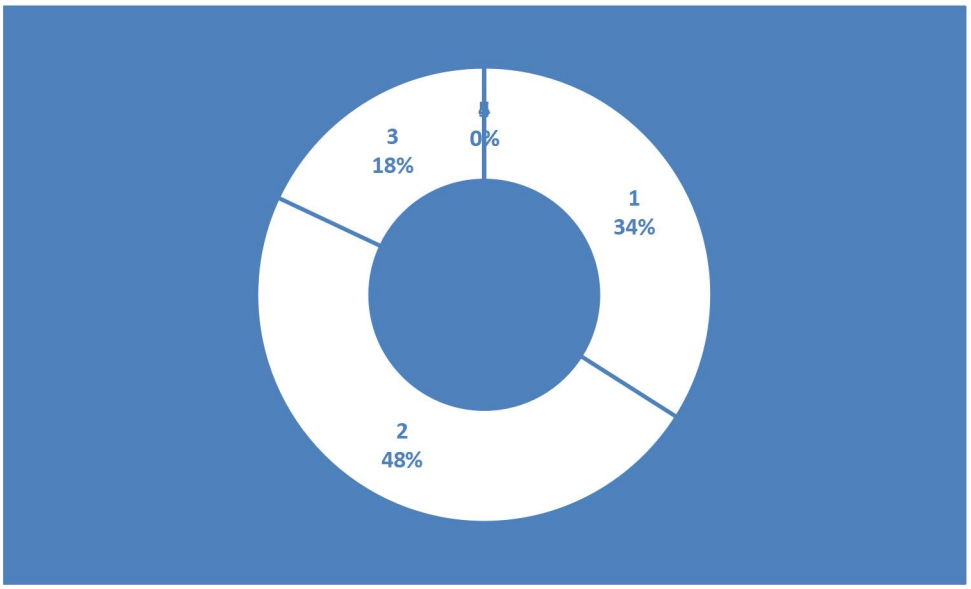

Figure 21: Network segmentation

This figure presents the responses of the survey participants on the if network segmentation can enhance network performance by reducing congestion and improving network availability. It was found that 34% of the respondents strongly agreed to the statement, while 48% agreed. Also 18% were on the neutral side as regards to the statement. Therefore, in as much as the larger percentage of the respondent have agreed to the statement, it then means that network segmentation indeed can enhance network performance by reducing congestion and improving network availability.

6.3.10 Intrusion detection and prevention systems

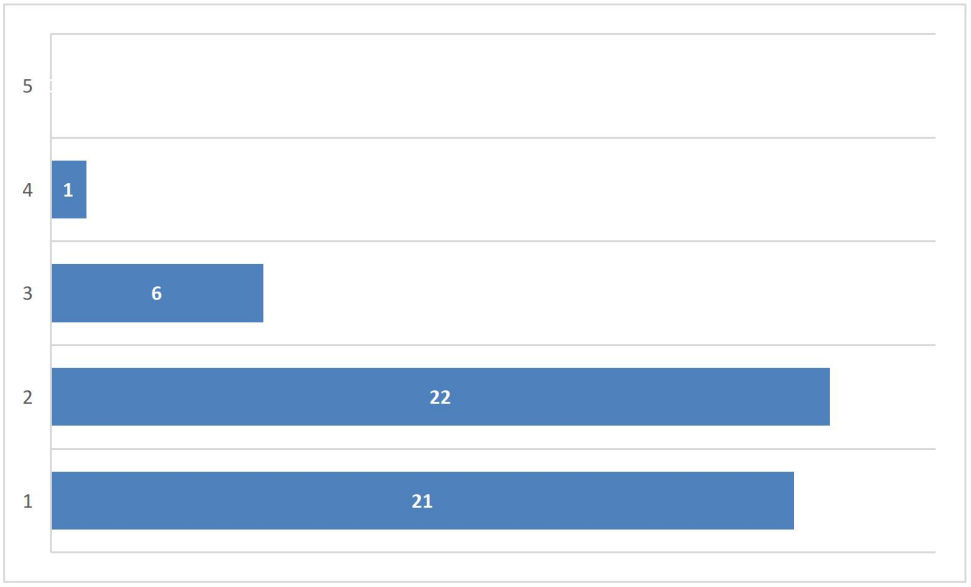

Figure 22: Intrusion detection and prevention systems.

The figure above represents the responses of the respondent on if intrusion detection and prevention systems can enhance IPv6 security network latency. One respondent disagreed with the statement, while 6 individuals were of neutral stand. However, 22 respondents agreed to the statement, while 21 strongly agreed to the statement. In view of that, 43 respondents in total agreed to the statement. This implies that intrusion detection and prevention systems can enhance IPv6 security network latency.

6.4 Thematic analysis

Table 2: Themes and coding

Categories	Theme	Sub-themes or Coding
Strategies to ensure compliance and governance	Implementation of network access control. Adoption of address	Access control Encryption

Categories	Theme	Sub-themes or Coding
	management Use of encryption implementation of intrusion detection and prevention. Regular vulnerability assessment Implementation of role-based access control. Provision of regular security training	Authentication Network segmentation Intrusion detection and prevention Security training
ISO framework implementation and risk management in IPv6	ISO risk management policy document ISO risk assessment ISO risk treatment ISO risk communication ISO monitoring and review Documentation and records Continuous improvement	Risk management policy Risk communication Risk treatment Risk assessment Monitoring and review

6.5 Hypothesis testing confirmation

Table 3: Correlation between risk management policy and risk management of ISO framework

		Risk management policy	risk management performance of ISO framework
Risk management policy	Pearson Correlation	1	1.2
	Sig. (2-tailed)		.0034
	N	75	75
risk management performance of ISO framework	Pearson Correlation	1.2	1
	Sig. (2-tailed)	.0034	
	N	75	75

H10: Risk management policy has no impact on risk management performance of ISO framework.

H11: Risk management policy has an impact on risk management performance of ISO framework.

