



Al-Quds Open University

Faculty of Graduate Studies and Scientific Research

Master of Information Technology

**Cybersecurity Knowledge and Skills Applied in the Palestinian Customs
Police: A Case Study**

المعرفة والمهارات في مجال الأمن السيبراني التي يتم تطبيقها في جهاز الضابطة
الجمركية الفلسطينية: دراسة حالة

THESIS

by

Loai Basem Shalash

Student ID: 0330012210086

Supervisor

Dr. Waleed Awad

Submitted in Partial Fulfilment of the Requirements

For the Degree of Master of Information Technology at the Faculty of Graduate Studies

Ramallah, Palestine

July, 2025



Al-Quds Open University

Faculty of Graduate Studies and Scientific Research

Master of Information Technology

**Cybersecurity Knowledge and Skills Applied in the Palestinian Customs
Police: A Case Study**

المعرفة والمهارات في مجال الأمن السيبراني التي يتم تطبيقها في جهاز الضابطة
الجمركية الفلسطينية: دراسة حالة

THESIS

by

Loai Basem Shalash

Student ID: 0330012210086

Supervisor

Dr. Waleed Awad

Submitted in Partial Fulfilment of the Requirements

For the Degree of Master of Information Technology at the Faculty of Graduate Studies

Ramallah, Palestine

July, 2025

© 2025 Loai Shalash

Examination Committee Page

The committee for

Loai Basem Mohammed Shalash

certifies that this is the approved version of the following thesis and is acceptable in quality and form for publication in paper and in digital formats:

Cybersecurity Knowledge and Skills Applied in the Palestinian Customs Police: A Case Study

Committee Members

Committee Supervisor: **Waleed Awad**

Signature: _____

Date: _____ 2025/7/22 _____

Committee First Member: **Yousef Abuzir**

Signature: _____

Date: _____ 2025/7/23 _____

Committee Second Member: **Raed Daraghmeh**

Signature: _____

Date: _____ 2025/7/23 _____

Declaration

I, **Loai Basem Mohammed Shalash**, hereby declare that the work presented in this thesis has not been submitted for any other degree or professional qualification, and that it is the result of my own independent work.

Signed: **Loai Basem Mohammed Shalash**

Date: 2025/7/23

Abstract

Cybersecurity Knowledge and Skills Applied in the Palestinian Customs Police: A Case Study

This study explores the cybersecurity knowledge and skills required within the Palestinian Customs Police and the extent to which these skills are applied in daily operations. The research problem stems from the growing cybersecurity threats facing law-enforcement agencies and the limited studies that address the specific context of the Palestinian Customs Police.

A descriptive analytical approach was adopted, and data were collected through a questionnaire administered to 146 officers and staff members across various departments. The data were analyzed using SPSS, employing statistical methods to determine the relationship between available knowledge, operational skills, and the practical implementation of cybersecurity measures.

The findings indicate significant challenges, including insufficient specialized training, limited technical resources, and gaps in awareness of legal frameworks related to cybersecurity. Nevertheless, the results show notable initiatives and efforts by officers to apply cybersecurity practices despite these constraints.

This study provides evidence-based recommendations to strengthen training programs, improve technological resources, and develop clear policies that enhance the overall cybersecurity capacity of the Palestinian Customs Police.

المعرفة والمهارات في مجال الأمن السيبراني التي يتم تطبيقها في جهاز الضابطة الجمركية الفلسطينية: دراسة حالة

تتناول هذه الدراسة معرفة ومهارات الأمن السيبراني المطلوبة لدى جهاز الضابطة الجمركية الفلسطينية ومدى تطبيق هذه المهارات في العمليات اليومية. وتتبع مشكلة البحث من تزايد التهديدات السيبرانية التي تواجه أجهزة إنفاذ القانون، وقلة الدراسات التي تتناول السياق الخاص بالضابطة الجمركية الفلسطينية.

اعتمدت الدراسة المنهج الوصفي التحليلي، وتم جمع البيانات من خلال استبانة وُزعت على 146 ضابطاً وموظفاً في مختلف الإدارات. وتم تحليل البيانات باستخدام برنامج SPSS، مع توظيف أساليب إحصائية لتحديد العلاقة بين المعرفة المتاحة والمهارات التشغيلية والتطبيق العملي لإجراءات الأمن السيبراني.

تشير النتائج إلى وجود تحديات كبيرة، من بينها نقص التدريب المتخصص، وضعف الموارد التقنية، والفجوات في الوعي بالأطر القانونية المتعلقة بالأمن السيبراني. ومع ذلك، أظهرت النتائج مبادرات وجهوداً ملحوظة من قبل الضباط لتطبيق ممارسات الأمن السيبراني رغم هذه المعوقات.

وتقدّم هذه الدراسة توصيات قائمة على الأدلة تهدف إلى تعزيز برامج التدريب، وتحسين الموارد التقنية، ووضع سياسات واضحة تسهم في رفع كفاءة الأمن السيبراني لدى جهاز الشرطة الجمركية الفلسطينية.

Acknowledgements

In the name of Allah, Most Gracious, Most Merciful

All praise is due to Allah, who granted me the strength, patience, and clarity to complete this work. His mercy and guidance have been my greatest support throughout this academic journey.

I would like to extend my sincere gratitude to my supervisor, Waleed Awad for his continuous support, encouragement, and valuable insights. His mentorship played a crucial role in shaping the direction and depth of this research.

My heartfelt appreciation goes to the Palestinian Customs Police for their cooperation and assistance during the fieldwork. I also thank Al-Quds Open University for providing the resources and academic environment that allowed me to carry out this study.

I am deeply grateful to my family, especially my parents, for their endless love, prayers, and encouragement. Their unwavering belief in me gave me the strength to persevere.

Lastly, I would like to acknowledge my colleagues and friends who provided guidance, motivation, and support during every stage of this work.

May Allah reward you all.

Loai, Shalash

July 2025

Table of Contents

Examination Committee Page	iii
Declaration	iv
Abstract	v
الخلاصة	vi
Acknowledgements	vii
Table of Contents	viii
List of Figures	xi
List of Tables	xiii
List of Abbreviations	xiv
Chapter 1: Introduction	1
1.1 Overview and Background	1
1.2 Motivation	6
1.3 Problem Statement	6
1.4 Research Objectives	7
1.5 Research Questions	7
1.6 Thesis Contribution to the Field/ Significance and /or Impact of the Research	9
1.7 Thesis Outline	9
Chapter 2: Theoretical Concepts and Literature Review	11
2.1 Introduction	11
2.2 The Palestinian Customs Police – Roles, Challenges, and Institutional Vision	11
2.2.1 Firewall and Branch Centralized Management	17
2.2.2 Network Segmentation via VLANs (Juniper)	21
2.2.3 Centralized Authentication via Active Directory Domain Controller	26
2.2.4 Securing Wireless Access – Mist AP32	30
2.2.5 Endpoint Protection System – ESET XDR	35
2.2.6 Continuous Monitoring and Logging	39
2.2.7 Camera System Segmentation and Security	42

2.2.8	Updates and Security Awareness	46
2.3	Security framework: ISO/IEC 27001	50
2.3.1	Overview of ISO 27001 Standards	51
2.3.2	Key Terms in ISO 27001	52
2.3.3	Objectives of ISO/IEC 27001	52
2.3.4	Annex A Controls	53
2.3.5	Implementation Process	53
2.3.6	Importance of ISO/IEC 27001 in Information Security	53
2.3.7	Challenges of ISO/IEC 27001 Implementation	54
2.3.8	Alignment with Other Standards	55
2.3.9	Future Trends in ISO 27001	55
2.4	Cybersecurity knowledge and skills.....	56
2.5	Conclusion.....	65
Chapter 3:	Methodology	67
3.1	Introduction	67
3.2	Study Design	67
3.3	Population.....	67
3.4	Sampling.....	67
3.5	Instrument of study and validation indicators	67
3.6	Ethical approval.....	68
3.7	Tool Validity	69
3.7.1	Virtual Validity	69
3.7.2	Exploratory Data Analysis (Construct Validity).....	69
3.8	Reliability	71
3.9	Statistical analysis	71
3.10	Conclusion	72

Chapter 4: Results and Data Analysis.....	73
4.1 Introduction	73
4.2 Socio-Demographic Analysis.....	73
4.3 Descriptive Statistics:	74
Chapter 5: Conclusion and Recommendations	87
References	99
Appendix A: Survey	106

List of Figures

Figure 1: Internet Users in Palestine (% of population, 2005–2021). Adapted from GlobalEconomy.com (2021).....	3
Figure 2: Reported cybercrime cases in Palestine (2013–2018) Adapted from Safarini (2017); Palestinian News and Info Agency (2019); Abu Al Rab (2019).	4
Figure 3: PCP’s Network Topology Diagram Adapted from (Palestinian Customs Police, 2023).	15
Figure 4: Comprehensive Network Security Implementation Adapted from (Palestinian Customs Police, 2023).....	16
Figure 5: Active IPS threats and blocked CVEs Adapted from (Palestinian Customs Police, 2023).	18
Figure 6: web filter Adapted from (Palestinian Customs Police, 2023).....	19
Figure 7: Logging and Monitoring via FortiCloud Adapted from (Palestinian Customs Police, 2023).	20
Figure 8: Juniper VLAN network segmentation setup Adapted from (Palestinian Customs Police, 2023).....	23
Figure 9: Firewall rules between VLANs Adapted from (Palestinian Customs Police, 2023). .	24
Figure 10: LACP trunk configuration for switch uplinks Adapted from (Palestinian Customs Police, 2023).....	25
Figure 11: Malware types and distribution Adapted from (Palestinian Customs Police, 2023).	25
Figure 12: Domain Controller Environment Adapted from (Palestinian Customs Police, 2023).	27
Figure 13: Access Rights and Permission Management Adapted from (Palestinian Customs Police, 2023).....	28
Figure 14: Group Policy managment Adapted from (Palestinian Customs Police, 2023).	29
Figure 15: security properties Adapted from (Palestinian Customs Police, 2023).....	30
Figure 16: Mist AP32 configuration and usage Adapted from (Palestinian Customs Police, 2023).	31
Figure 17: Connected Wi-Fi clients and SSIDs Adapted from (Palestinian Customs Police, 2023).	32
Figure 18: Organizational Wi-Fi analytics overview Adapted from (Palestinian Customs Police, 2023).	33
Figure 19: WLAN authentication with RADIUS and 802.1X Adapted from (Palestinian Customs Police, 2023).....	34
Figure 20: SSID overview and bandwidth limits Adapted from (Palestinian Customs Police, 2023).	34
Figure 21: ESET dashboard: protection and vulnerabilities Adapted from (Palestinian Customs Police, 2023).....	36
Figure 22: Task automation for software and module updates Adapted from (Palestinian Customs Police, 2023).....	36
Figure 23: Detected threats and actions by ESET Adapted from (Palestinian Customs Police, 2023).	38
Figure 24: ESET XDR incidents and endpoint behavior Adapted from (Palestinian Customs Police, 2023).....	39

Figure 25: Live Fortinet session log with destinations Adapted from (Palestinian Customs Police, 2023).....	41
Figure 26: DHCP interface lease tracking Adapted from (Palestinian Customs Police, 2023).	41
Figure 27: NVRs per location with online status Adapted from (Palestinian Customs Police, 2023).	43
Figure 28: NVR system login via domain account Adapted from (Palestinian Customs Police, 2023).	44
Figure 29: Role-based access to camera systems Adapted from (Palestinian Customs Police, 2023).	45
Figure 30: Threat occurrence over time Adapted from (Palestinian Customs Police, 2023). .	47
Figure 31: Malware types and distribution Adapted from (Palestinian Customs Police, 2023).	49
Figure 32: Three Pillars of Cybersecurity Adapted from (Palestinian Customs Police, 2023).	59

List of Tables

Table 2-1: VLAN Names and Their Functions/Locations.....	22
Table 3-1: Pearson correlation coefficient between the items and the total score of the related to aspects.....	70
Table 3-2: Cronbach's Alpha values for the exploratory sample among employees distributed by aspects.....	71
Table 4-2: Descriptive statistics of the level of knowledge and skills that are being applied in Palestinian security institutions (a case study (PCP))	74
Table 4-3: Descriptive statistics of implementation and compliance with information security policies that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))	75
Table 4-4: Descriptive statistics of risk management and assessment in Palestinian security institutions (a case study Palestinian Customs Police (PCP))	77
Table 4-5: Descriptive statistics of risk management and incident response in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).....	78
Table 4-6: Descriptive statistics of roles and responsibilities that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))	80
Table 4-7: Descriptive statistics of employee competence in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).....	81
Table 4-8: Descriptive statistics of confidentiality and information protection in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).....	82
Table 4-9: Descriptive statistics of asset and inventory management (equipment) that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).....	83
Table 4-10: Descriptive statistics of information access that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).....	85
Table 4-11: Descriptive statistics of physical access controls that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))	86

List of Abbreviations

MOI	Ministry of Interior
CP	Customs Police
PSI	Palestinian Security Institution
PCP	Palestinian Customs Police

Chapter 1: Introduction

1.1 Overview and Background

In the digital age, cybersecurity has become a critical concern for governments, businesses, and security institutions worldwide. The rapid expansion of Information and Communication Technologies (ICT) has led to increased cyber threats, data breaches, and security vulnerabilities (Otieno, 2020). Developing countries, including Palestine, face unique cybersecurity challenges due to limited resources, weak regulatory frameworks, and a shortage of skilled professionals (Adhikari, 2017). These challenges highlight the urgent need for enhanced knowledge and skill development in cybersecurity, particularly within law enforcement agencies such as the Customs Police.

The Palestinian Security Institution (PSI), established under the 1993 Oslo Accords, serves as the primary governmental body responsible for maintaining internal security, combating crime, and preserving public order within the Palestinian territories. Within this framework, the Palestinian Customs Police plays a vital role in border security, trade regulation, and preventing smuggling and cyber-enabled financial crimes. However, as both entities increasingly rely on digital systems, databases, and surveillance technologies, they face growing cybersecurity threats.

Cybercriminals exploit network vulnerabilities, outdated security protocols, and insufficient cybersecurity awareness among personnel, posing serious risks to national security and economic stability (Kshetri, 2010). Given the PSI's responsibility for overall security and the Customs Police's critical role in economic and border protection, enhancing cybersecurity infrastructure, training, and regulatory enforcement is essential to safeguard Palestinian digital assets, financial transactions, and sensitive security data. Addressing these cybersecurity gaps is not only a technical necessity but also a strategic imperative for ensuring the PSI's effectiveness in a digitally evolving security landscape.

Technological advancements have become indispensable in enhancing the performance of security organizations worldwide. In the Palestinian context, technology offers a powerful tool for improving the efficiency and effectiveness of the PSI, particularly the Customs Police. By leveraging technology for enhanced monitoring, analysis, and rapid response, the PSI can better achieve its security goals.

However, the increasing reliance on technology exposes the PSI to cyber threats. The International Telecommunication Union (ITU) defines cybersecurity as the collection of tools, policies, and practices used to protect the cyber environment and organizational assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. (ITU, 2018).

As cyber threats evolve, developing countries like Palestine are investing in cybersecurity measures and building in-house expertise to address application security, intelligence, analytics, and data protection. The Palestinian security institution, like the rest of the institutions of the Palestinian state, is not immune to cyber-attacks. The incident that occurred in the Palestinian Ministry of Health which led to the loss of the data of all patients and members of the National Health Insurance is a case in point.

The escalating prevalence of cybercrime globally underscores the importance of cybersecurity for economic and national security. With the rapid growth of cyberspace and increasing connectivity, the potential for cyberattacks has expanded significantly. This is particularly relevant in Palestine, where internet usage has surged, leading to a rise in cybercrime cases.

The use of the Internet has increased significantly in Palestine from 9.2% in 2004 to 80% in 2019 (PCBS 2013, PCBS 2020). As a result, the number of cases related to cybercrimes increased dramatically from 174 in 2013 to 2568 in 2018, according to the Anti-Cyber Crime Unit of the Palestinian Police (Safarini 2017, Palestinian News and Info Agency 2019, Abu Al-Rab 2019).

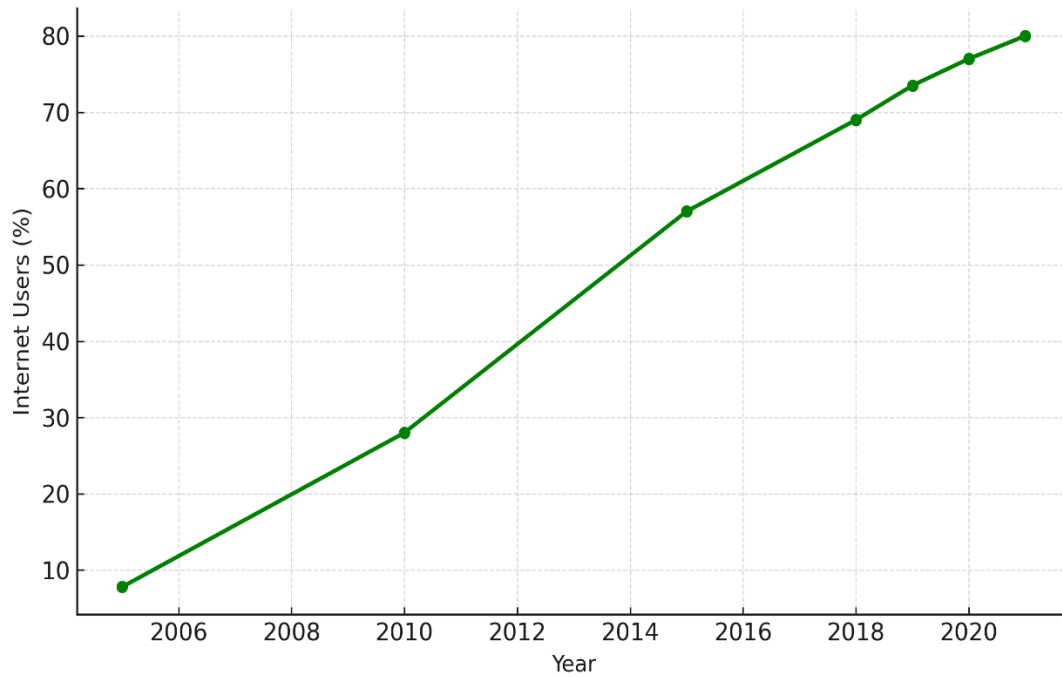


Figure 1: Internet Users in Palestine (% of population, 2005–2021). Adapted from GlobalEconomy.com (2021).

As a result of the above-mentioned, the percentage of cybercrimes perpetration in Palestine has increased significantly, according to statistics issued by the General Investigation Department (Safarini 2017, Palestinian News and Info Agency 2019, Abu Al-Rab 2019). The chart below illustrated the increase in the number of cybercrimes perpetration in the years (2013-2018):

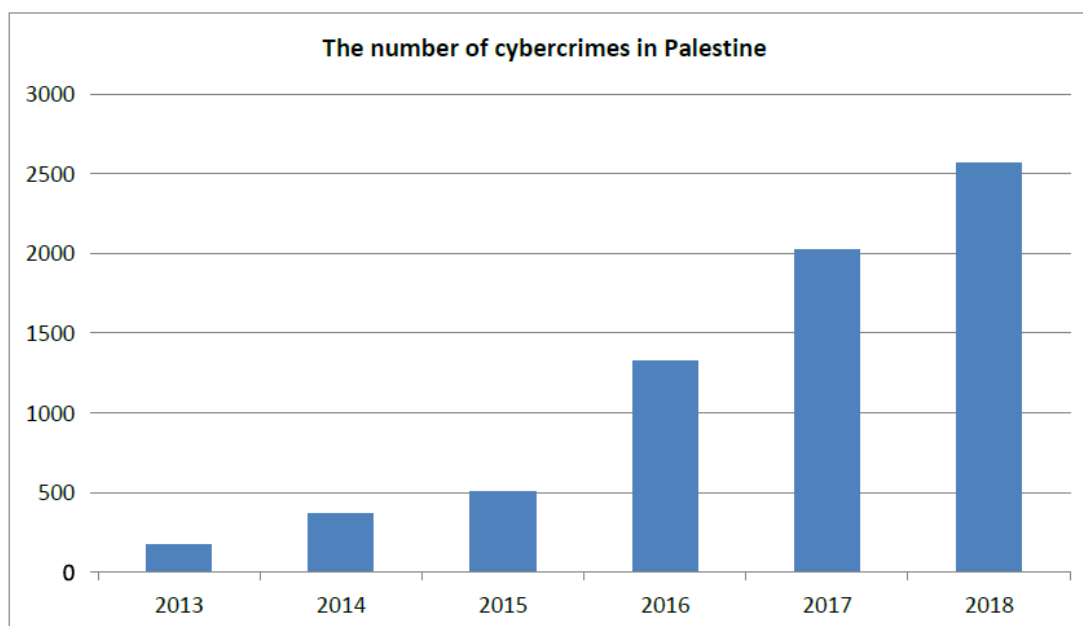


Figure 2: Reported cybercrime cases in Palestine (2013–2018) Adapted from Safarini (2017); Palestinian News and Info Agency (2019); Abu Al Rab (2019).

Despite efforts by the Anti-Cyber Crime Unit of the Palestinian Police to raise awareness and combat cybercrime, challenges remain. Many cybercrimes go unreported, highlighting the need for further research and intervention. According to police records, there were 1327 cases reported in the year 2016, and about 450 cases until mid of April 2017. (2017، الإعلام، صدی) Most of these cases are related to females using their social network profiles. Statistics report that 80% of cybercrimes in Palestine are not transferred to the Police, and victims prefer to keep silent, which clearly indicates the importance of raising awareness and implementing proper security measures.

Cybercrime is defined as: “Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)” (Halder & Jaishankar, 2012).

According to the National Institute of Standards and Technology (NIST), cybersecurity compliance refers to adhering to applicable cybersecurity standards, laws, or regulations through implementing controls that mitigate risks. These controls are designed to ensure the confidentiality, integrity, and availability (CIA) of information (NIST, 2023).

Amro (2018) explores the growing threat of cybercrime in Palestine, emphasizing its impact on individuals and the institutional challenges in combating such threats. The study highlights that the most common cybercrimes reported include identity theft, hacking, malware, financial fraud, and defamation largely facilitated through social media platforms. Despite the establishment of a cybercrime unit and the adoption of a cybercrime law, the study finds that a significant number of victims remain silent due to fear of scandal or mistrust in authorities. The study further critiques the Palestinian school curriculum for lacking comprehensive content on cybersecurity and ethics, which leaves young people ill-prepared to navigate online threats. A survey of 300 participants revealed that while awareness of cybercrime is relatively high, victims often resort to informal help from friends rather than reporting to officials. The study concludes with several recommendations, including updating educational curricula, strengthening cyber laws, and enhancing public trust in official cybercrime units.

Most cybersecurity and data protection laws focus on sensitive data. This includes personally identifiable information (PII), financial information, and protected health data. Other sensitive information includes race, religion, IP addresses, email addresses, and biometric data like facial recognition.

Cybersecurity compliance encompasses various measures designed to protect digital infrastructure and sensitive information from unauthorized access and cyber threats. Among these measures, encryption ensures data confidentiality by converting information into a secure format, while network firewalls act as a protective barrier between internal and external networks, preventing unauthorized access. Additionally, password policies enforce strong authentication practices to safeguard accounts and systems. Beyond technical measures, cyber insurance provides financial protection against cyber incidents, and employee training plays a crucial role in raising cybersecurity awareness and reducing human error. Furthermore, incident response plans establish structured protocols for detecting, mitigating, and recovering from cyber threats, ensuring organizations can respond effectively to security breaches. (Otieno, 2020).

This research aims to bridge the cybersecurity gap within the Palestinian Security Institution (PSI), particularly focusing on the Customs Police and their reliance on digital technologies in security operations. By assessing the knowledge and skills applied in cybersecurity practices, this study seeks to identify existing strengths and uncover critical vulnerabilities. Understanding these gaps will provide actionable insights for improving cybersecurity

readiness, enhancing digital resilience, and ensuring that PSI personnel are well-equipped to mitigate evolving cyber threats in an increasingly digitized security environment.

1.2 Motivation

The rapid digital transformation in security institutions has brought significant opportunities and challenges, particularly in cybersecurity. The Palestinian Security Institution (PSI), including the Customs Police, is increasingly relying on digital systems, surveillance technologies, and data-driven operations to enhance security and combat financial crimes. However, cyber threats, unauthorized access, and network vulnerabilities pose serious risks to national security, economic stability, and operational effectiveness. This research is motivated by the urgent need to assess and improve cybersecurity knowledge and skills within PSI to ensure robust digital protection against evolving cyber threats.

By addressing this gap, the research aims to provide valuable insights into existing cybersecurity practices, identify areas for improvement, and propose strategies to strengthen digital security frameworks within the PSI. The findings of this study will contribute to developing targeted training programs, strengthening cybersecurity policies, and fostering a proactive security culture within PSI. Ultimately, supporting national security efforts in an increasingly digital landscape.

1.3 Problem Statement

The Palestinian Customs Police play a pivotal role in ensuring economic security and combating threats like smuggling and cyber-enabled crimes. However, limited research has explored the specific knowledge and skills such as legal expertise, operational tactics, and cybersecurity proficiency that enable their effectiveness.

This gap, compounded by Palestine's constrained political and economic environment, hinders efforts to optimize training and performance. This study addresses this deficiency by evaluating the competencies applied within the Customs Police and proposing strategies to enhance their operational capacity. To address this deficiency, the present study systematically evaluates the knowledge and skills encompassing operational, legal, interpersonal, and technological (including cybersecurity) competencies applied within the PCP. It further proposes practical strategies to enhance these competencies and build a more capable, future-ready force.

1.4 Research Objectives

The primary goal of this research is to explore and analyse the knowledge and skills currently being applied in Palestinian security institutions, with a specific focus on the Customs Police. This goal is driven by the need to understand how effectively these skills and knowledge are utilized to enhance the efficiency and effectiveness of the Customs Police.

To achieve this goal, the study will pursue the following specific objectives:

Objective 1: To identify the key knowledge areas and skills required for effective performance within the Customs Police.

Objective 2: To evaluate the current level of knowledge and skills among Customs Police officers by assessing their strengths and identifying areas for improvement.

Objective 3: Provide recommendations for enhancing knowledge and skill development in the Customs Police.

This research builds on existing studies of security training and skills application by focusing specifically on the Palestinian Customs Police, an area that has received limited attention. It diverges from previous research by incorporating a detailed case study approach, providing in-depth insights into the specific challenges and opportunities within this institution. A quantitative survey will be used to provide a comprehensive understanding of the knowledge and skills applied in the Customs Police.

1.5 Research Questions

In light of the background, problem statement, and research objectives, this study seeks to investigate the application of knowledge and skills within Palestinian security institutions, with a particular focus on the Palestinian Customs Police (PCP). Understanding how knowledge and skills are utilized in this critical institution is essential to identify strengths, gaps, and opportunities for development in the areas of security governance and information protection.

The main research question:

What is the level of knowledge and skills that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To explore this question in depth, the following **sub-questions** have been formulated:

Question #1: What is the level of implementation and compliance with information security policies that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

Question #2: What is the level of risk management and assessment in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

Question #3: What is the level of risk management and incident response الاستجابة للحوادث in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

Question #4: What is the level of roles and responsibilities that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

Question #5: What is the level of employee competence in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

Question #6: What is the level of confidentiality and information protection in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

Question #7: What is the level of asset and inventory management (equipment) that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

Question #8: What is the level of information access that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

Question #9: What is the level of physical access controls that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

1.6 Thesis Contribution to the Field/ Significance and /or Impact of the Research

This thesis aims to make a substantial contribution to the field of cybersecurity by providing a comprehensive analysis of the knowledge and skills applied in the Palestinian Customs Police. The significance and impact of this research extend beyond academic contributions, offering practical recommendations for policy and training improvements that can enhance the cybersecurity operational effectiveness of security institutions. By addressing the specific context of the Palestinian Customs Police, this study also contributes to a deeper understanding of cybersecurity dynamics in the PSI.

1.7 Thesis Outline

The study consists of five main chapters to comprehensively investigate Cybersecurity Knowledge and Skills within Palestinian security institutions, with a focus on the Palestinian Customs Police (PCP). The outline of the chapters is as follows:

Chapter One: Introduction

This chapter provides the general background of the study, the research problem, objectives, significance, and scope. It also presents the main and sub-research questions and concludes with this thesis outline.

Chapter Two: Literature Review

This chapter reviews relevant theoretical and empirical literature related to cybersecurity, institutional knowledge and skills, risk management, and information security in public institutions. It also highlights existing gaps and how this study contributes to the body of knowledge.

Chapter Three: Methodology

This chapter explains the research design, data collection methods, sampling techniques, and tools used for analysis. It also discusses the validity, reliability, and ethical considerations of the study.

Chapter Four: Results and Data Analysis

This chapter presents the findings of the research based on the collected data. The results are analyzed and discussed in relation to the research questions and the reviewed literature.

Chapter Five: Conclusion and Recommendations

This chapter summarizes the main findings, answers the research questions, discusses the implications of the results, and provides practical recommendations for improving knowledge and skills development in the Palestinian Customs Police. It also proposes ideas or suggestions for future research.

Chapter 2: Theoretical Concepts and Literature Review

2.1 Introduction

The role of security knowledge and skills in law enforcement agencies is pivotal for maintaining public safety and order. This literature review aims to synthesize existing research on the application of security knowledge and skills within the context of Palestinian security institutions, with a particular focus on the Customs Police. Understanding these elements is crucial for evaluating the effectiveness, challenges, and areas for improvement within these institutions.

The security sector in Palestine, like many other regions, plays a crucial role in maintaining stability and enforcing the law. The Customs Police, a specialized unit within the Palestinian security apparatus, is responsible for combating smuggling and enforcing customs regulations. Sayigh (2007) notes that the Customs Police play a vital role in safeguarding the Palestinian economy by preventing the influx of illegal goods and enforcing tax regulations.

The formation of the Palestinian Customs Police can be traced back to the Oslo Accords in the early 1990s, which laid the groundwork for the establishment of formal security institutions in the Palestinian territories. According to Tartir (2015), these institutions were developed with the assistance of international donors to build the necessary infrastructure for effective governance and law enforcement.

2.2 The Palestinian Customs Police – Roles, Challenges, and Institutional Vision

The Palestinian Customs Police (PCP) plays a vital and multifaceted role in safeguarding the national economy and ensuring public safety. As detailed in the strategic document outlining the goals of various central departments (2023–2028), that emphasizes multi-dimensional development, aligning internal operations with national economic protection, legal regulation, digital modernization, and community engagement.

▪ Economic Protection and Anti-Smuggling Measures

The core objective of the Operations and Field Inspection Department is to protect the national economy by combating tax evasion and smuggling, particularly at key border points and internal commercial zones. This includes expanding customs coverage, securing all seized

evidence, and reducing smuggling-related risks by establishing sub-checkpoints and secure storage units for confiscated materials.

- **Legal and Institutional Reform**

The Legal Affairs Department focuses on improving legal awareness among employees and ensuring procedural integrity. This includes the development of standardized legal processes, human rights compliance, and coordination with the judiciary for proper handling of legal cases. The aim is to improve the overall legal structure governing the PCP's operations.

- **Administrative Oversight and Security**

The Department of Security and Oversight plays a key role in internal auditing, risk prevention, and ensuring administrative and financial discipline. It monitors staff compliance, handles emergencies, and provides security recommendations to leadership, thus maintaining organizational integrity and safeguarding against internal and external threats.

- **Digital Transformation and Information Management**

The Information Systems and Communications Department is responsible for automating administrative procedures, building secure digital infrastructure, and protecting data from tampering or loss. It also works to ensure fast communication between departments and enhance information accessibility.

- **Community Engagement and Public Awareness**

The Public Relations and Media Department aims to raise public awareness about the Customs Police's role through media campaigns and outreach events. It also seeks to increase community trust, encourage voluntary cooperation, and foster transparency between the institution and the public.

- **Financial and Human Resource Development**

The Administrative and Financial Affairs Department works on structuring financial operations, ensuring budgetary discipline, and maintaining accurate employee and logistics records. It also facilitates coordination with related ministries and manages contractual operations such as rentals and procurements.

▪ **Gender Mainstreaming and Equality**

The Gender Department is committed to promoting women's participation in leadership and operational roles within the PCP. It advocates for equal training opportunities, gender-sensitive services, and public facilities that are inclusive of all societal groups.

▪ **International Relations and Cooperation**

The International Relations Department focuses on building partnerships with embassies, consulates, and international organizations. It facilitates joint training, knowledge exchange, and representation in regional and international events, thereby strengthening the PCP's global network and diplomatic engagement.