The table above shows that there is a strong positive correlation to the tune of 1.2 between risk management policy and risk management performance of ISO framework. Also, risk management

policy is statistically significant at 0.0034 to risk management performance of ISO framework. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

Table 4: Correlation between risk assessment and risk management of ISO framework

		Risk assessment	risk management performance of ISO framework
Risk assessment	Pearson Correlation	1	1.12
	Sig. (2-tailed)		.003
	N	75	75
risk management performance of ISO framework	Pearson Correlation	1.12	1
	Sig. (2-tailed)	.003	
	N	75	75

H20: Risk assessment has no impact on risk management performance of ISO framework.

H21: Risk assessment has an impact on risk management performance of ISO framework.

The table above shows that there is a strong positive correlation to the tune of 1.12 between risk assessment and risk management performance of ISO framework. Also, risk assessment is statistically significant at 0.003 to risk management performance of ISO framework. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

Table 5: C orrelation between risk treatment and risk management of ISO framework

		Risk treatment	risk management performance of ISO framework
Risk treatment	Pearson Correlation	1	1.3
	Sig. (2-tailed)		.0028
	N	75	75
risk management performance of ISO framework	Pearson Correlation	1.3	1
	Sig. (2-tailed)	.0028	
	N	75	75

H30: Risk treatment has no impact on risk management performance of ISO framework.

H31: Risk treatment has an impact on risk management performance of ISO framework.

The table above shows that there is a strong positive correlation to the tune of 1.3 between risk treatment and risk management performance of ISO framework. Also, risk treatment is statistically significant at 0.028 to risk management performance of ISO framework. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

Table 6:Correlation between risk communication and risk management of ISO framework

		Risk communication	risk management performance of ISO framework
Risk communication	Pearson Correlation	1	1.36
	Sig. (2-tailed)		.0002
	N	75	75
risk management performance of ISO framework	Pearson Correlation	1.36	1
	Sig. (2-tailed)	.0002	
	N	75	75

H40: Risk communication has no impact on risk management performance of ISO framework.

H41: Risk communication has an impact on risk management performance of ISO framework.

The table above shows that there is a strong positive correlation to the tune of 1.36 between risk communication and risk management performance of ISO framework. Also, risk treatment is statistically significant at 0.002 to risk management performance of ISO framework. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

Table 7: Correlation between monitoring and reviewing and risk management of ISO framework

		Monitoring and reviewing	risk management performance of ISO framework
Monitoring and reviewing	Pearson Correlation	1	.08
	Sig. (2-tailed)		.005
	N	75	75
risk management performance of ISO framework	Pearson Correlation	.08	1
	Sig. (2-tailed)	.005	
	N	75	75

H50: Monitoring and review have no impact on risk management performance of ISO framework.

H51: Monitoring and review impact the risk management performance of ISO framework.

The table above shows that there is no linear correlation between monitoring and review and risk management performance of ISO framework at 0.08. However, Monitoring and reviewing is statistically significant at 0.05 to risk management performance of ISO framework. This shows that despite the statistical significance, there is no significant relationship between the two variables. Null hypothesis is thus accepted.

Table 8: Correlation between access control and security performance of IPv6 network

		Access control	Security performance of IPv6 network
Access control	Pearson Correlation	1	.99
	Sig. (2-tailed)		.0001
	N	75	75
Security performance of IPv6 network	Pearson Correlation	.99	1
	Sig. (2-tailed)	.0001	
	N	75	75

H60: Access control does not enhance the security performance of IPv6 network.

H61: Access control enhances the security performance of IPv6 network.

The table above shows that there is a weak positive correlation to the tune of 0.99 between access control and security performance of IPv6 network. Also, access control is statistically significant at 0.001 to security performance of IPv6 network. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

Table 9: Correlation between encryption and security performance of IPv6 network

		Encryption	Security performance of IPv6 network
Encryption	Pearson Correlation	1	1.2
	Sig. (2-tailed)		.0001
	N	75	75
Security performance of IPv6 network	Pearson Correlation	1.2	1
	Sig. (2-tailed)	.0001	

		Encryption	Security performance of IPv6 network
Encryption	Pearson Correlation	1	1.2
	Sig. (2-tailed)		.0001
	N	75	75
Security performance of IPv6 network	Pearson Correlation	1.2	1
	Sig. (2-tailed)	.0001	
	N	75	75

H70: Encryption does not enhance the security performance of IPv6 network.

H71: Encryption enhances the security performance of IPv6 network.

The table above shows that there is a strong positive correlation to the tune of 1.2 between encryption and security performance of IPv6 network. Also, encryption is statistically significant at 0.001 to security performance of IPv6 network. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

Table 10:Correlation between authentication and security performance of IPv6 network

		Authentication	Security performance of IPv6 network
Authentication	Pearson Correlation	1	1.22
	Sig. (2-tailed)		.0011
	N	75	75
Security performance of IPv6 network	Pearson Correlation	1.22	1
	Sig. (2-tailed)	.0011	
	N	75	75

H80: Authentication does not enhance the security performance of IPv6 network.

H81: Authentication enhances the security performance of IPv6 network.

The table above shows that there is a strong positive correlation to the tune of 1.22 between authentication and security performance of IPv6 network. Also, authentication is statistically significant at 0.011 to security performance of IPv6 network. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

Table 11: Correlation between network segmentation and security performance of IPv6 network

		Network segmentation	Security performance of IPv6 network
Network segmentation	Pearson Correlation	1	1.26
	Sig. (2-tailed)		.004
	N	75	75
Security performance of IPv6 network	Pearson Correlation	1.22	1
	Sig. (2-tailed)	.004	
	N	75	75

H90: Network segmentation does not enhance the security performance of IPv6 network.

H91: Network segmentation enhances the security performance of IPv6 network.

The table above shows that there is a strong positive correlation to the tune of 1.26 between network segmentation and security performance of IPv6 network. Also, network segmentation is statistically significant at 0.011 to security performance of IPv6 network. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

Table 12: Correlation between Intrusion detection and prevention and security performance of IPv6 network

		Intrusion detection and prevention	Security performance of IPv6 network
Intrusion detection and prevention	Pearson Correlation	1	1.08
	Sig. (2-tailed)		.0048
	N	75	75
Security performance of IPv6 network	Pearson Correlation	1.08	1
	Sig. (2-tailed)	.0048	
	N	75	75

H100: Intrusion detection and prevention do not enhance the security performance of IPv6 network.