To support its evolving mission and strategic vision, the Palestinian Customs Police (PCP) has invested in establishing a robust digital infrastructure that aligns with its operational, administrative, and security goals. The official technical report detailing the PCP's network structure, cybersecurity tools, and surveillance systems reflects a clear commitment to digital transformation, information security, and centralized control as outlined in the institution's strategic goals (2023–2028) as following:

▪ **Centralized Network Architecture and Digital Control**

The PCP's headquarters functions as the core hub, hosting the central data center. Through a combination of VPN and Internet connectivity, secured by dual firewalls and managed by core switches, the network enables secure, hierarchical communication between departments. Floor switches distribute access to internal systems including servers, workstations, VoIP devices, printers, and managed wireless access points. The centralized management of these access points through a unified portal ensures consistency, visibility, and remote control—features critical for operational efficiency across the entire institution.

▪ **Branch Connectivity and Secure Isolation**

Across 16 regional branches, the PCP maintains a replicated network structure that mirrors the headquarters' architecture. Each branch operates with dedicated firewalls and switches, connecting staff and systems securely while ensuring physical and logical segmentation. Notably, access points in branches are restricted to Internet-only use, fully isolated from

internal networks, which significantly reduces risk exposure and potential lateral attacks. This approach directly supports the PCP's cybersecurity objective of protecting critical resources from unauthorized access and external threats.

- **Cybersecurity and Network Governance**

The PCP employs a comprehensive cybersecurity management system that aligns with global standards. Firewall activities are monitored through a cloud-based portal, providing real-time visibility into performance and security incidents. All computing devices are protected using endpoint security software (XRP), offering proactive detection and response to threats. Furthermore, the deployment of Virtual Local Area Networks (VLANs) ensures departmental segmentation preventing data leakage and enforcing strict access control policies. These measures are consistent with the institution's goals of risk prevention, oversight, and administrative accountability.

- **User Access and Centralized Authentication**

All employees access internal resources via a domain-based authentication system, where permissions are role-specific. This centralized structure not only facilitates effective access control but also supports secure file sharing and compliance with internal policies. It also reflects the PCP's intent to standardize and automate workflows, as referenced in the strategic goal of improving administrative and financial transparency.

- **Surveillance and Security Integration**

The PCP has implemented a centralized video surveillance system covering both headquarters and branches. Surveillance data is collected and managed through a central Network Video Recorder (NVR) within a separate VLAN, ensuring that video infrastructure remains isolated from sensitive operational systems. This design underscores the institution's approach to layered security and physical monitoring, as described in its operational security goals.

- **Awareness and Continuous Security Improvement**

The network strategy also incorporates cybersecurity awareness initiatives through regular training and bulletins on phishing prevention, safe browsing, and password management. Simultaneously, the IT team maintains rigorous system updates, applying patches to operating

systems, servers, and monitoring tools demonstrating the PCP’s commitment to ongoing improvement and resilience.

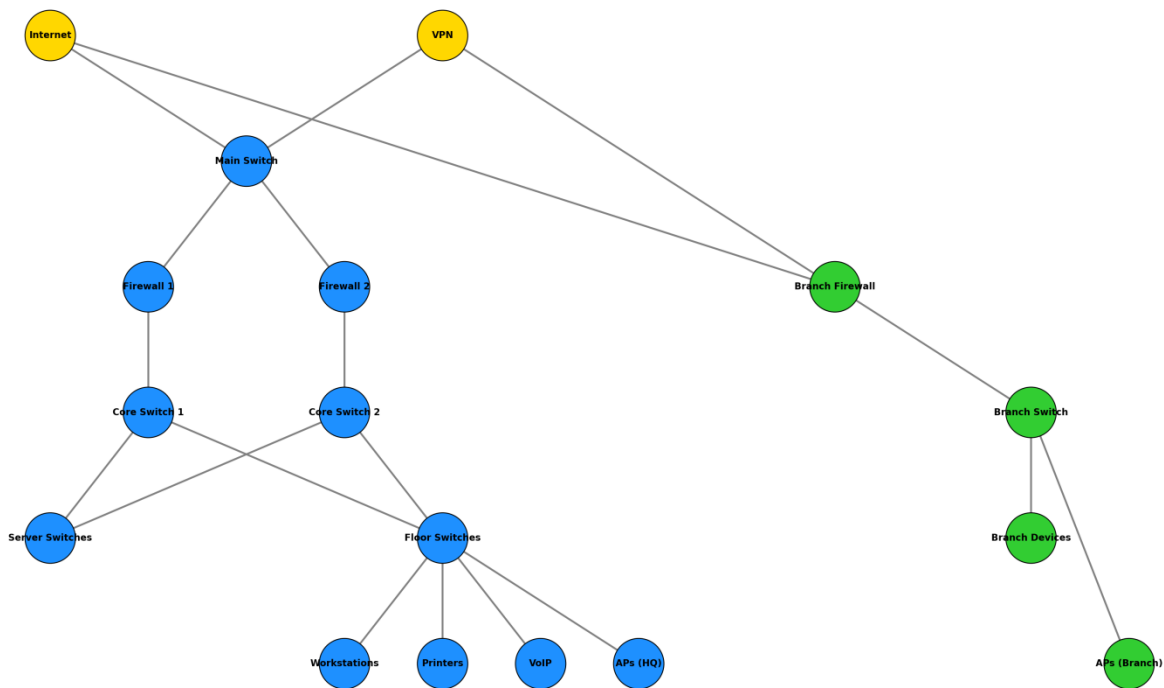


Figure 3: PCP’s Network Topology Diagram Adapted from (Palestinian Customs Police, 2023).

To achieve its mission effectively and address contemporary threats, the Palestinian Customs Police has significantly invested in strengthening its digital infrastructure and cybersecurity capabilities. These advancements are not only aligned with the institution's operational and strategic priorities but also reflect global best practices in network protection, endpoint defense, access control, and real-time threat monitoring. The following outlines the detailed implementation of these cybersecurity measures ranging from firewall configurations and VLAN segmentation to centralized authentication, wireless network isolation, and endpoint protection systems. Together, these components form a cohesive and resilient security architecture designed to safeguard sensitive information, support operational continuity, and reinforce the PCP’s institutional resilience in the face of evolving cyber threats.

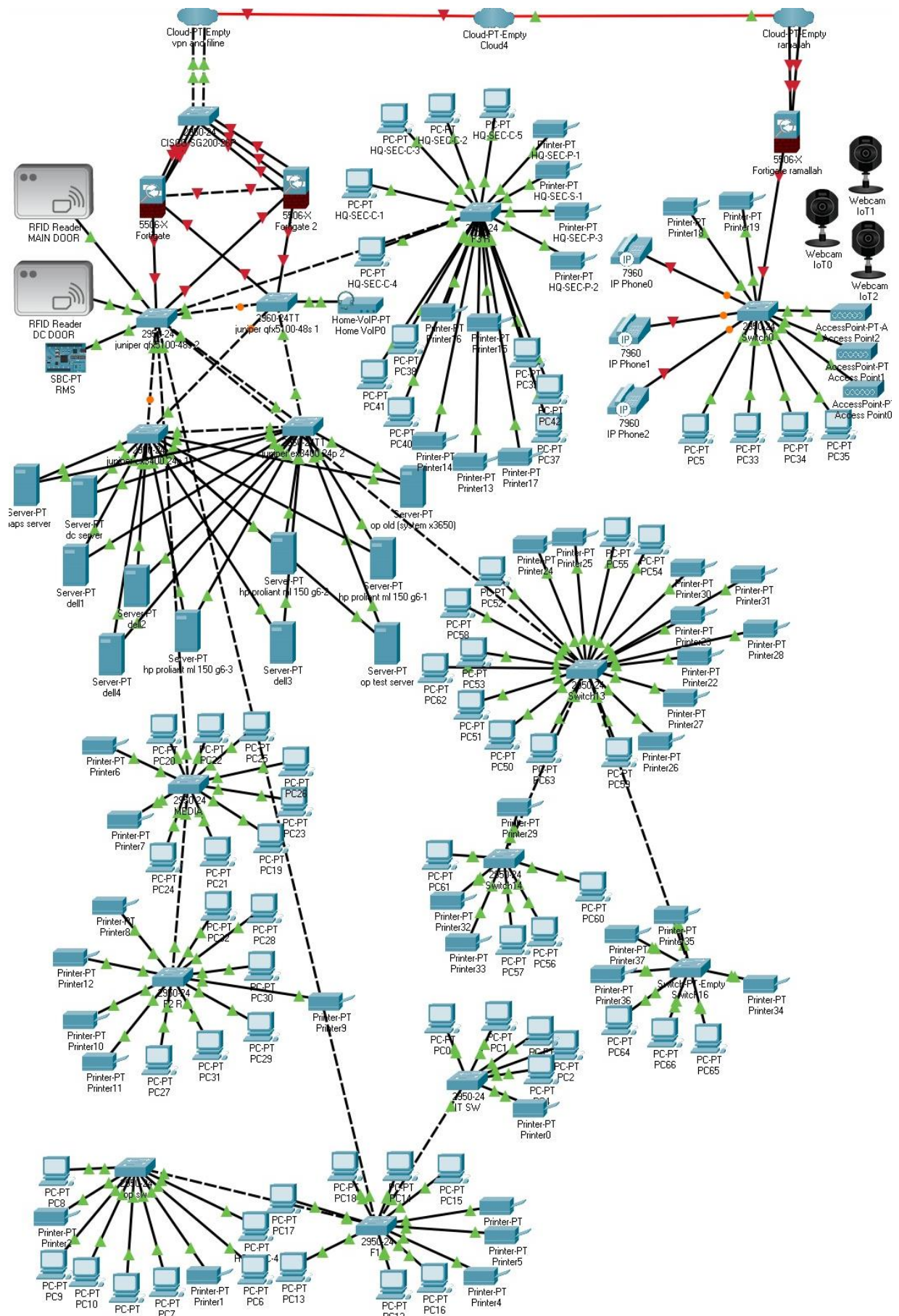


Figure 4: Comprehensive Network Security Implementation Adapted from (Palestinian Customs Police, 2023).

2.2.1 Firewall and Branch Centralized Management

In any security focused digital infrastructure, protecting network entry points is a fundamental requirement. For the Palestinian Customs Police (PCP), this challenge is addressed through the deployment of a comprehensive firewall solution built around Fortinet's FortiGate systems. These devices offer advanced features such as intelligent packet filtering, encrypted traffic inspection, integrated threat intelligence, and centralized cloud-based management through Forti Cloud. Their implementation marks a critical step toward securing all traffic entering and exiting the organization's internal network while maintaining centralized visibility and control across multiple sites.

2.2.1.1 Securing Network Entry Points (FortiGate)

Overview and Architecture

Recognizing that network entry points are highly vulnerable to cyber threats; the PCP has strategically implemented FortiGate firewalls to provide robust perimeter protection. At the central headquarters, two FortiGate devices operate in a High Availability (HA) configuration to ensure failover protection and continuous service availability. These devices regulate both Internet and VPN connectivity through strict access policies that permit only trusted traffic. Moreover, Secure Sockets Layer (SSL) inspection is enabled to decrypt and analyze HTTPS communications effectively identifying hidden threats within encrypted data streams.

To further strengthen protection, the Intrusion Prevention System (IPS) is activated in Prevention Mode, leveraging frequently updated signature databases to proactively detect and block a wide array of known vulnerabilities and exploit attempts (CVEs). This layered defense model enables real-time threat identification and mitigation before malicious payloads can reach internal resources.

Branch-Level Deployment

Each regional branch is equipped with its own FortiGate firewall, all of which are centrally managed via Forti Cloud. A secure IPSec VPN tunnel links every branch to the headquarters, ensuring encrypted communication and the seamless extension of uniform security policies across the entire organization. This centralized model enhances consistency, facilitates rapid policy enforcement, and simplifies administrative overhead.

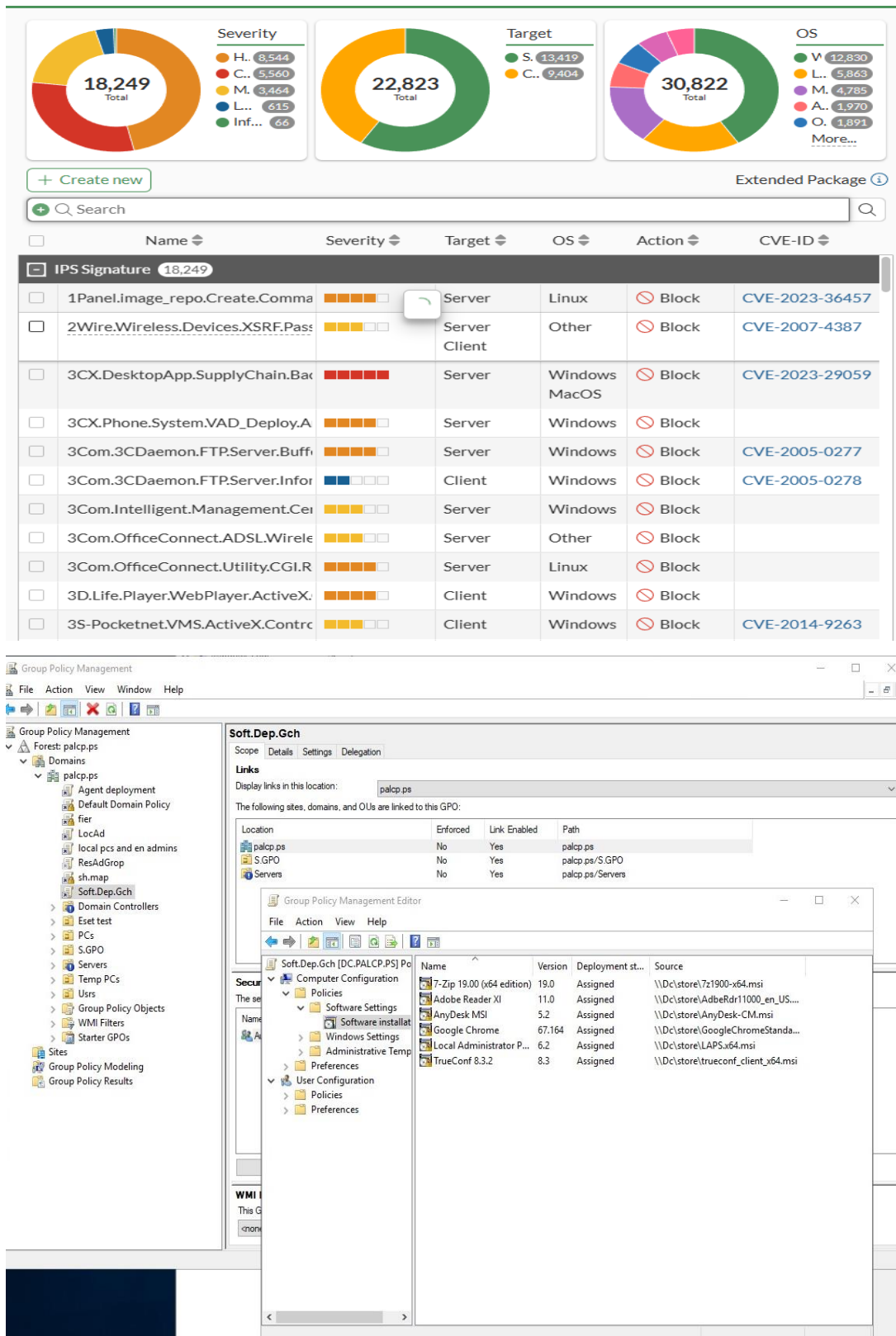


Figure 5: Active IPS threats and blocked CVEs Adapted from (Palestinian Customs Police, 2023).

Tools and Techniques Enabled

The firewall system is complemented by a suite of advanced security tools integrated within FortiOS, including:

- **Web Filtering:** Restricts access to categories of websites (e.g., social media, news) and blocks known malicious domains, reducing the risk of phishing and malware infections.

Edit Web Filter Profile

Name

wifi-default

Comments

Default configuration for offloading WiFi traffic.50/255

Feature set

Flow-based

Proxy-based

☒ FortiGuard Category Based Filter

✓ Allow

👁 Monitor

🚫 Block

⚠ Warning

👤 Authenticate

Name	Action
<div><div>+</div>Potentially Liable 12</div>	
<div><div>-</div>Adult/Mature Content 15</div>	
Alternative Beliefs	<div>🚫 Block</div>
Abortion	<div>🚫 Block</div>
Other Adult Materials	<div>🚫 Block</div>
Advocacy Organizations	<div>🚫 Block</div>
Gambling	<div>🚫 Block</div>
Nudity and Risque	<div>🚫 Block</div>
Pornography	<div>🚫 Block</div>
Religion	<div>🚫 Block</div>

9% 95

☐ Allow users to override blocked categories

🔍 Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ☐

🔍 Static URL Filter

Block invalid URLs☒

URL Filter☐

Block malicious URLs discovered by FortiSandbox☐

Content Filter☐

🔍 Rating Options

Behavior when FortiGuard is unreachable ⓘ

Allow all websites

Block all websites

Rate URLs by domain and IP Address☐

🔍 Proxy Options

HTTP POST Action

Allow

Block

Remove Cookies☐

Figure 6: web filter Adapted from (Palestinian Customs Police, 2023).

- **Intrusion Prevention System (IPS):** Offers proactive defense against Zero-Day attacks, port scans, and SQL injection attempts.

19

- **Application Control:** Prevents unauthorized applications such as file-sharing tools and proxy servers from operating within the network.
- **Forti View:** A visual analytics dashboard that provides real time traffic insights, segmented by source, destination, application, and risk category.

Logging and Monitoring via Forti Cloud:

All network events and security alerts are logged and monitored through Forti Cloud, ensuring that suspicious activities are promptly flagged and investigated.

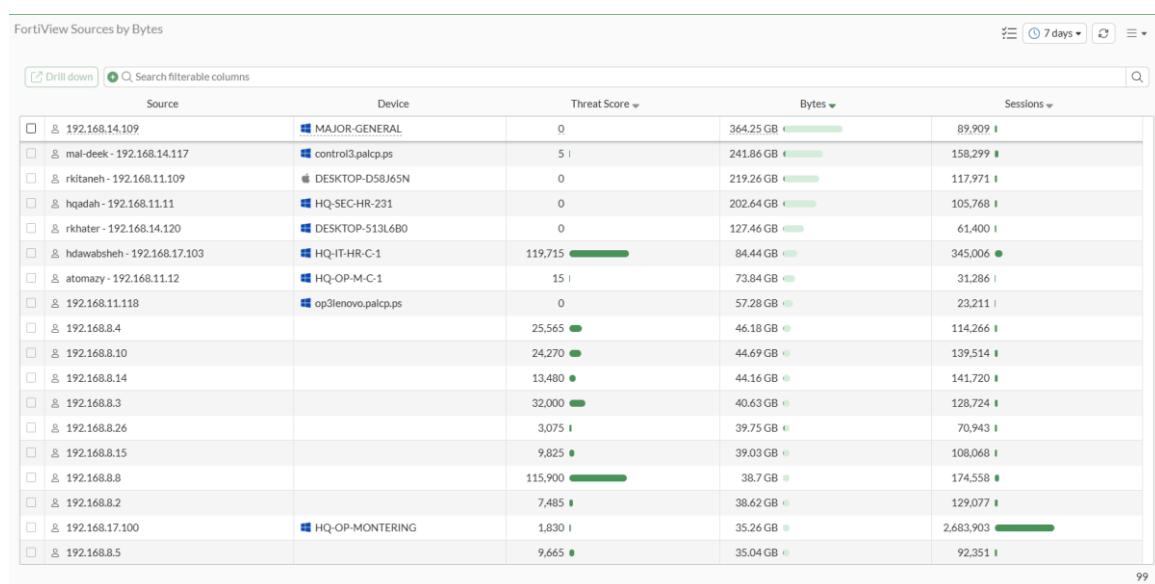


Figure 7: Logging and Monitoring via FortiCloud Adapted from (Palestinian Customs Police, 2023).

Sample Security Policies Implemented

To enforce secure communication practices, the following example policies are in place:

- Blocking the download of executable files (.exe) from the Internet except from trusted domains.
- Restricting VPN connections to predefined IP addresses.
- Disabling vulnerable or unnecessary protocols, such as Telnet and SMB, for external traffic.

Security Benefits

The FortiGate based infrastructure provides the Palestinian Customs Police with several strategic advantages:

- Centralized control through Forti Cloud enables efficient policy enforcement and streamlined threat monitoring across all branches.
- Real time intrusion detection and prevention at the perimeter level, reducing response time to incidents.
- Enhanced security posture against advanced cyber threats without reliance on third party appliances.

2.2.2 Network Segmentation via VLANs (Juniper)

Effective network segmentation is a cornerstone of enterprise level cybersecurity, particularly in organizations with diverse departmental needs and sensitive data flows. To meet these demands, the Palestinian Customs Police (PCP) has implemented a well-structured Virtual Local Area Network (VLAN) architecture, using Juniper switches managed centrally through a unified portal. This architecture not only ensures logical separation of network domains but also enhances operational efficiency, security, and administrative control.

Security Objectives

The VLAN implementation is guided by three primary security and performance objectives:

- Isolating departments and device categories to reduce lateral movement and limit the spread of threats within the internal network.
- Minimizing broadcast domains to optimize bandwidth usage and overall network performance.
- Enabling tailored access control policies per department based on the nature of their operations and data sensitivity.

Approved VLAN Structure

The VLAN framework is organized by physical floors and functional departments:

Table 2-1: VLAN Names and Their Functions/Locations

VLAN Name	Function/Location
First floor	Devices on the first floor
Second floor	Devices on the second floor
Third floor	Devices on the third floor
Fourth floor	Devices on the fourth floor
IT	Information Technology Department
Manage	Senior Management
Cam	Surveillance Camera System
WIFI	Wi-Fi Network (Guests and Staff)
Srv	Network Servers

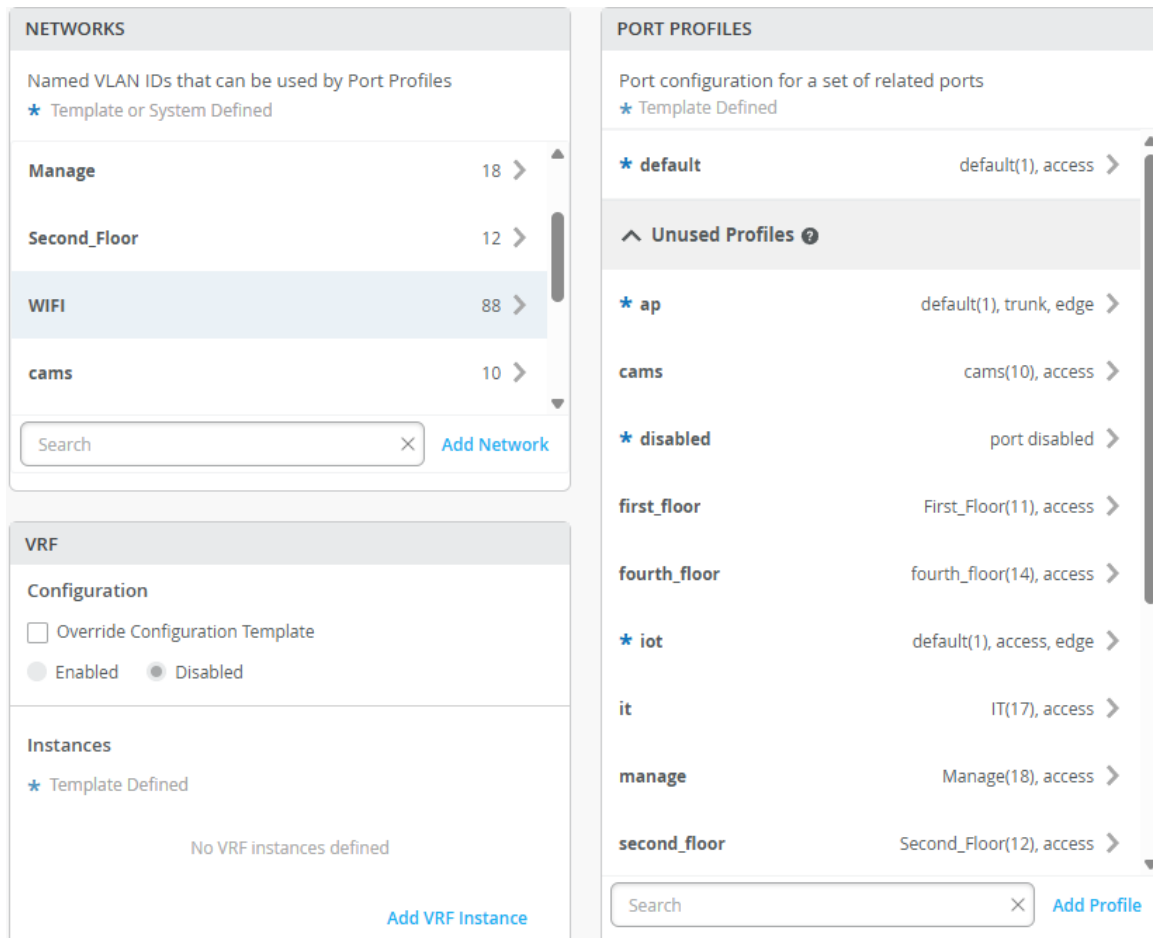


Figure 8: Juniper VLAN network segmentation setup Adapted from (Palestinian Customs Police, 2023).

Configuration and Centralized Management

Using the Juniper central portal, VLANs are configured and monitored from a single interface. Each switch port is assigned to a specific VLAN according to its physical location and function. Trunk ports linking switches to each other and to the FortiGate firewall are configured using the 802.1Q protocol to carry multiple VLANs efficiently. This setup enables administrators to manage the entire switching infrastructure remotely, reducing configuration errors and increasing response speed for adjustments or troubleshooting.

Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type
1floor-test-camsram (49)	1st floor	Remote-Branch	1st floor address	ramallah	always	ALL	✓ ACCEPT		Di...	Standar
HQ MOF (33)	1st floor 2nd floor	MOF (port3)	1st floor address 2nd floor address	mof_subnet	always	ALL	✓ ACCEPT		NAT	Standar
mof (29)	SSL-VPN tunnel interface (ssl.root)	MOF (port3)	borders SSLVPN_TUNNEL_ADDR1	mof_subnet	always	ALL	✓ ACCEPT		NAT	Standar
Mathlonuser-Floor1 (53)	SSL-VPN tunnel interface (ssl.root)	1st floor SERVERS MOF (port3)	Branch SSLVPN_TUNNEL_ADDR1 SERVERS address	1st floor address MOF-subnet SERVERS address	always	ALL	✓ ACCEPT		NAT	Standar
Branches TO DMZ (32)	Remote-Branches (port2)	Remote-Branch	all	NVR	always	ALL	✓ ACCEPT		Di...	Standar
floor to Branches (25)	1st floor 2nd floor	Remote-Branch	all	NVR	always	ALL	✓ ACCEPT		Di...	Standar
FLOOR TO DMZ (31)	1st floor 2nd floor	DMZ-MAP	all	all	always	ALL	✓ ACCEPT		Di...	Standar
1st to cam (26)	1st floor 2nd floor	Cams	all	all	always	ALL	✓ ACCEPT		Di...	Standar
VLANs to CAM DEVICE (24)	1st floor 2nd floor	IT	all	CAM DEVICE	always	ALL	✓ ACCEPT		Di...	Standar
From-Outside-To-server (23)	PALTEL-INTERNET-WAN (port1)	DMZ-MAP	all	server-443-tcp server-5443-tcp	always	Port:	✓ ACCEPT		Di...	Standar

Security Rating Insights (19)

Figure 9: Firewall rules between VLANs Adapted from (Palestinian Customs Police, 2023).

Firewall Integration and VLAN Policy Enforcement

To enforce inter-VLAN security policies, each VLAN is mapped as a sub interface on FortiGate, with a corresponding VLAN ID. FortiGate acts as the central control point for traffic flowing between VLANs, applying granular security rules as needed. For instance, traffic from the Wi-Fi VLAN may be entirely blocked from accessing the server VLAN, while the IT VLAN may have limited access based on specific roles or systems. These rules ensure that sensitive resources remain protected and that access is always purposeful and monitored.

Advanced Features and Enhancements

Additional configurations further enhance the system's performance and resilience:

- Link Aggregation Control Protocol (LACP) is enabled for uplink trunk ports, boosting bandwidth and fault tolerance between core network devices.
- VLAN ID overviews and logical mapping are maintained for transparency and simplified troubleshooting.

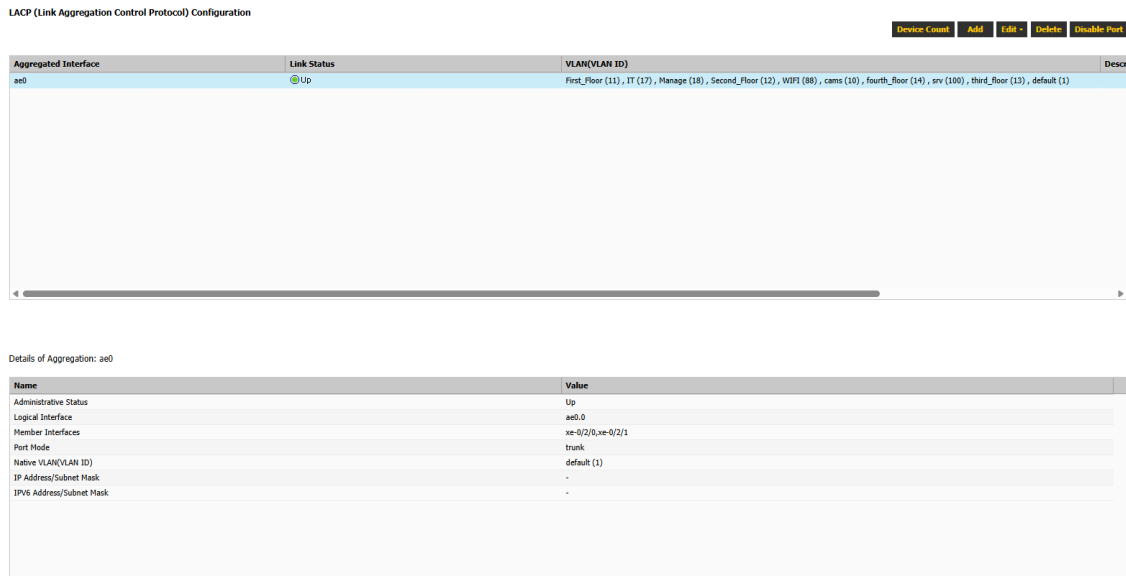


Figure 10: LACP trunk configuration for switch uplinks Adapted from (Palestinian Customs Police, 2023).

VLAN Name	VLAN ID/List	Description
First_Floor	11	None
IT	17	None
Manage	18	None
Second_Floor	12	None
WIFI	88	None
cams	10	None
default	1	None
fourth_floor	14	None
srv	100	None
third_floor	13	None

Figure 11: Malware types and distribution Adapted from (Palestinian Customs Police, 2023).

Achieved Benefits

This implementation has delivered several operational and security advantages:

- **Advanced Security:** by isolating traffic within segmented VLANs, attackers face significant barriers in moving laterally across the network.
- **Centralized Control:** administrators can monitor switch status, push updates, and enforce policies from a unified dashboard eliminating the need for onsite configurations.
- **Flexible Security Policies:** VLAN interactions can be modified in real-time through FortiGate, adapting to organizational needs instantly.

- **Robust Integration:** seamless communication between Juniper switches and Fortinet firewalls ensures high performance, stability, and infrastructure coherence.

2.2.3 Centralized Authentication via Active Directory Domain Controller

In contemporary enterprise environments, secure and centralized identity management is essential to maintaining control over user access, enforcing organizational policies, and ensuring accountability. To meet these needs, the Palestinian Customs Police (PCP) has implemented a centralized authentication system using Microsoft Active Directory (AD). This architecture enables unified user authentication, centralized device management, and fine-grained access control from a single point of administration at the organization's headquarters.

Security Objectives

The centralized authentication system was designed with the following goals:

- Standardize and secure the authentication process for all users accessing network resources.
- Prevent unauthorized access to sensitive files, systems, and services.
- Enforce organizational security policies related to device usage, password complexity, and login protocols.
- Enable comprehensive auditing and traceability of user activities across departments and devices.

Architecture and Implementation

- **Active Directory Domain Environment**

At the heart of the setup is a centrally located Domain Controller, hosting Active Directory Domain Services (AD DS). All endpoint devices both at headquarters and regional branches are joined to the domain and connected securely via VPN. Each employee is issued a unique domain account tied to an Organizational Unit (OU) that reflects their departmental affiliation, allowing for department-specific policy enforcement.