H101: Intrusion detection and prevention enhance the security performance of IPv6 network.

The table above shows that there is a strong positive correlation to the tune of 1.08 between intrusion detection and prevention and security performance of IPv6 network. Also, intrusion detection and prevention is statistically significant at 0.048 to security performance of IPv6 network. This shows significant relationship between the two variables. Null hypothesis is thus rejected.

7 Conclusion, recommendation, and discussion

7.1 Overview

This chapter is expected to elucidate on the findings of the survey analysis. It will expatiate each of the variable in line with the findings and what other scholars have done and conclude on whether the objective is achieved or not and then link the findings to a similar study

7.2 Discussion

Both quantitative and qualitative data were collected from the survey participants comprising different professionals within the Information technology (IT) sector, these data were collected to measure objectives three and four and to accept or reject the hypothesis formulated, as well as to answer the research question posed.

Objective three was to formulate and develop a strategy to ensure compliance and governance of IPv6 security network. From both qualitative and quantitative data analysed above, the identified strategies are access control, encryption, authentication, network segmentation, intrusion detection and prevention as well as security training.

Access control allows organisations to manage who has authority to access corporate data and resources. With secure access control in place, organisation is able to use policies to verify users claim on who they claim to be and this ensures that the right access control is given to the authorised used. This is because implementation of this strategy is very critical to ensuring IPv6 network security. Without a control on who can access what on the organisations IPv6 network, there could be an issue of data breaches and phishing attack, on-path attack, buffer overflow attack, KRACK attack (Saxena, 2019), among others. There are different ways through which access control works, for example, physical access control helps to create an access control list to check IDs and ensure people accessing the network are authorised to do so, password can as well be used, thumbprint scan, among others. It is therefore not surprising that the larger percentage of the respondents chose access control as one of the strategies that can ensure compliance and governance of IPv6 security network, as it was also found that access control measures can enhance network performance especially through processing overhead and latency, if implement with IPv6 network traffic. This finding therefore corroborates the findings of Parameswari, (2019). On this note, it is therefore safe to conclude that access control impacts IPv6 network security performance.

Encryption is another identified strategy, it is a significant privacy tool when sensitive, confidential, and personal data is sent across the Internet network. It scrambles plain text into a form of secret code which malicious attackers cannot read, even if they hijack the network and access the file before it reaches its intended recipients. What makes encryption a IPv6 network security strategy is that when the recipients receive the message, they have their own key to unscramble the information into readable format. Encryption may be symmetric and asymmetric. The former uses a single password to encrypt and decrypt data, while the latter, uses two keys to encrypt and decrypt, alongside a public key shared among users and private key which is not shared. Encryption keeps IPv6 network secure through secure sockets layer (SSL), which is a form of crypted data sent to and from a website and keeps hackers from accessing the data while on transit (Rafter, 2022). This probably could have formed the basis for the respondents recognizing it as a strategy to ensure compliance and governance, thus, modern hardware and software solutions optimised for encryption can impact IPv6 network security performance. This finding therefore aligns with the findings of Malladi (2019). As such, it can be concluded that encryption impact IPv6 network security performance.

Authentication technology is another identified strategy. It provides access control for systems by verifying that the users' credential matches the ones in the database of authorised users or in a data authentication server. This is done to secure the systems, processes, and organisation information security. This strategy identifies the use of single-factor-authentication, however, in the recent times, unique code as an authentication factor has been introduced to provide further security to the network asset and prevent intruders from access the network. In the same vein, authentication can go further by requiring user id and password or 2-factor authentication, which require id, password, and biometric signature. Since most of the respondent supported this statement, it is therefore safe to conclude that authentication can enhance IPv6 network performance through additional processing and bandwidth for identity verification. This outcome is line with the findings of Rafter (2022), therefore, authentication impact positively the IPv6 network security performance.

Another variable identified as one of the strategies is network segmentation. This strategy allows helps organisation to divide their network into smaller, distinct sub-networks that allows the network teams to compartmentalize the sub-networks and deliver unique security controls and services to each of the sub-network. This strategy allows IPv6 network to be partitioned into sub logical networks for easy control. A large fiat IPv6 network is an attractive ground for malicious attackers, but with this segmentation, the attack surfaces are reduced and prevent lateral movement. The larger percentage of the respondents favoured network segmentation as a strategy for

compliance and governance of IPv6 network, as such it can be concluded that the variable impact positively the IPv6 network performance, because it has the capacity to reduce congestion and improve network availability due to the partitioning. These findings corroborate the findings of de Oliveira (2017)

Intrusion detection and prevention system is a network security strategy identified from the response of the survey participants. It is a tool used in continuously monitoring a network for malicious contents or activity and then prompt the users to promptly take action to prevent such intrusion. It is usually placed inline in the flow of network traffic between source and destination just behind the firewall. Larger majority of the respondents believed it can impact compliance and governance of IPv6 network security. Thus, it is therefore concluded that it can enhance IPv6 network security latency.

Objective four was about conducting survey on the implementation of ISO frameworks to risk management in IPv6. It was found that ISO frameworks such as risk management policy, risk assessment, risk treatment, risk communication and monitoring and review all have positive impact on risk management performance in IPv6.

In term of risk management policy, almost all of the respondents agreed that organisation should have a risk management policy because it is necessary for ISO framework risk performance. The essence of having risk management policy on ground for ISO framework risk performance is to demonstrate the readiness of any organisation to anticipate risks, assess it, avoid excessive risk, embrace necessary or desirable risk with the right safeguards. There is no organisation that is risk-free, However, risk management policy shows the readiness of the organisation to frontally tackle any risk that may surface. It is therefore safe to conclude that having risk management policy in place will help organisation to perform exceptionally in their risk management performance, which is what ISO framework intends to achieve to engender high level of preparation for risk. This outcome mirrors the position of Thensen (2019).