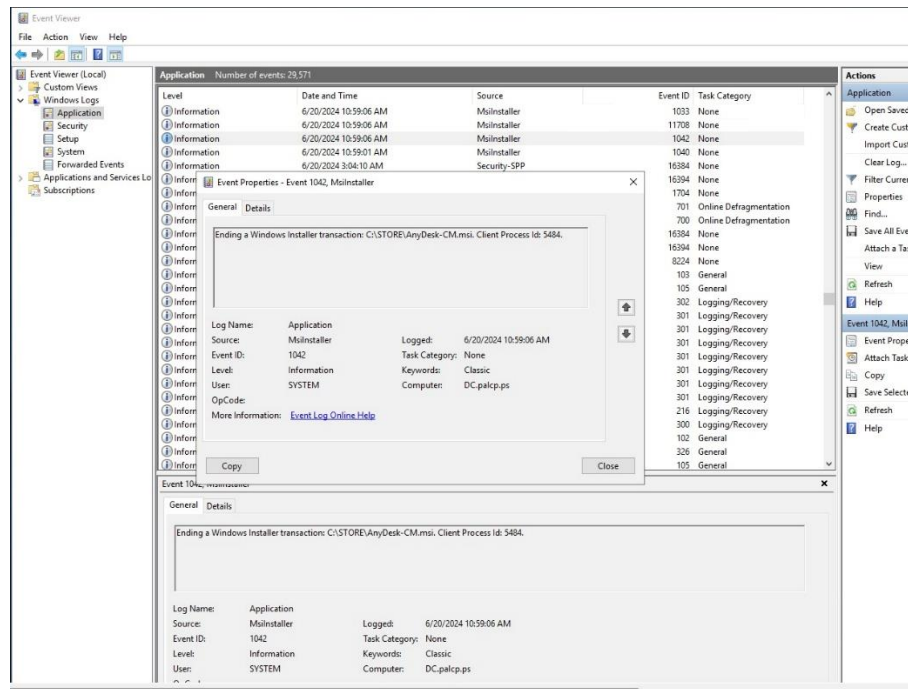


Figure 12: Domain Controller Environment Adapted from (Palestinian Customs Police, 2023).

- **Access Rights and Permissions Management**

The PCP adheres to the principle of least privilege, whereby users are granted only the minimum permissions required for their job functions. Access controls are implemented at both the NTFS and Share Permission levels, ensuring that confidential directories such as those used by the Finance and Administration departments remain accessible solely to authorized personnel.

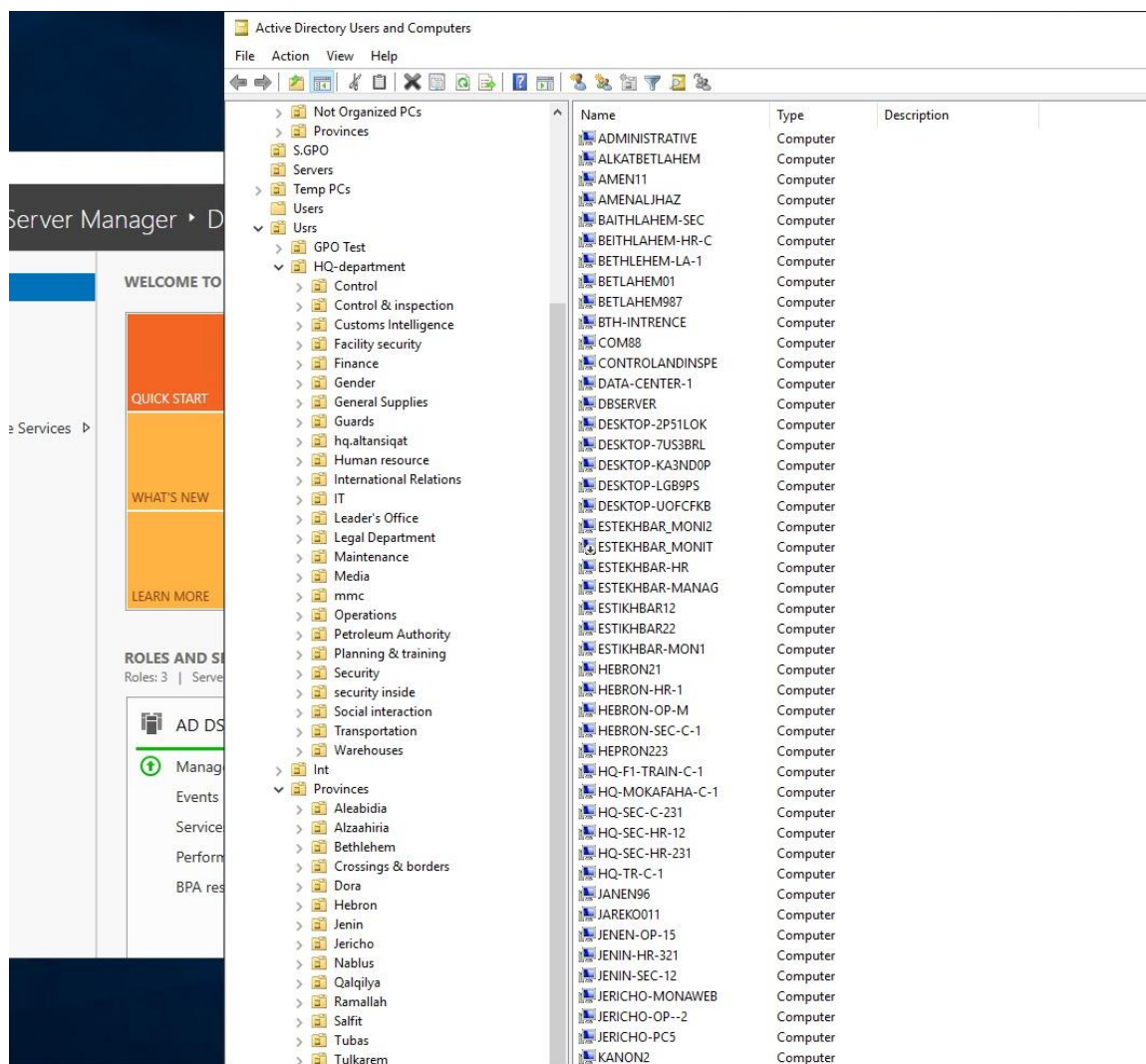


Figure 13: Access Rights and Permission Management Adapted from (Palestinian Customs Police, 2023).

- **Group Policy Objects (GPOs)**

To automate security enforcement and maintain consistency across all domain-joined devices, the PCP leverages Group Policy Objects (GPOs). These policies include:

- Enforcing password changes every 90 days.
- Restricting USB port usage on non-IT systems.
- Blocking software installations by unauthorized users.
- Displaying login banners to reinforce security compliance.

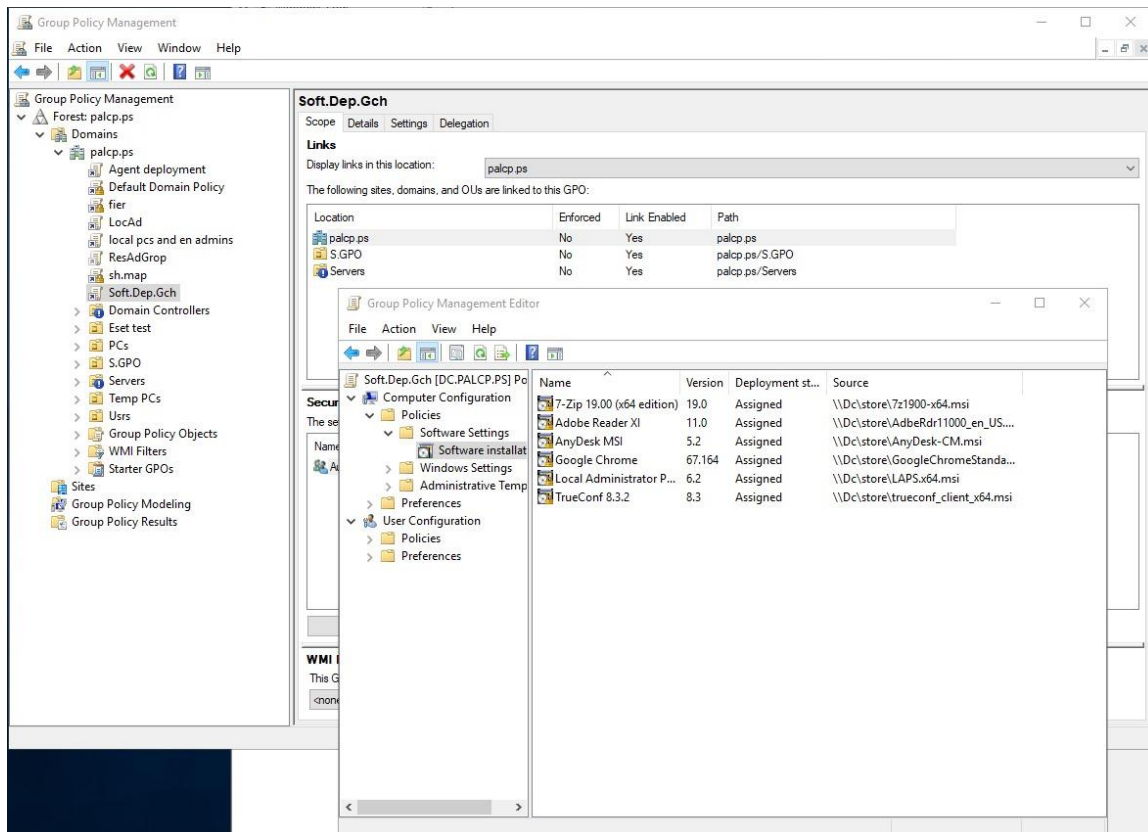


Figure 14: Group Policy management Adapted from (Palestinian Customs Police, 2023).

- **Shared File Distribution**

Centralized file servers host shared departmental resources, accessible only to authenticated users. For branches requiring remote access, the system utilizes Distributed File System (DFS) to ensure seamless connectivity and file availability, regardless of location.

Security Benefits

The implementation of Active Directory provides a secure, scalable, and auditable identity management framework with the following benefits:

- Reduced attack surface through strict access controls and elimination of local authentication dependencies.
- Full visibility and traceability of login attempts and file interactions, viewable through Windows Event Viewer and Security Information and Event Management (SIEM) systems.

- Rapid incident response, allowing administrators to isolate or disable compromised accounts instantly.
- Improved user accountability and compliance with cybersecurity standards through centralized control.

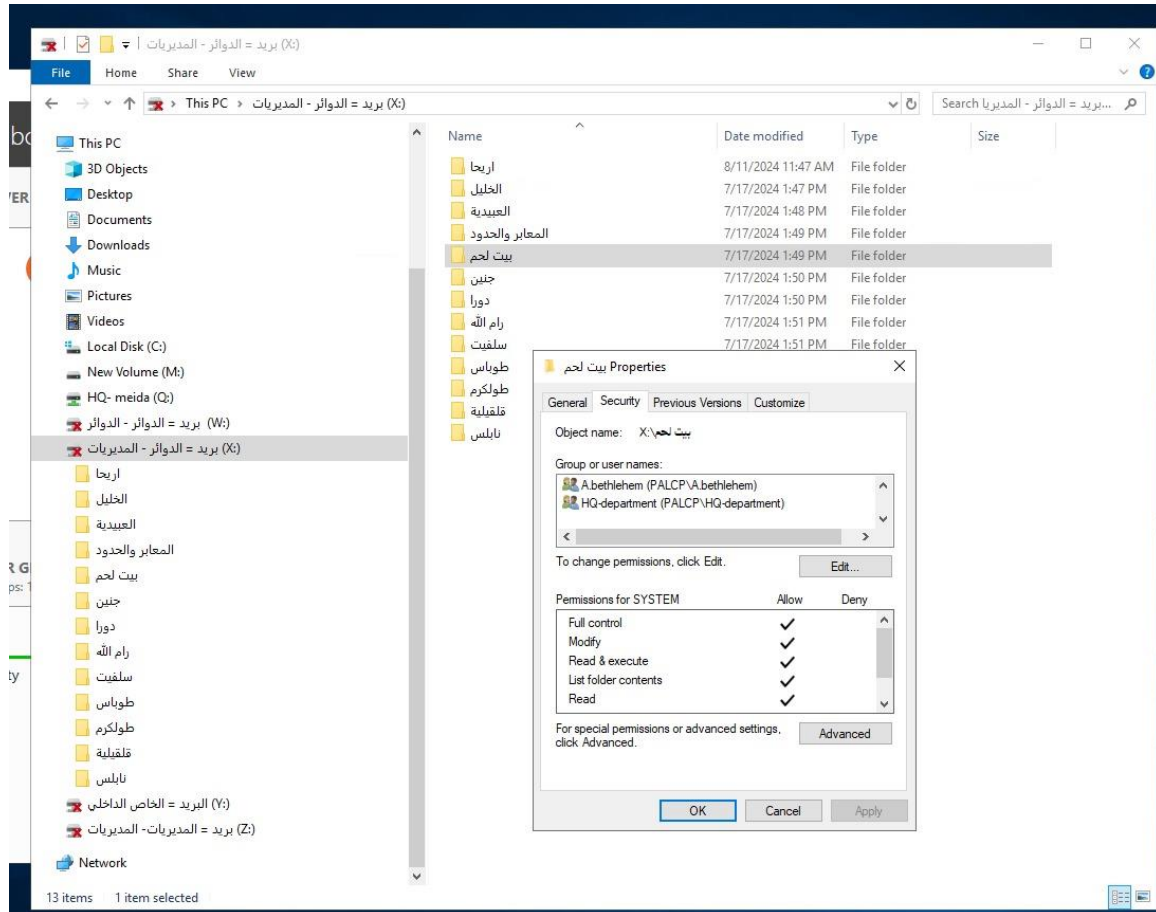


Figure 15: security properties Adapted from (Palestinian Customs Police, 2023).

2.2.4 Securing Wireless Access – Mist AP32

In any modern network infrastructure, wireless access points represent both a critical utility and a potential vulnerability. Given the open nature of wireless communications, insufficiently protected access points may serve as gateways for cyberattacks, particularly from mobile devices or unauthorized users. To mitigate these risks, the Palestinian Customs Police (PCP) has implemented a secure and centralized wireless architecture using Mist AP32 access points from Juniper. This advanced solution is managed via the Mist Cloud platform, enabling

centralized control, real-time analytics, and AI-driven optimization to uphold the highest standards of wireless security.

Wireless Security Objectives

The design and deployment of the wireless system were guided by the following security goals:

- Ensure complete isolation of wireless traffic from the core internal network.
- Continuously monitor and analyze wireless connections in real time.
- Minimize the risk of breaches originating from mobile devices or guest access points.

Implementation Architecture

- Access Point Deployment and Management

Mist AP32 access points have been deployed across all PCP facilities, including both headquarters and branch locations. The entire infrastructure is administered through Mist Cloud, which enables real-time configuration management, cloud-based analytics, and over-the-air updates. Its microservices architecture ensures high availability and responsive network behavior, reducing potential downtimes and improving scalability.

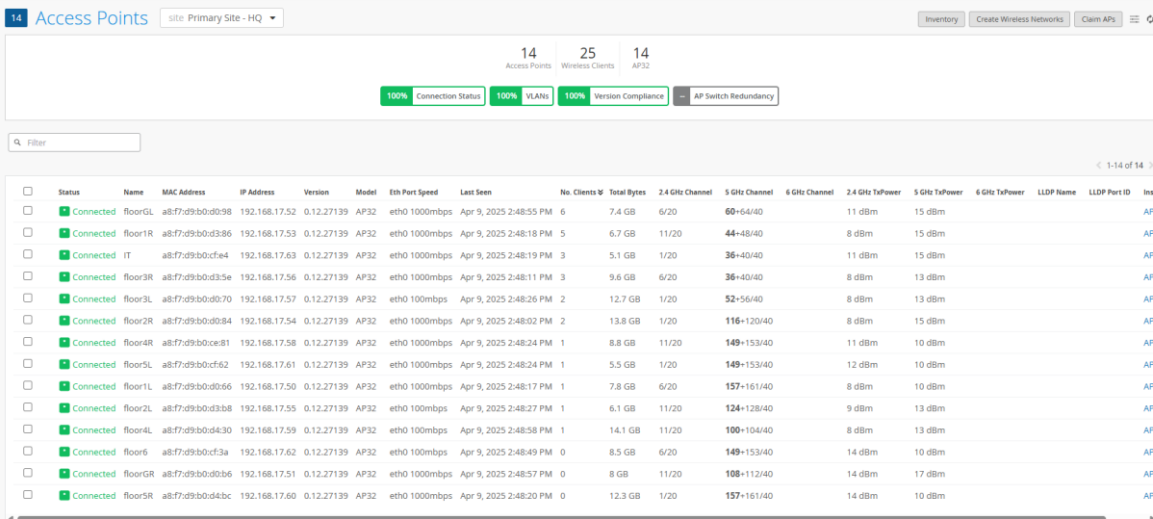


Figure 16: Mist AP32 configuration and usage Adapted from (Palestinian Customs Police, 2023).

- **Wireless Network Isolation**

To enforce strict separation from internal systems, the wireless network is mapped to a dedicated VLAN (e.g., Vlan: Wi-Fi). Traffic originating from this VLAN is restricted from reaching internal services such as file servers or management workstations. Instead, devices connected to this network are limited to Internet access only, effectively containing any potential threats originating from wireless clients.

- **SSID Configuration and Access Control**

Multiple SSIDs are configured through Mist Cloud to segment user access according to organizational roles:

- **Employee Wi-Fi:** Provides Internet-only access for staff members using WPA3 encryption and controlled through Dynamic Pre-Shared Keys (DPSK).
- **Guest Wi-Fi:** Designed for visitors, this network is completely isolated from internal resources and operates under strict access limitations.
- **Client Isolation:** Enabled within each SSID to prevent peer-to-peer communications, ensuring that one wireless client cannot interact with another.

25

WiFi Clients

site Primary Site - HQ

Live Guest

25

Wireless Clients

122.4 GHz

135 GHz

12802.11ac

2802.11ax

11802.11n

Filter

<1-25 of 25>

<input type="checkbox"/>	User	IPv4 Address	MAC Address	Device Type	AP Name	R	SSID	Pre-Shared Key	Insights
<input type="checkbox"/>	wyousef	192.168.8.85	60a5e2911a72	Intel Corporate	floor1L		PCP		Client Insights
<input type="checkbox"/>	hramadan	192.168.8.12	4218de9de54f	Unknown	floor1R		PCP		Client Insights
<input type="checkbox"/>	halhodaly	192.168.8.51	466e84ad34c3	iPhone	floor1R		PCP		Client Insights
<input type="checkbox"/>	halhodaly	192.168.8.26	48875918ee86	Xiaomi Communications Co Ltd	floor1R		PCP		Client Insights
<input type="checkbox"/>	mshbeeb	192.168.8.33	92972553eaddf	Samsung Galaxy S22 Ultra	floor1R		PCP		Client Insights
<input type="checkbox"/>	bsawafah	192.168.8.32	e6ba0861e011	Unknown	floor2L		PCP		Client Insights
<input type="checkbox"/>	ftomaizeh	192.168.8.35	12dbd8a39b94	Unknown	floor2R		PCP		Client Insights
<input type="checkbox"/>	AMPAK Technology	192.168.8.87	e076d07739ad	AMPAK Technology	floor2R		TV		Client Insights
<input type="checkbox"/>	raafat	192.168.8.42	9251fa8dd6d8d	Unknown	floor3L		PCP		Client Insights
<input type="checkbox"/>	alim	192.168.8.25	ea72803c17bb	Unknown	floor3L		PCP		Client Insights
<input type="checkbox"/>	android-9f7a5002856a884b	192.168.8.3	000bfa0511d6	Asiarock Technology Limited	floor3R		TV		Client Insights
<input type="checkbox"/>	aayoub	192.168.8.27	1a819134f5a7	iOS	floor3R		PCP		Client Insights
<input type="checkbox"/>	fadle	192.168.8.39	be0c5e5dc95e	Unknown	floor3R		PCP		Client Insights
<input type="checkbox"/>	stafesh	192.168.8.22	c2363d25fb7f	Unknown	floor4L		PCP		Client Insights
<input type="checkbox"/>	Rallah	192.168.8.73	aa92241f8bref	Unknown	floor4R		PCP		Client Insights
<input type="checkbox"/>	Apple	192.168.8.10	caf15fd421bf	Apple	floor5R		PCP GUEST		Client Insights
<input type="checkbox"/>	bjebreen	192.168.8.7	2a54957bd086	ZTE Blade A1	floorGL		PCP		Client Insights
<input type="checkbox"/>	bjebreen	192.168.8.4	4ed40989423e	iPhone	floorGL		PCP		Client Insights
<input type="checkbox"/>	hshad	192.168.8.16	fa6b0a00704c3	Unknown	floorGL		PCP		Client Insights

Figure 17: Connected Wi-Fi clients and SSIDs Adapted from (Palestinian Customs Police, 2023).

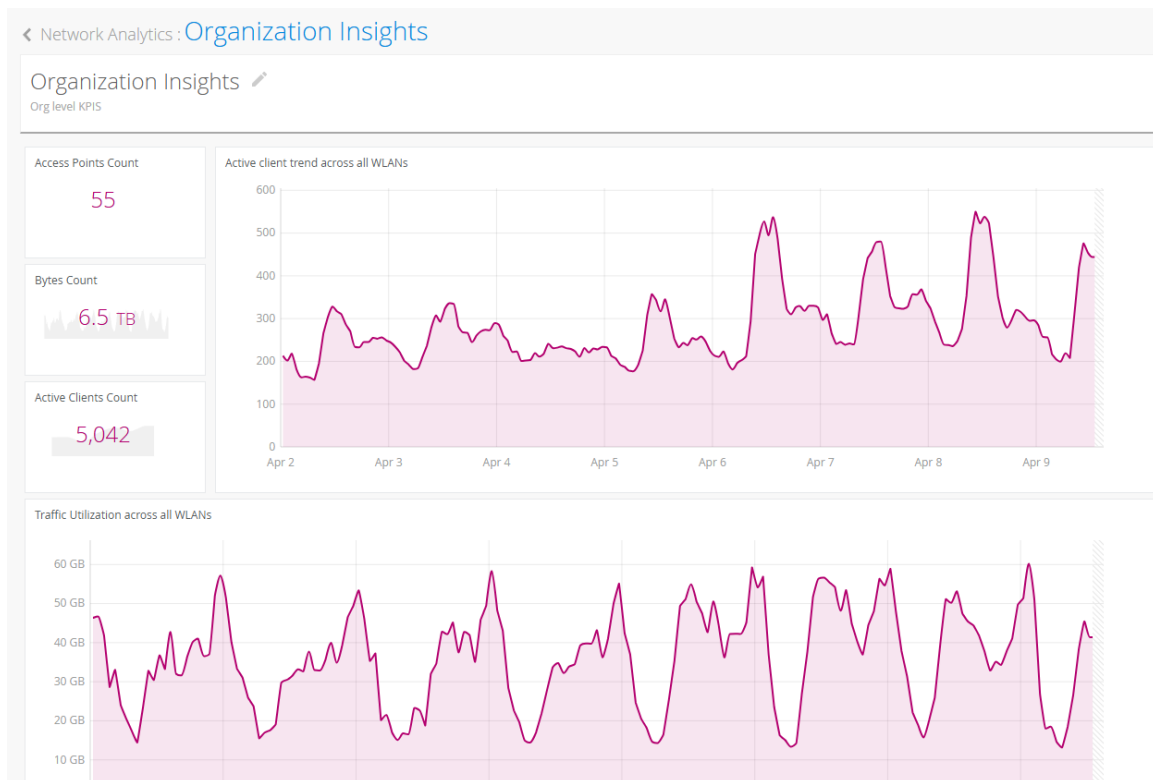


Figure 18: Organizational Wi-Fi analytics overview Adapted from (Palestinian Customs Police, 2023).

- **Encryption and Policy Enforcement**

The employee SSID is secured using WPA3-Enterprise encryption protocols, and all user credentials are authenticated via 802.1X and RADIUS servers. Strong password policies are enforced and regularly updated. Mist's Service Level Expectations (SLEs) and AI-driven analytics monitor the wireless environment for anomalies, service degradation, and suspicious behavior.

CUSTOMS POLICE

SSID

PCP

WLAN ID

7e147248-ec89-424d-a982-91615baf09c8

Labels

PCP x +

WLAN Status

☒ Enabled ☐ Disabled

☐ Hide SSID

☐ Broadcast AP name

☐ Disable WLAN when AP Gateway is unreachable

Radio Band

☒ 2.4 GHz ☒ 5 GHz ☐ 6 GHz

Band Steering

☐ Enable

Client Inactivity

Drop inactive clients after seconds: 3600

Geofence

☐ Minimum client RSSI (2.4G) 0

☐ Minimum client RSSI (5G) 0

☐ Minimum client RSSI (6G) 0

Block clients having RSSI below the minimum

Security

Security Type

WPA3 WPA2 OWE Open Access

Enterprise (802.1X) Personal (PSK)

☐ MAC address authentication by RADIUS lookup

☐ Prevent banned clients from associating

Edit banned clients in [Network Security Page](#)

Fast Roaming

☐ Default

☐ Opportunistic Key Caching (OKC)

☒ .11r

802.1X Web Redirect

Allow 802.1X Web Redirect for quarantine or posture assessment based on RADIUS server response containing url-redirect AVP

☐ Enabled ☒ Disabled

Passpoint

☐ Enabled ☒ Disabled

Authentication Servers

RADIUS

RADIUS Authentication Servers

192.168.1.8 : 1812 primary

Add Server

Apply to Access Points

All APs AP Labels Specific APs

Isolation

Prohibit peer to peer communication

☒ Disabled ☐ Same AP ☐ Same Subnet

Filtering (Wireless)

☐ ARP

☐ Broadcast/Multicast

☐ Ignore Broadcast SSID Probe Requests

Custom Forwarding

☐ Custom Forwarding to None

SSID Scheduling

☐ Enabled ☒ Disabled

QoS Priority

☐ Override QoS

AirWatch

☐ Enabled ☒ Disabled

Bonjour Gateway

☐ Enabled ☒ Disabled

Figure 19: WLAN authentication with RADIUS and 802.1X Adapted from (Palestinian Customs Police, 2023).

WLANs site: Primary Site - HQ Add WLAN

Filter

	SSID	Enabled	Template	Band	Security	VLAN ID	WLAN Limit	Client Limit	Guest Portal	WLAN Labels	Forwarding
<input type="checkbox"/>	IT	<input checked="" type="radio"/>	none	2.4GHz, 5GHz	WPA2/PSK	88	Unlimited / Unlimited	Unlimited / Unlimited	Disabled		Disabled
<input type="checkbox"/>	PCP	<input checked="" type="radio"/>	none	2.4GHz, 5GHz	WPA2/EAP (802.1X)	88	Unlimited / Unlimited	3 Mbps / 6 Mbps	Disabled	PCP	Disabled
<input type="checkbox"/>	PCP GUEST	<input checked="" type="radio"/>	none	2.4GHz, 5GHz	Open Access	88	5 Mbps / 10 Mbps	Unlimited / Unlimited	Disabled		Disabled
<input type="checkbox"/>	TV	<input checked="" type="radio"/>	none	2.4GHz, 5GHz	WPA2/PSK	88	5 Mbps / 10 Mbps	Unlimited / Unlimited	Disabled		Disabled

Figure 20: SSID overview and bandwidth limits Adapted from (Palestinian Customs Police, 2023).

Security Benefits

This wireless security framework has yielded substantial advantages:

- **Full network segmentation**, preventing wireless users from accessing sensitive internal systems.
- **Centralized visibility and control** over all access points, connections, and user activities.

- **AI enhanced security**, enabling automated detection of vulnerabilities and enforcement of protection measures.
- **Rapid response capabilities**, including immediate revocation of access or deactivation of devices upon detection of unauthorized or suspicious activity.

2.2.5 Endpoint Protection System – ESET XDR

In modern network environments, end-user devices are among the most exposed and frequently targeted components. Serving as the primary interface between users and critical organizational resources, these endpoints often become the entry point for cyber threats such as ransomware, malware, and advanced persistent threats. To address these vulnerabilities, the Palestinian Customs Police (PCP) has implemented the ESET Extended Detection and Response (XDR) system. This advanced endpoint protection platform combines artificial intelligence, behavioural analytics, and centralized control to secure user devices and enable proactive threat response.

Security Objectives

The ESET XDR system is designed with the following security goals:

- Protecting all endpoint devices against a wide spectrum of threats, including viruses, malware, and ransomware.
- Monitoring and analyzing the behavior of applications and files in real time.
- Detecting advanced threats and responding either automatically or through administrator-guided actions.

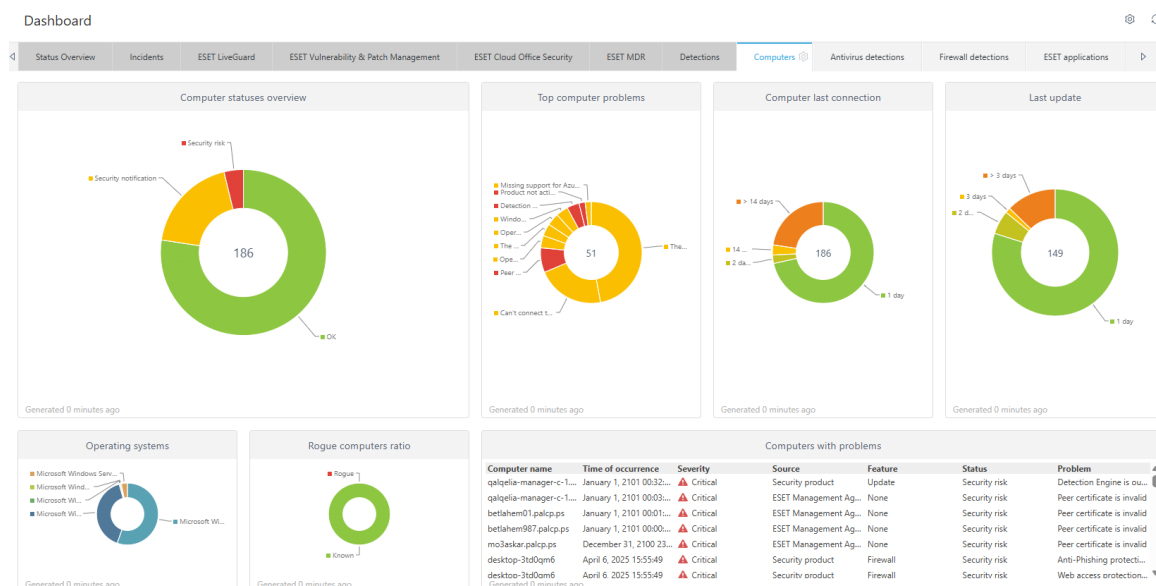


Figure 21: ESET dashboard: protection and vulnerabilities Adapted from (Palestinian Customs Police, 2023).

Implementation Approach

• System Deployment and Central Management

The ESET XDR agent has been installed on all organizational endpoints across both headquarters and branch offices. All protected devices are connected to the ESET PROTECT Cloud Console, which serves as the centralized command center for monitoring endpoint health, issuing policies, scheduling scans, and pushing updates. This architecture ensures that every device receives consistent and up-to-date security configurations.

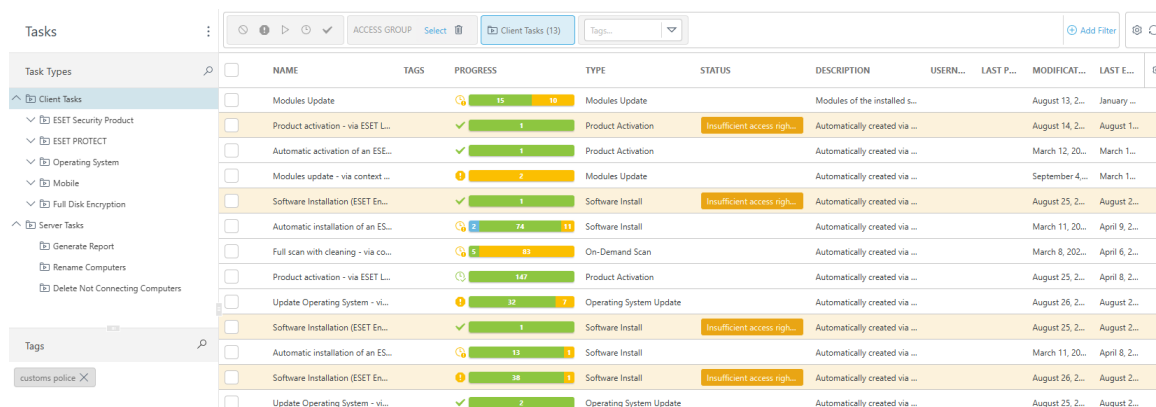


Figure 22: Task automation for software and module updates Adapted from (Palestinian Customs Police, 2023).