Risk assessment is another ISO framework strategy needed to enhance the risk management performance in IPv6 network security. It provides a systematic approach for the identification and evaluation of potential risk that the IPv6 network poses to an organisation. it tends to protect the network asset from threats to information confidentiality, integrity and availability (CIA). Because the process identifies areas for vulnerability and helps to create suitable controls so as to reduce attack risks, larger percentage of the respondents agreed that by implementing effective risk assessment, network assets can be well protected, as incidents of risks are preventing, detected and

responded to on time. it is therefore safe to conclude that risk assessment has a positive impact on risk management performance in IPv6 network. This thus aligns with the position of Miessler (2015); de Oliveira (2017)

Almost all the respondents agreed that risk treatment enhances the risk management performance of IPv6 network and this is because it involves the selection and implementation of right risk prevention strategies to reduce the probability and the effect of the identified risks. The process of risk treatment within the risk management of the IPv6 network, prioritises and allocates resources effectively, and it ensures that the most critical risks are expressly addressed. When an organisation ensures there is effective risk treatment implementation, there is a high likelihood to reduce incidences of security vulnerabilities which may lead to different attacks, thereby reducing the probable event of such incidents occurring. On this premise, it is therefore concluded that risk treatment reduces the likelihood of IPv6 network security attack. Thereby justifying the position of Henriksen (2006); Bacon, 2017)

Communication is important when it comes to risk management, effective sharing of risk communication has been found to enhance risk management performance. This is because sharing information's on risks and the risk management strategies with all the stakeholders will keep them abreast of the happening within the risk management portfolio and this is why risk management policy comes in handy. Effective risk communication enhances awareness creation about the likelihood of potential risks and promotion of security consciousness and culture. With the right risk communication, stakeholders will be in the known of the risk management strategies being pulled by the management. Not only that, it will also bring them up to speed with their roles and responsibilities in ensuring that such strategies are well implemented. This therefore affirms the reason why the larger percentage of the respondents opined that risk communication is highly needed in the risk management performance in IPv6 network.

The ISO framework is positively disposed to monitoring and review, and the larger percentage of the respondents agreed that the process can help to maintain resilience against any form of security threats and make ISO framework stay updated and effective in tackling any form of security vulnerabilities. Specifically, monitoring and review helps to identify changes in the risk profile of an organisation and ensuring that the risk management strategies implemented are adapted with accordingly.

7.3 Conclusion

Objective one was to assess the implementation of the ISO risk management framework. This was achieved in chapter four, section 4.2, sub-section 4.2.1, such it can be concluded that implementing an effective ISO risk management framework can improve the performance of an organisations if the procedures are followed properly and the organization follows the correct regulations. Implementing IoT security with the ISO framework, the established controls are designed to identify and prevent threats.

Objective two was to enforce security measures in all phases of IOT. This was achieved in chapter three, where functionality, technical, and business risks are well guarded against to protect data confidentiality, integrity, and availability in the IoT devices.

Objective three was to formulate and develop a strategy to ensure compliance and governance, and this was achieved in chapter two and chapter seven of this work and some of such strategies are access control, encryption, authentication, network segmentation among others. Objective four was also achieved in chapter seven where it was concluded that ISO framework such as risk management policy, risk treatment, risk assessment, risk communication and monitoring and reviewing were all important for the risk management performance in IPv6 network.

The proposed framework for risk management doesn't reinvent the wheel. It adds to the existing standards related to the Internet of Things (IoT). It provides a more proactive approach to managing risk that enables leaders to stay ahead of the curve and manage the transition to IPv6.To align operations with the company's objectives and maximize return on investment, it is important to consider the various risks and opportunities that can affect the business.

To avoid becoming a victim of the IoT device marketing hype, enterprises should consider hiring experts to help them manage their security and risk. This includes penetration testers, network engineers, and security analysts who have extensive experience with both IPv6 and IPv4. They know that even though compliance is not always prioritized, monitoring security is vital. Project managers who are knowledgeable about security and have the necessary skills to ensure that all hardware purchases are IPv6 compatible. Before implementing the latest standards, it's important that organizations thoroughly research the requirements and ensure that they can rely on them. Doing so will allow them to avoid getting hit by the security bugs that can arise from the IoT. Another promising area of research is the development of a fog computing layer that can help reduce the complexity of implementing security controls in the IoT.

The study was focused on the management of risk within an organization, not on the security of individuals or their homes. It only mentioned IPv6 as the preferred protocol for interfacing with IoT devices, though there are other protocols.

7.4 Implication of the study

The lack of a comprehensive risk and security policy for the Internet of Things (IoT) is a major issue that continues to raise questions about the potential impact of this standardization. Although this is being worked on, the lack of a clear and consistent approach to managing this issue is still puzzling. As a result, it is very important that organizations implement a strategy that is geared toward addressing these issues. The complexity of the Internet of Things (IoT) and Big Data has created a daunting challenge for governments and enterprises. Due to the complexity of the Internet of Things (IoT), it can be hard for an organization to understand how to implement and manage it. This is especially true for small and medium-sized businesses. In some cases, the use of IoT technologies has been approved by the IT department. Without realizing that they are using the Internet of Things (IoT). senior management members of companies are not aware of the potential risks that they are exposed to. This means that they are not able to monitor the various attack vectors and threats that are associated with this technology. Therefore, inherent risks associated with the Internet of Things (IoT) are due to the lack of security in the various processes involved in the development of these devices. This study has therefore provided information on risk management strategies using ISO framework for organisations to protect themselves against different forms of attack. . It has added to the existing standards related to the Internet of Things (IoT). It provides a more proactive approach to managing risk that enables leaders to stay ahead of the curve and manage the transition to IPv6.

7.5 Recommendations

Based on the findings of this work, the following recommendations are made

i. On the risk management policy, framework such as ISO 31000 or NIST cybersecurity can serve as a guide to formulate a more substantial risk management policy that will serve as best practices for organisation to identify, assess and manage risks effectively.

ii. Having affirmed that risk assessment has positive impact on the risk management performance, it is imperative to always define the scope of the risk assessment, this will help with a thorough

analysis of the network to identify certain threats and vulnerabilities and help come up with bespoke strategy to mitigating them.

iii. Although enhancement of risk communication may not totally resolve network vulnerabilities and threats, even though poor risk communication can enhance those threats. However, risk communication must be closely linked to the risk management and risk managers must understand and accept that risk communication is a continuous affair and never one-off issue. This will help to quickly identify and prevent network exposures to malicious attack threats.

iv. To make risk treatment more effective, risk manager must deploy suitable security controls, as well as prioritizing risks. This will help to develop a comprehensive risk management plan that carries all stakeholders along and strong enough to identify and mitigate against any threat

Reference

AbdAllah, E.G.,Zulkernine,M.,Hassanein, H.S.,2018. Preventing unauthorized access in information centric networking, Harvard: P. 234

Act, A., 1996. Health insurance portability and accountability act of 1996, Chicago: P. 13

Ahmadalinejad, M. and Hashemi, S.M.,2015. "A national model to supervise on virtual banking systems through the Bank 2.0 approach.", Chicago: IEEE.

Ahsan, K.,Ho,M. and Khan,S., 2013. Trend analysis of car recalls, Harvard:

Tapolcai,J., Ho, P.H.,Barbarczi,P., 2015. The segment routing architecture, Harvard: IEEE Global Communications Conference (Globecomm),.

Al-Khafaji, A., 2018. Obstacles and reasons that prevent transition to IPv6., Harvard:.

Alhasan, A.,Audah,L.,Ibrahim,I.,Al-Asharaa, A.,Al-Ogaili,A.S. and M.Mohammed, J.,2022. A case-study to examine doctors' intentions to use IoT healthcare devices in Iraq during Covid-19 pandemic, Harvard:

Amoore, L.,2018. Cloud geographies: Computing, data, sovereignty. Progress in Human Geography, Harvard:

LAN/MAN Standards Committee of the IEEE Computer Society, 2020. IEEE Std 802.15.4-2020 - IEEE Standard for Low-Rate Wireless Networks. [Online] Available at: https://ieeexplore.ieee.org/document/9144691 (accessed 02 June 2023).

Anu P,. and S.Vimala. 2017. A survey on sniffing attacks on computer networks, Harvard: IEEE.

Aravind, S and Padmavathi, G 2015. Migration to IPv6 from IPv4 by dual stack and tunneling techniques, India: s.n.

Armitage, G. J., 2002. Inferring the extent of network address port translation at public/private Internet boundaries., Harvard:

ATH, 2023 Data presentation-Types and its importance. Available at: https://analyticstraininghub.com/data-presentation-types-importance/ (Accessed 03 March 2023)

Atlasis, A., 2012. Attacking ipv6 implementation using fragmentation. Blackhat europe, pp.14-16..

Aura, T. and Roe,M., 2006. Designing the mobile IPv6 security protocol., Harvard: PRESSES POLYTECHNIQUES ROMANDES..

Bacon, M., 2017. St. Jude Medical finally patches vulnerable medical IoT devices, Chicago: Search Security Techtarget.

Banerjee, A., Chaudhury, S., Singh, D.K., Banerjee, I., Mahato, A.K. and Haldar, S., 2007. Statistics without tears-inputs for sample size calculations. Indian Psychiatr Jr, 16, pp.150-2.

Banerjee, A and Chaudhury, S. 2010. Statistics without tears: populations and samples. Ind Psychiatry J; 19(1); 60-65

Barcena, M. B. 2015. Insecurity in the Internet of Things, Chicago: Security response, symantec.

Barfield, R., 2007. Risk appetite–How hungry are you.,Harvard

Barker, K., 2013. The security implications of IPv6., Harvard: Network Security.

Benaroch, M., 2002. "Managing information technology investment risk: A real options perspective.", Chicago: IEEE.

Bhatt, S., Manadhata, P.K and Zomlot, L., 2014. The operational role of security information and event management systems, Chicago: IEEE.

Blaxter, L., Hughes, C. and Tight, M. (2006) How to Research, 3rd edn. Buckingham: Open University Press.

Blaze, M. Ioannidis, J. and Keromytis,A.D., 2002. Trust management for IPsec., Harvard:.

Board, 2013. Financial Stability. "Principles for an effective risk appetite framework, Harvard: IEEE

Board, 2022. Why cyber risk communication is an important part of cybersecurity. Available at https://www.boardish.io/why-cyber-risk-communication-is-an-important-part-of-cybersecurity/#:~:text=What%20Is%20Cyber%20Risk%20Communication,how%20they%20can%20be%20mitigated. (Accessed 03 March 2023)

Bound, J. B and Mike. C., 2003. RFC3315: Dynamic host configuration protocol for IPv6 (DHCPv6, Chicago: s.n.

Bowling, D. 2005. Success factors for implementing enterprise risk management: building on the COSO framework for enterprise risk management to reduce overall risk., Harvard: s.n.

Brandt, A., Hui,J., Kelsey,R., Levis,P.,Pister,K., Struik,J.P Vasseur,J.P. and Alexander,R,. 2012. RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, Chicago: IEEE.

Brass, I. , 2021. Adaptive governance for the Internet of Things, Chicago: s.n.

Brock, D. L., 2001. The electronic product code (epc), Chicago: IEEE.

Caicedo, C. E. Joshi, J.B and Tuladhar,S.R., 2009. IPv6 security challenges, Harvard: s.n.

Caldwell, J, 2016 “IBM Internet of Things Point of View and Strategy,” IBM, [Online]. Available: https://www.ieeetoronto.ca/wp-content/uploads/2020/06/TOR-IEEE-IBM-IoT-Jan-28-2016-Final.pdf. [Accessed Feburary 2023].

Chapman, C., 2004. Bringing ERM into focus. In: A new COSO study provides some much-needed clarity and structure to the fluid topic of enterprise risk management.. Chicago: Internal Auditor, pp. 30 - 36.

Chelius, G. Fleury,E. and Toutain, L., 2005. Administration Protocol (NAP) for IPv6 router auto-configuration., Chicago: IEEE.

Cho, K., Luckie,M. and Huffaker,B., 2004. Identifying IPv6 network problems in the dual-stack world, Chicago: s.n.

Chowdhury, M.F. 2014.Interpretivism in Aiding Our Understanding of the Contemporary Social World. Open Journal of Philosophy, 04(03), pp.432-438

Colitti, L. D. B2004. Colitti, L., Di Battista, G. and Patrignani, M, Harvard: IEEE.

Colletaz G., Hurlin,C. and Perignon, C 2013. the Risk Map: A new tool for validating risk models. Journal of Banking & Finance, Vancouver: IEEE.