- **Active Security Functions:**

- **Real-Time Threat Detection:** Continuously scans running applications and system processes to detect known and unknown threats, including zero-day attacks.
- **Behavioral Analysis:** Observes application behavior patterns to identify suspicious activity that may bypass traditional signature-based detection.
- **Exploit Blocker:** Prevents exploitation of vulnerabilities in widely used applications such as web browsers and document editors.
- **Ransomware Shield:** Actively defends against ransomware attacks by monitoring attempts to encrypt files or escalate privileges.
- **Firewall & Network Attack Protection:** Detects and blocks network-based attacks at the device level, adding an extra layer of protection beyond the perimeter firewall.

- **Centralized Response Capabilities**

In the event of a security incident, the system enables rapid containment and remediation through the management console:

- **Automatic Isolation:** Infected or high-risk devices are immediately quarantined from the network.
- **Remote Response:** Administrators can remotely initiate scans, remove malware, or terminate suspicious processes without user intervention.
- **Real-Time Notifications:** Alerts are dispatched to system administrators to ensure timely investigation and resolution.

- **Reporting and Analytics**

ESET XDR provides comprehensive insights into the organization's security posture through:

- **Automated Reports:** Regularly generated summaries include threat detection statistics, system health, and compliance levels.

- **Security Scores:** Departments are assigned security ratings based on endpoint performance and risk exposure, facilitating targeted improvements.
- **Threat Logs:** A detailed audit trail of detected threats and actions taken enhances forensic analysis and accountability.

STAT	DETECTION CAT	DETECTION TYPE	CAUSE	ACTION	OCC	RES	COMPUTER NAME	IP ADDRESS	OBJECT	PRO	USER	OCCURRED
1	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:20:11
1	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:20:48
13	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	13	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:20:48
13	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	13	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:20:48
1	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:21:05
2	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	2	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:21:19
2	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	2	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:21:33
2	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	2	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:21:45
1	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:22:15
1	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:22:18
1	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:22:39
1	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:22:45
1	Antivirus	Potentially unwanted application	Win3...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:22:50
1	Antivirus	Trojan	LNK/...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:23:43
1	Antivirus	Trojan	MSIL/...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:23:56
1	Antivirus	Trojan	MSIL/...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:23:56
1	Antivirus	Trojan	MSIL/...	Cleaned ...	1	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:23:56
3	Antivirus	Trojan	Win3...	Deleted	3	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:23:56
3	Antivirus	Trojan	Win3...	Deleted	3	✓	backup...	192.168.1.2	file:///...	NT AU...	NT AU...	March 12, 2025 17:23:56

Figure 23: Detected threats and actions by ESET Adapted from (Palestinian Customs Police, 2023).

Achieved Security Benefits

The deployment of ESET XDR has resulted in several measurable advantages for the PCP:

- Multi-layered protection for all endpoints against a variety of known and emerging threats
- Centralized visibility and control over all organizational devices through a single cloud interface
- Faster incident response, minimizing the impact of attacks without halting day-to-day operations
- Effective threat containment, limiting the spread of infections and preserving network integrity

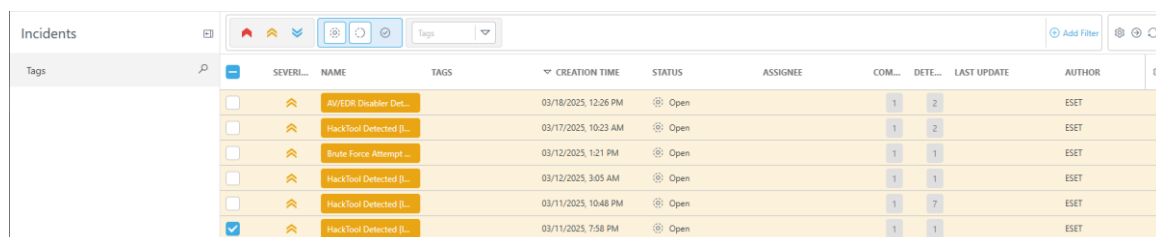
2.2.6 Continuous Monitoring and Logging

In modern cybersecurity frameworks, perimeter defenses and access control mechanisms alone are insufficient to secure an organization's infrastructure. Continuous monitoring and centralized logging are essential components of an effective defense in depth strategy. These tools provide real-time visibility into network and endpoint activities, allowing administrators to detect anomalies, trace incidents, and respond to threats swiftly. For the Palestinian Customs Police (PCP), a comprehensive monitoring infrastructure has been established to track user behavior, analyze traffic patterns, and ensure compliance with regulatory requirements.

Primary Objectives

The implementation of continuous monitoring aims to achieve the following:

- Enable early detection of unusual or potentially harmful behavior across systems and users.
- Maintain detailed logs of all critical events, including login attempts, file modifications, and system alerts.
- Simplify the analysis and response process during or after security incidents.
- Ensure compliance with audit and legal requirements by maintaining a verifiable record of system activities.



Incidents										
Tags	SEVERITY	NAME	TAGS	CREATION TIME	STATUS	ASSIGNEE	COM...	DETE...	LAST UPDATE	AUTHOR
<input type="checkbox"/>	High	AV/EDR Disabled Det...		03/18/2025, 12:26 PM	Open		1	2		ESET
<input type="checkbox"/>	High	HackTool Detected [L...		03/17/2025, 10:23 AM	Open		1	2		ESET
<input type="checkbox"/>	High	Brute Force Attempt ...		03/12/2025, 1:21 PM	Open		1	1		ESET
<input type="checkbox"/>	High	HackTool Detected [L...		03/12/2025, 3:05 AM	Open		1	1		ESET
<input type="checkbox"/>	High	HackTool Detected [L...		03/11/2025, 10:48 PM	Open		1	7		ESET
<input checked="" type="checkbox"/>	High	HackTool Detected [L...		03/11/2025, 7:58 PM	Open		1	1		ESET

Figure 24:ESET XDR incidents and endpoint behavior Adapted from (Palestinian Customs Police, 2023).

Monitoring and Logging Mechanisms

- **Forti Cloud Logging – Firewall Event Management**

All FortiGate firewalls deployed across the headquarters and regional branches are integrated with Forti Cloud, providing centralized log aggregation and analysis.

Critical events such as failed login attempts, suspicious outbound connections, and unauthorized inter-VLAN activity are automatically detected and logged. The system generates real-time alerts that are displayed in the management dashboard or sent via email, ensuring rapid administrator awareness and intervention.

- **Forti View – Traffic Analytics and Visualization**

Forti View, a powerful tool within the Fortinet ecosystem, is used to monitor and analyze live traffic flows. It provides insights into:

- Source IP addresses.
- Applications and protocols used.
- Destination countries or regions.
- Policy ID classifications and rule matches.

This visual representation enables network administrators to understand who is accessing the network, what resources are being used, and whether those interactions align with internal policies.

- **ESET XDR – Endpoint Monitoring**

Complementing the firewall systems, ESET XDR provides detailed endpoint logging and security intelligence. Through the ESET PROTECT Cloud Console, the following information is continuously monitored and reported for each device:

- Last update time.
- Security status.
- Number of detected and resolved threats.

This endpoint-level insight reinforces network visibility and strengthens the institution's ability to respond to internal threats.

2025/04/09 16:03:10	192.168.1.4	DC	8.8.8.8 (dns.google)	DNS	✓ Accept (159 B / 253 B)	SER to INTERNET (1
2025/04/09 16:03:10	192.168.8.22		57.144.120.141 (starfallback.c10r.facebook.com)	udp/443	✓ Accept (1.88 kB / 5.69 kB)	WIFI to INTERNET (:
2025/04/09 16:03:10	192.168.8.3		172.67.163.215 (www.hanajula.com)	udp/443	✓ Accept (3.68 kB / 5.04 kB)	WIFI to INTERNET (:
2025/04/09 16:03:09	192.168.8.42		142.250.200.238 (android.clients.google.com)	HTTPS	✓ Accept (2.57 kB / 7.54 kB)	WIFI to INTERNET (:
2025/04/09 16:03:09	192.168.40.45		34.141.162.50 (nl-ams-gcp-r001.router.teamviewer.com)	tcp/5938	✓ Accept (1.71 MB / 1.48 MB)	DMAZ-TO-Internet
2025/04/09 16:03:09	185.207.214.234		213.6.8.91	Portal-Services	✓ Accept (0 B / 300 B)	From-Outside-To-ser
2025/04/09 16:03:09	192.168.1.3	DATA-CENTER-1	172.172.255.218	HTTPS	✓ Accept (8.75 kB / 11.67 kB)	SER to INTERNET (1
2025/04/09 16:03:09	95.130.93.42		213.6.8.92	tcp/8484	✓ Accept (397 B / 180 B)	Track-SRV (50)
2025/04/09 16:03:09	192.168.8.4		157.240.253.5 (chat-e2ee.c10r.facebook.com)	tcp/5222	✓ Accept (3.23 kB / 1.34 kB)	WIFI to INTERNET (:
2025/04/09 16:03:09	192.168.8.3		172.247.13.218 (www.dxfzps.com)	HTTPS	✓ Accept (60 B / 0 B)	WIFI to INTERNET (:
2025/04/09 16:03:08	192.168.8.24		91.108.17.53	udp/598	✓ Accept (310.61 MB / 288.49 MB)	WIFI to INTERNET (:
2025/04/09 16:03:08	192.168.8.16		34.194.94.135 (ec2-34-194-94-135.compute-1.amazonaws.com)	HTTPS	✓ Accept (240 B / 0 B)	WIFI to INTERNET (:
2025/04/09 16:03:08	192.168.8.27		213.244.78.10 (v77.tiktokcdn.com)	HTTPS	✓ Accept (4.95 kB / 72.91 kB)	WIFI to INTERNET (:
2025/04/09 16:03:08	192.168.8.27		2.21.12.167 (e28622.bakamaledge.net)	HTTPS	✓ Accept (4.72 kB / 1.28 kB)	WIFI to INTERNET (:
2025/04/09 16:03:08	192.168.8.27		213.244.78.10 (v77.tiktokcdn.com)	HTTPS	✓ Accept (2.21 kB / 1.2 kB)	WIFI to INTERNET (:
2025/04/09 16:03:08	192.168.8.27		213.244.74.194 (qsearch-a.akamaihd.net)	HTTPS	✓ Accept (2.16 kB / 1.12 kB)	WIFI to INTERNET (:
2025/04/09 16:03:08	nsamara (192.168.11.190)	HQ-OP-ENTRY-C-2	192.168.10.199	udp/8610	✓ Accept (176 B / 0 B)	1st to cam (26)
2025/04/09 16:03:08	nsamara (192.168.11.190)	HQ-OP-ENTRY-C-2	192.168.10.199	udp/8610	✓ Accept (ip-conn)	1st to cam (26)
2025/04/09 16:03:08	192.168.8.18		2.18.254.57 (rtlog16-normal-allsg.tiktokv.com.byetwlb.akadns.net)	HTTPS	✓ Accept (1.32 kB / 1.24 kB)	WIFI to INTERNET (:

Figure 25: Live Fortinet session log with destinations Adapted from (Palestinian Customs Police, 2023).

Server and System Logging

Using Windows Event Viewer, login sessions, file access events, and policy modification attempts are logged on servers and administrative systems. For broader correlation and analysis, logs can be centralized via Security Information and Event Management (SIEM) platforms, enhancing threat detection across the infrastructure.

DHCP

106

Total

Leased out

Removed due to co...

100

4

106

Total

Wi-Fi

1st floor

2nd floor

4th floor

3rd floor

More...

21

21

21

10




























6

⌂

Revolve

🔍

Search

<input type="checkbox"/>	Device	IP	Interface	Status	MAC	Reserved	Host Information
<input type="checkbox"/>	 Android	192.168.11.100	 1st floor	Leased out	00:e0:db:7a:7f:b7	 Not Reserved	VCI: Poly-StudioX50 Hostname: StudioX50-7A7FB7FB
<input type="checkbox"/>	 DESKTOP-PB5OAQT	192.168.11.102	 1st floor	Leased out	00:1b:21:ec:36:8d	 Not Reserved	VCI: MSFT 5.0 Hostname: DESKTOP-PB5OAQT
<input type="checkbox"/>	 op3lenovo.palcp.ps	192.168.11.118	 1st floor	Leased out	00:1b:21:ec:33:16	 Not Reserved	VCI: MSFT 5.0 Hostname: op3lenovo
<input type="checkbox"/>	 KM085251	192.168.11.107	 1st floor	Leased out	d4:f0:c9:08:52:51	 Not Reserved	Hostname: KM085251
<input type="checkbox"/>	 DESKTOP-D58J65N	192.168.11.109	 1st floor	Leased out	bce9:2fa6:dc:da	 Not Reserved	VCI: MSFT 5.0 Hostname: DESKTOP-D58J65N
<input type="checkbox"/>	 HQ-OP-ENTRY-C-2	192.168.11.190	 1st floor	Leased out	c0:18:03:b8:35:b2	 Not Reserved	VCI: MSFT 5.0 Hostname: hq-op-entry-c-2
<input type="checkbox"/>	 OP322022	192.168.11.120	 1st floor	Leased out	c4:65:16:23:95:8b	 Not Reserved	VCI: MSFT 5.0 Hostname: op322022
<input type="checkbox"/>	 HQ-TRAINING-C-3	192.168.11.104	 1st floor	Leased out	c0:18:03:b6:c5:86	 Not Reserved	VCI: MSFT 5.0 Hostname: hq-training-c-3
<input type="checkbox"/>	 DESKTOP-9ICA31R	192.168.11.126	 1st floor	Leased out	10:1f:74:ee:43:5d	 Not Reserved	VCI: MSFT 5.0

Firmware

View repository

FG-SEC

Figure 26: DHCP interface lease tracking Adapted from (Palestinian Customs Police, 2023).

Operational and Security Benefits

The deployment of continuous monitoring and logging solutions has significantly improved the PCP's cybersecurity posture by:

- Supporting detailed forensic investigations following incidents or breaches.
- Detecting stealthy or low-profile attacks that may evade traditional security systems.
- Building a behavioral dataset to understand normal and abnormal activity patterns.
- Empowering data-driven decision-making through accurate and timely security intelligence.

2.2.7 Camera System Segmentation and Security

The Closed-Circuit Television (CCTV) surveillance system plays a vital role in enhancing situational awareness and securing critical infrastructure. However, integrating such systems into the broader organizational network without proper isolation can introduce significant cybersecurity vulnerabilities. Recognizing these risks, the Palestinian Customs Police (PCP) have implemented a dedicated, segmented network architecture for its surveillance infrastructure. This approach ensures that video traffic remains secure, controlled, and separate from core business operations.

Security Objectives

The CCTV system's design is aligned with the following security goals:

- Prevent unauthorized internal or external access to the camera infrastructure.
- Restrict access to live streams and recorded footage to approved devices and personnel.
- Prevent the surveillance network from serving as a launchpad for cyberattacks on other systems.

The screenshot displays the HikCentral Professional Web Client interface. The left sidebar shows navigation options like 'Resource Management', 'Device and Server', 'Encoding Device', 'Display Screen', 'Network Transmission D...', 'Recording Server', 'Streaming Server', 'DeepinMind Server', 'Area', 'Firmware Upgrade', and 'Device Application'. The main content area is titled 'Resource Management' and shows a list of devices. The table below represents the data shown in the screenshot.

Device Name	Device Address	Serial No.	Version	Available Cameras	Alarm Inputs/Outp...	Network Status	Password Strength	Operation
dora	10.40.128.5	DS-7616NI-K2/16P162...	V4.74.205 build 230712	5	0/0	Online	Strong	
salit	10.235.128.5	DS-7616NI-K21620180...	V4.30.5 build 200628	9	4/1	Online	Risky	
qigila	10.180.128.5	DS-7616NI-K216202201...	V4.60.0 build 211129	8	4/1	Online	Strong	
tulkarem	10.165.128.5	DS-7616NI-K216202202...	V4.60.5 build 220108	8	4/1	Online	Strong	
thahria	10.41.128.5	DS-7608NI-K20820220...	V4.32.116 build 220112	6	4/1	Online	Medium	
tubas	10.230.128.5	DS-7616NI-K2162024...	V4.82.7 build 240321	9	4/1	Online	Strong	
baithlahem	10.60.128.5	DS-7616NI-K2162024...	V4.82.7 build 240321	10	4/1	Online	Strong	
lucanem	10.109.128.5	DS-7608NI-K20820220...	V4.13.116 build 230112	5	4/1	Online	Medium	

Below the table, there is a section for 'Online Device' with a search bar and a table with columns: Device Address, Serial No., Device Port, HTTP Port, Subnet Mask, Gateway, Activated or Not, Added or Not, Used DHCP or ..., and Operation. The table is currently empty, showing 'No data'.