Cooper, D., Purdy, G., Wood, M., Bosnich, P., Raymond, G., Grey, S., Walker, P. 2014. Project Risk Management Guidelines: Managing Risk with ISO 31000 and IEC 62198. United Kingdom: Wiley. P432

Cybenko, G. A, 2004. Cognitive Hacking, Chicago: s.n.

Dali, A., 2012. ISO 31000 risk management, Chicago: EDPACS.

David, M. and Sutton, C. 2004. Social Research: The Basics. London: Sage

Davies, J., 2012. Understanding IPv6: Understanding IPv6 , Chicago: Pearson Education.

de Oliveira, U.R.,Marins,F.A.S.,Rocha, H.M. and Salomon, V.A.P., 2017. The ISO 31000 standard in supply chain risk management, Chicago: s.n.

Dean, K., Joseph, J., Roberts, J. and Wight, C., 2006. Realism, Philosophy and Social Science

DeNardis, L., 2006. Questioning IPv6 Security, Chicago: Business Communications Review Magazine.

Depren, O. M. 2005. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks, Chicago:

Dey, A. R 2016. Home automation using Internet of Thing, New York: IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON

Do, S. L., 2019. SDN/NFV-based network infrastructure for enhancing IoT gateways, Chicago: IEEE.

Doff, R., 2008. A critical analysis of the Solvency II proposals. In: The Geneva Papers on Risk and Insurance-Issues and Practice. 33(2). 193 - 206.

Durdagi, E.and Buldu,A., 2010. IPv4/IPv6 security and threat comparisons, Chicago: WCES.

Elleithy, K. B., 2005. Denial of service attack techniques: analysis, implementation and comparison, Harvard: s.n.

Elmore, H.,Stephens, B. and Camp,L.J., 2008. Diffusion and adoption of IPv6 in the arin region, Chicago: SSRN.

Faber J, and Fonseca LM. 2014. How sample size influences research outcomes. Dental Press J Orthod. 19(4):27-9. DOI: http://dx.doi. org/10.1590/2176-9451.19.4.027-029.ebo

Fabig, C and Hassper, A, 2018. Secure Your Business: Insights to Governance, Risk, Compliance & Information Security. Germany: BoD-Books on Demand. P164

Feldner, B. and Herber,P., 2018. A qualitative evaluation of IPv6 for the Industrial Internet of Things, Chicago: Procedia Computer Science.

Firdous, S. N., Baig, Z., Valli, C. and Ibrahim,A., 2017. Modelling and evaluation of malicious attacks against the iot mqtt protocol, Chicago: IEEE.

Flick, U, 2011. Introducing research methodology: A beginner's guide to doing a research, Sage.

Gabriel, D. 2013. Inductive and deductive approaches to research. Available at: https://deborahgabriel.com/2013/03/17/inductive-and-deductive-approaches-to-research/ (Accessed 03 March 2023)

Gjerdrum, D. 2009. The new international standard on the practice of risk management–A comparison of ISO 31000: 2009 and the COSO ERM framework. Risk management, Harvard: s.n.

Greer, C. D., 2014. NIST framework and roadmap for smart grid interoperability standards, Chicago: s.n.

Hagen, S., 2006. IPv6 essentials, Harvard: O'Reilly Media,inc.

Hamelmann E., Beyer,K.,Gruber, C., Lau.S.,Matricardi,P.M.,Nickel,R., Niggemann,B. and Wahn,U., 2008. avoiding risk or providing protection, Vancouver: s.n.

Henriksen, P. and Uhlenfeldt, T.,2006. Contemporary Enterprise-Wide Risk Management Frameworks: A Comparative Analysis. In: Chicago: pp. 107 - 129.

Hiles, A., 2012. Enterprise risk management, Chicago: The definitive handbook of business continuity management.

Hudson, D., 2017. Value propositions for the Internet of things, Harvard: s.n.

Huston, G., 2013. A Primer on IPv4, IPv6 and Transition, Harvard: The ISP Column, Internet Society.

Ibhaze, A.E., Okoyeigbo,O., Samson,U.A., Obba,P. and Okwakwu, I.K., 2020. Performance evaluation of IPv6 and IPv4 for future technologies, Harvard: Springer, Cham.

IEEE, 2012. "IEEE Standard for Local and metropolitan area networks, Chicago: Wireless Body Area Networks.

IEEE, 2016.. IEEE Standard for Low-Rate Wireless Networks, Chicago: IEEE. P. 2

Indrayan A. 2008. Basic methods of medical research. India: AITBS Publishers. p. 116

Javaid U, S.., 2018. Mitigating loT device-based DDoS attacks using blockchain., Vancouver: 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems.

Jong Hyuk park, M and Hsiao- Hwa Chen, H., 2009. Advance in information security and assurance, Chicago: s.n.

Jung, M. M. K. 2014. Variational image segmentation models involving non-smooth data-fidelity terms, Chicago: s.n.

Kafle, V. P. 2016. Internet of things standardization in ITU and prospective networking technologies, Chicago: s.n.

Kim, D., Solomon, M. G. 2013. Fundamentals of Information Systems Security. United States: Jones & Bartlett Learning. P544

Kleffner A. 2003. The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. Risk Management and Insurance Review., Vancouver: s.n.

Korkusuz, A. Y., 2012. ntroduction to IPv6 and benefits of IPv6., Chicago: Electrical-Electronics Engineering Department.

Laghari,A., 2021. A review and state of art of Internet of Things (IoT)., Chicago: Archives of Computational Methods in Engineering.

Lam, J., 2017. Implementing enterprise risk management, Harvard: s.n.

Lee, I., 2020. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management, Harvard: IEEE.

Leedy, P. D. 1993. Practical research: planning and design. New Jersey: Prentice-Hall.

Lehmann, B. N., 1990. "Residual risk revisited., CHicago: s.n.

Lengnick-Hall, M. L. , 2003. The impact of e-HR on the human resource management function, Chicago: Journal of labor research, 2(1), 12-16.

Leu, F. L.., 2015. S-PMIPv6: An intra-LMA model for IPv6 mobility, 2015: Computer Applications.

Library, 2019. Public health research guide: primary and secondary data definitions. Available at: https://cdn.ymaws.com/www.safestates.org/resource/resmgr/connections_lab/glossary_citation/Primary__Secondary_Data_Defi.pdf (Accessed 03 March 2023)

LO., N., 2017. Using the CIA and AAA models to explain cybersecurity activities, Vancouver: PM World Journal..

Loshin, P., 2004. IPv6: Theory, protocol, and practice., Chicago: s.n.

Malladi, S., 2019. Bug bounty programs for cybersecurity: Practices, issues, and recommendations., Harvard: IEEE.

Marsan, C., 2006. Network Time Protocol works with IPv6;* Moonv6 demonstrates that NTP runs over IPv6, Harvard: Network World.

Maurizio Aiello, E. C. 2014. An on-line intrusion detection approach to identify low-rate DoS attacks, s.l.: In Proceedings of the International Carnahan Conference on Security Technology (ICCST'14).

Microsoft, 2023. Microsoft learn. [Online]
Available at: https://learn.microsoft.com/en-us/dotnet/fundamentals/networking/IPv6-overview#IPv6-auto-configuration (Accessed 03 March 2023)
Miessler, D., 2015. Securing the Internet of things: Mapping attack surface areas using the OWASP IoT, Chicago: s.n.
Mitchell, S., 2017. GRC Capability Model (Red Book) in Paperback, Harvard: s.n.
Mockapetris, P. 1988. Development of the domain name system., Harvard: s.n.
Molina-Castilo, F and Munuera-Aleman, J. 2009.The joint impact of quality and innovativeness on short-term new product performance. Industrial Marketing Management; 38(8), pp. 984-993.
Morabito, R., 2017. Virtualization on Internet of things edge devices with container technologies: A performance evaluation, Chicago: IEEE.
Morton, D., 1997. Understanding IPv6., Harvard: Network Advisor.
N-able, 2023. Network risk management. Available at: https://www.n-able.com/features/network-risk-management#:~:text=Network%20risk%20management%20attempts%20to,as%20digital%20information%20in%20transit. (Accessed 03 March 2023)
Nikander, P.,Gurtov,A and Henderson,T.R.,2010. Host identity protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks, Harvard: IEEE.
Nikander, P. Kempf, J. and Nordmark, E., 2004. IPv6 neighbor discovery (ND) trust models and threats, Chicago: s.n.
Nikolina, K., 2022. Overview of the progress of IPv6 adoption in Croatia, Chicago: Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO).
Oliveira, L.M., De Sousa,A.F. and Rodrigues,J.J., 2011. Routing and mobility approaches in IPv6 over LoWPAN mesh networks, Harvard: International Journal of Communication Systems,
Open Learn, 2020. Understanding different research perspectives. Available at: https://www.open.edu/openlearn/money-management/understanding-different-research-perspectives/content-section-6 (Accessed 03 March 2023)
Pachgharge, V, 2019. Cryptography and information security, third edition.): PHI Learning Pvt. Ltd..
Parameswari, M. amd Moses, M.B.,2019. Efficient analysis of water quality measurement reporting system using IOT based system in WSN, Chicago: s.n.
Pironti, J., 2010. Developing an information security and risk management strategy., Harvard: s.n.
Porter, M. E.., 2001. ilustraciones Gibbs. "Strategy and the Internet, Chicago: s.n.

Radanliev, P. De Roure,D.,Nurse J.R.Nicolescu,R., Huth,M Cannaday,S. and Montaivo, R.M., 2019. Cyber risk impact assessment-assessing the risk from the IoT to the digital economy., Harvard: s.n.

Rafter, D, 2022. What is encryption and how does it protect your data? Available at: https://us.norton.com/blog/privacy/what-is-encryption# (Accessed 03 March 2023)

Rapid7, 2023 cybersecurity risk management. Available at: https://www.rapid7.com/fundamentals/what-is-cybersecurity-risk-management/#:~:text=Cybersecurity%20risk%20management%20is%20the,pose%20threats%20to%20a%20business. (Accessed 03 March 2023)

Rosas, C., 2019. The future is femtech: Privacy and data security issues surrounding femtech applications., Harvard: s.n.

Rudestam, K. E. and Newton, R. 2007. Surviving Your Dissertation: a Comprehensive Guide to Content and Process, 3rd edn. Thousand Oaks, CA: Sage

Rukmana, D. 2014. Sample Frame. In: Michalos, A.C. (eds) Encyclopedia of Quality of Life and Well-Being Research. Springer, Dordrecht. https://doi.org/10.1007/978-94-007-0753-5_2551

Ryan, G., 2018. Introduction to positivism, interpretivism and critical theory. Nurse Researcher, 25(4), pp.14-20

Samonas, S. and Coss,D.,2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. , Harvard: Journal of Information System Security.

Sanghvi, H.P., and Dahiya,M.S., 2013. Cyber Reconnaissance: An Alarm before Cyber Attack. Cyber Reconnaissance: An Alarm before Cyber Attack, 63, p. 38.

Sarokin, D. 2020. What is a risk management policy statement? Available at: https://smallbusiness.chron.com/risk-management-policy-statement-68528.html (Accessed 03 March 2023)

Saunders, M. Lewis, P., &Thornhill, A. (2009) Research methods for business students.(eighth Edition) London.

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students, (6th ed.) London: Pearson.

Saunders, M.N.K., and Tosey, P., 2015. Handbook of Research Methods on Human Resource Development. Edward Elgar Publishing

Savolainen, T. J.., 2013. IPv6 addressing strategies for IoT, Harvard: IEEE Sensors.

Saxena, N. 2018. Practical Network Security: Auditees guide to zero findings. India: BPB PUBN. P. 250

Schiefer, M., 2015. Smart home definition and security threats, Chicago: IEEE.

Scribbr. 2020. Research methods/definitions, types and examples. Available at: https://www.scribbr.com/category/methodology/ (Accessed 03 March 2023)

Sen, J and Mehtab, S 2020. Computer and Network Security. United Kingdom: IntechOpen. P. 136

Setia, M., 2016. Methodology series module 3: Cross-sectional studies. Indian Journal of Dermatology, 61(3), p.261.

Shelby, Z. K.., 2014. RFC 7252: The constrained application protocol (CoAP)., Harvard: IEEE.

Shen, L., 2014. The NIST cybersecurity framework: Overview and potential impacts, Chicago: Scitech Lawyer.

Singalar S, B. R., 2018. Performance analysis of IPv4 to IPv6 transition mechanisms. I, Vancouver: Fourth International Conference on Computing Communication Control and Automation (ICCUBEA).

Singh D, S.., 2020. An overview of IoT hardware development platforms, Vancouver: s.n.

Srisuresh, P. ., 2001. Traditional IP network address translator, Chicago: s.n.

Supriyanto, I. H.., 2014. Risk Analysis of the Implementation of IPv6, Malaysia: National Advanced IPv6 Centre, Universiti Sains Malaysia, Malaysia.

Suresh, P. D., 2014. A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment., Harvard: IEEE.

Swetnam, D. (2000) Writing Your Dissertation: How to Plan, Prepare and Present Successful Work, 3rd edn. Oxford: How To Books

Szykman, S. S., 1999. The NIST design repository project, Harvard: Springer London.

Target, T., 2023. Tech Target Security. [Online]

Available at: https://www.techtarget.com/searchsecurity/definition/authentication-authorization-and-accounting (Accessed 03 March 2023)

Tashakkori, A, and Charles. 1998. Mixed Methodology: Combining Qualitative and Quantitative Approaches. Applied Social Research Methods Series, 46; Thousand Oaks: Sage Publications.

Tech-Faq, n.d. Tech-Faq. [Online]. Available at: https://www.tech-faq.com/packet-fragmentation.html (Accessed 13 February 2023)

The White House., 2013. Executive order -- Improving Critical Infrastructure Cybersecurity. [Online]

Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (Accessed 15 March 2023)

Themsen, T. N. 2018. The performativity of risk management frameworks and technologies, Chicago: s.n.

Tjensvold, J., 2007. Comparison of the IEEE 802.11, 802.15. 1, 802.15. 4 and 802.15. 6 wireless standards, Harvard: IEEE.

Tomaiko, E.., 2021. Cybersecurity threats to cardiac implantable devices, Chicagoo: s.n.

Tripathi, N.., 2021. Application layer denial-of-service attacks and defense mechanisms, Harvard: a survey. ACM Computing Surveys (CSUR).

Uslu, B. T.., 2019. Evaluation of the difficulties in the Internet of things (IoT) with multi-criteria decision-making, Cicago: s.n.

Vendatu, 2023. Presentation of data. Available at: https://www.vedantu.com/commerce/presentation-of-data (Accessed 03 March 2023)

Villalba, L. M.., 2011. Auto-configuration protocols in mobile ad hoc networks. Sensors, Harvard: s.n.

Villegas, F, 2023. Thematic analysis: what it is and how to do it? Available at: https://www.questionpro.com/blog/thematic-analysis/#:~:text=Thematic%20analysis%20is%20a%20method,making%20sense%20of%20the%20data. (Accessed 03 March 2023)

Voxco, 2021. The difference between exploratory and conclusive research. Available at: https://www.voxco.com/blog/the-difference-between-exploratory-and-conclusive-research/#:~:text=What%20is%20exploratory%20research%3F,reach%20conclusions%20or%20make%20decisions (Accessed 03 March 2023)

Waddington, D. 2002. Realizing the transition to IPv6, Chicago: IEEE Communications Magazine.

Weinberg, D., 2002. Qualitative research methods. Oxford, OX: Blackwell Publishers

Wu, P.., 2012. Transition from IPv4 to IPv6: A state-of-the-art survey., Harvard: IEEE.

Xenidis, Y. 2005. Identification and classification of risks in a new modelling process for build-operate-transfer projects., Chicago: s.n.

Žagar, D. K.., 2007. Security aspects in IPv6 networks–implementation and testing, Chicago: s.n.

Appendices

Questionnaire

Dear participants,

Kindly fill in your response to the survey questions presented below. There are two main parts after the demography part. The first part is to rank the order of your agreement with the statement posed, while the second part gives you the liberty to provide the answer you deem right to the question.
For the part that deals with ranking, five ranking scales strongly agree (SA), Agree (A), Neutral (N), Disagree (D) and strongly disagree (SD)

Demography

Please provide answers to the following

Education qualification:

Years of experience:

Position:

Certification:

Gender:

Part A

S/N	Statement	SA	A	N	D	SD
1	Organisations should not have a risk management policy because it is unnecessary for ISO framework risk performance.					
2	Implementation of effective risk assessment can help an organisation prepare against security threats.					
3	Risk treatment reduces the likelihood of incidences of security vulnerabilities.					

4	Effective risk communication helps raise awareness about potential risks and promote a security culture.					
5	Monitoring and reviewing processes can help maintain resilience against security threats and help the ISO framework stay updated and effective.					
6	Access control measures can enhance network performance, especially through processing overhead and latency, if implemented with network traffic.					
7	Modern hardware and software solutions optimised for encryption can impact network performance.					
8	Authentication can enhance network performance through additional processing and bandwidth for identity verification.					
9	Network segmentation can enhance network performance by reducing congestion and improving network availability.					
10	Intrusion detection and prevention systems can enhance IPv6 security network latency.					

Part B

From a business perspective, how will the IoT device be used, and what business value/ROI is anticipated?

What threat and attack vectors are expected, and how will they be mitigated against?

Who will be authorised to access the IoT device, and how will their identities be authenticated?

In the unfortunate event of an attack or vulnerability, what is the process for updating the IoT device?

Who is responsible for monitoring and reporting new attacks or vulnerabilities pertaining to the IoT device?

Has a cost-benefit analysis been conducted to evaluate risk scenarios against the anticipated business value?

What sensitive/personal information is collected, stored and/or processed by the IoT device?

Do we have the consent of the persons whose information is being collected and used?

How satisfied are you with IoT governance and Compliance? Would you evaluate room for improvement?

What are the major principles of implementing ISO frameworks to IPv6, and what are some challenges?

How frequently do you update or review its IPv6 security measures to be effective against evolving threats?

To what extent has implementation of IPv6 security measures impacted network performance, including latency, throughput, and availability?