Figure 27: NVRs per location with online status Adapted from (Palestinian Customs Police, 2023).

Implementation Details:

- **Dedicated VLAN for Camera Infrastructure**

All surveillance cameras across PCP's headquarters and regional branches are connected to a dedicated VLAN (cam) that is fully isolated from the main network. This VLAN is configured on Juniper switches, with access ports exclusively assigned to surveillance devices. Each location houses a local Network Video Recorder (NVR) for on-site video storage, minimizing the need for real-time data transfer across the network and preserving bandwidth.

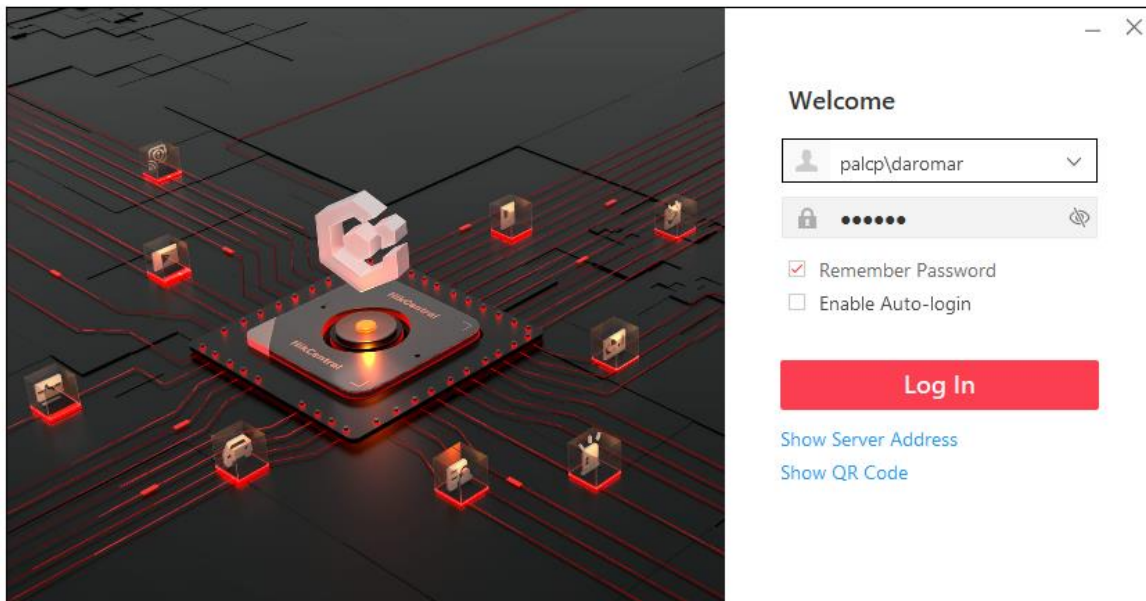


Figure 28: NVR system login via domain account Adapted from (Palestinian Customs Police, 2023).

- **Network Isolation**

The cam VLAN is strictly segmented from other VLANs such as SRV (servers) or WIFI (wireless users). Wireless devices, public IP addresses, and general internet traffic are entirely blocked from accessing the camera system. Only authorized devices typically within the IT VLAN can manage or retrieve footage, either directly or through secure VPN access via administrative workstations.

- **Access and Communication Security**

Security best practices are rigorously applied to all components of the camera infrastructure:

- Unique, strong passwords are enforced on all cameras and NVRs.
- HTTPS encryption is required for all communication between cameras, NVRs, and client interfaces.

- All login attempts to NVRs are logged and reviewed regularly for suspicious activity.

- **Recording Policies and Monitoring**

Cameras support motion detection, real-time alerts, and customizable recording modes (continuous or motion-based). Video retention periods are defined in line with the PCP's internal data privacy policy, ensuring both operational effectiveness and legal compliance.

+ Add Delete Inactivate Activate Refresh All				
<input type="checkbox"/>	Role Name ↕	Role Status ↕	Effective Period ↕	Description ↕
<input type="checkbox"/>	Administrator	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	The role has all the permissions
<input type="checkbox"/>	Operator	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	The role has permissions to access all the res
<input type="checkbox"/>	HQ	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	tulkarem	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	tubas	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	salfit	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	qalqilia	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	obaideia	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	nablus	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	lawazem	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	jericho	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	jenin	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	camp	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	internal control	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	thahrya	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	dora	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	hebron	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	
<input type="checkbox"/>	baithlehem	Normal	2016/01/01 00:00:00-2099/12/31 23:59:59	

Figure 29: Role-based access to camera systems Adapted from (Palestinian Customs Police, 2023).

Achieved Security Benefits

The isolation and segmentation of the camera system provide several advantages:

- Elimination of surveillance infrastructure as a potential attack vector.
- Improved video service quality by reducing competition for network resources.

- Centralized visibility and control over system access and activity logs.
- Alignment with regulatory and privacy standards, ensuring responsible use of surveillance technologies.

2.2.8 Updates and Security Awareness

In a rapidly evolving digital landscape, the resilience of an organization's cybersecurity posture hinges not only on technological defenses but also on the proactive management of system updates and the awareness level of its users. While outdated software remains a frequent entry point for cyberattacks, the human factor continues to be one of the most exploited vulnerabilities in modern threat scenarios. To mitigate these risks, the Palestinian Customs Police (PCP) have adopted a dual-focused policy combining scheduled security updates with continuous staff awareness training to ensure both technical and human elements of cybersecurity are equally fortified.

Objectives

The policy was designed to fulfill the following goals:

- Address known vulnerabilities by ensuring all systems and software are regularly updated.
- Minimize the attack surface caused by outdated applications, firmware, or operating systems.
- Empower employees with knowledge and best practices to detect, avoid, and report cybersecurity threats.

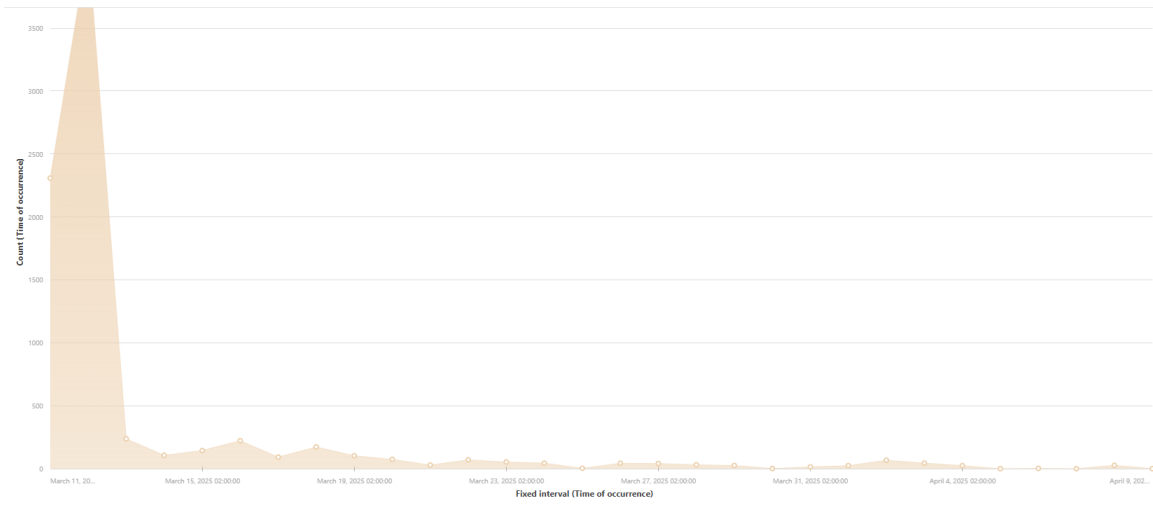


Figure 30: Threat occurrence over time Adapted from (Palestinian Customs Police, 2023).

Implementation Approach

- **System and Software Updates**

The IT team maintains responsibility for orchestrating regular updates across all systems, including:

- Windows operating systems installed on organizational endpoints.
- ESET XDR security software, managed through the centralized ESET Protect Console.
- Key infrastructure components, such as Mist access points, FortiGate firewalls, and Juniper switches.

Updates are deployed through automated tools such as Group Policy Objects (GPOs), Windows Server Update Services (WSUS), and vendor-specific cloud management platforms like Forti Cloud and Mist Cloud. Updates are tested in isolated environments prior to full rollout to ensure operational stability. Any failure in the update process triggers alert notifications to allow timely intervention.

- **Infrastructure and Firmware Maintenance**

Network devices, including Juniper switches and Mist APs, receive firmware and configuration updates via their respective centralized portals. Where possible, automatic updates are enabled to ensure minimal manual intervention. However, manual override functionality is retained to allow IT administrators to respond promptly to emergencies or critical patches.

- **Staff Cybersecurity Awareness**

Recognizing that technology alone is not enough, PCP places equal emphasis on ongoing cybersecurity awareness for all employees. Key initiatives include:

- Periodic email bulletins covering phishing prevention, password management, safe link/file sharing, and protocols for reporting suspicious activities.
- In-house training sessions conducted by the IT department, tailored to current threat trends and real-world case studies.
- Routine assessments of departmental compliance with digital security guidelines, including monitoring engagement with training materials and reporting behavior.

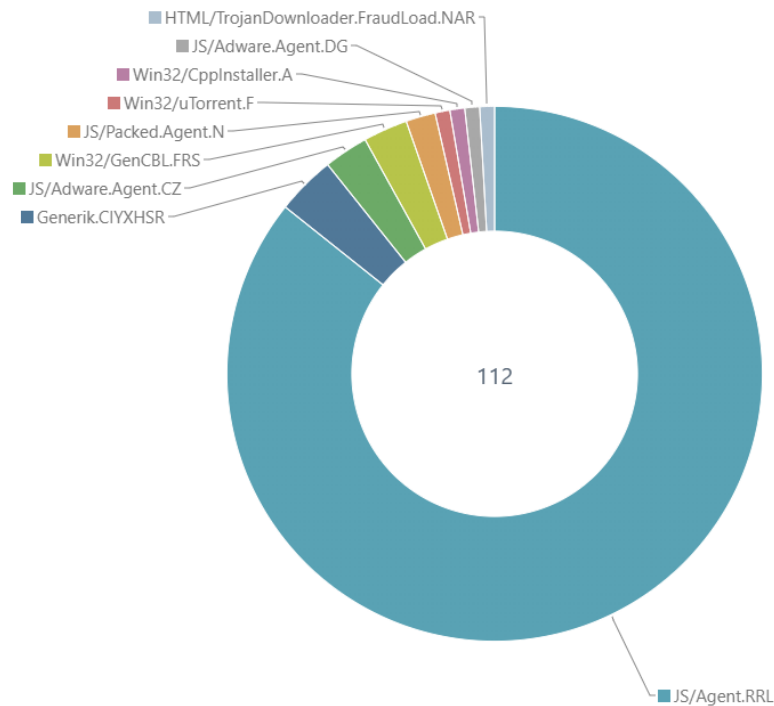


Figure 31: Malware types and distribution Adapted from (Palestinian Customs Police, 2023).

Achieved Security Benefits

The coordinated effort in maintaining system updates and enhancing staff awareness has delivered the following outcomes:

- Significant reduction in attacks leveraging outdated or unpatched software.
- Enhanced network stability and performance, with up-to-date firmware and operating systems across all devices.
- Improved user vigilance, resulting in fewer human-error-based incidents and quicker incident reporting.
- Fostered a culture of cybersecurity, where employees are actively engaged in protecting institutional data and systems.

2.3 Security framework: ISO/IEC 27001

ISO/IEC 27001 is an internationally recognized standard for information security management, providing a systematic approach to managing sensitive information and ensuring its confidentiality, integrity, and availability (International Organization for Standardization [ISO], 2013). This chapter explores the principles, framework, and implementation of ISO 27001, highlighting its critical role in strengthening cybersecurity practices. Additionally, the chapter discusses the standards and terms associated with ISO 27001 and its alignment with other frameworks, and future trends.

The increasing reliance on digital infrastructure has driven the demand for standardized security frameworks to protect sensitive information and ensure data integrity. Some of the most widely recognized frameworks are “ISO/IEC 27001”, a global standard for “Information Security Management Systems (ISMS)”. The framework provides a systematic approach in information security risk management, ensuring compliance with best practices, and encouraging a security-minded organizational culture (Humphreys, 2016).

ISO/IEC 27001 is a worldwide standard developed by the “International Organization for Standardization (ISO)” and the “International Electrotechnical Commission (IEC)” to help organizations implement, maintain, and continuously improve an ISMS (ISO, 2013). The standard has a “risk-based approach” to security, which requires organizations to discover, evaluate, and counter probable threats to security through a well-structured and continuously evolving security system (Calder & Watkins, 2019).

ISO/IEC 27001 applies the “Plan-Do-Check-Act (PDCA)” cycle to facilitate continuous improvement of security management (von Solms & von Solms, 2018). The standard includes “Annex A controls”, which are security policies for “access control, cryptography, asset management, and incident response” (ISO, 2022). The controls are designed to minimize “cybersecurity threats, unauthorized access, data breaches, and operational disruptions” (Al-Dhaheri et al., 2019).

The full spectrum of risks must be evaluated to give decision-makers a comprehensive understanding of these issues: both historical security breaches and potential future threats that may not have materialized yet. Different methodologies may be required to assess these two

risk categories. For instance, organizations might utilize internal logs to estimate the likelihood and consequences of security events.

In fact, some types of incidents have demonstrated remarkable consistency over time. For example, ISO/IEC 27001 provides guidance on handling security incidents, which many organizations have reported following a predictable pattern year after year.

However, evolving external factors could alter the frequency or severity of these events, requiring adjustments in response strategies. Additionally, some rare but high-impact threats may not have occurred yet simply because the conditions have not aligned. Thus, historical data alone is insufficient, and organizations need to supplement it with alternative risk modelling techniques. Expert insights or hypothetical scenario analysis can help fill gaps where past data is lacking, offering a more comprehensive approach to understanding and mitigating risks. By applying this framework, organizations can develop a well-rounded and proactive security management strategy that accounts for both current and emerging threats.

2.3.1 Overview of ISO 27001 Standards

ISO/IEC 27001 is part of the ISO/IEC 27000 family of standards, which provides a comprehensive framework for information security management. These standards are designed to help organizations manage the security of assets such as financial information, intellectual property, employee details, and third-party data (ISO, 2018). Key standards in the ISO/IEC 27000 family include:

- **ISO/IEC 27000:** Provides an overview and vocabulary for information security management systems (ISMS).
- **ISO/IEC 27001:** Specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS.
- **ISO/IEC 27002:** Offers guidelines for implementing the controls listed in Annex A of ISO 27001 (ISO, 2013).
- **ISO/IEC 27005:** Focuses on information security risk management (ISO, 2018).
- **ISO/IEC 27017:** Provides guidelines for information security controls applicable to cloud services (ISO, 2015).

These standards work together to create a holistic approach to information security, ensuring that organizations can address both technical and managerial aspects of cybersecurity (Calder & Watkins, 2019).

2.3.2 Key Terms in ISO 27001

Understanding the terminology used in ISO 27001 is essential for effective implementation. Below are some of the most important terms:

- **Information Security Management System (ISMS):** A systematic approach to managing sensitive company information, encompassing people, processes, and technology (Hinson, 2017).
- **Risk Assessment:** The process of identifying, analyzing, and evaluating risks to information assets (Karyda, Kiountouzis, & Kokolakis, 2005).
- **Risk Treatment:** The process of selecting and implementing measures to mitigate identified risks (IT Governance UK, n.d.).
- **Statement of Applicability (SOA):** A document that outlines the controls selected from Annex A and justifies their inclusion or exclusion (PwC, 2020).
- **Continual Improvement:** The ongoing process of enhancing the ISMS to adapt to changing threats and business needs.
- **Internal Audit:** A systematic evaluation of the ISMS to ensure compliance with ISO 27001 requirements (ISACA, 2021).
- **Certification:** The formal process of obtaining third-party validation that an organization's ISMS complies with ISO 27001 (National Institute of Standards and Technology [NIST], 2020).

2.3.3 Objectives of ISO/IEC 27001

1. **Information protection:** making sure that data is available, secure, and intact.
2. **Risk management:** Recognize, evaluate, and combat threats to information security.
3. **Legal Compliance:** Verify that pertinent laws and regulations are being followed.
4. **Increasing operational effectiveness:** Increasing information security management's efficacy and efficiency.
5. **Developing Trust:** Increasing stakeholders' and consumers' faith in the company's information security expertise.

2.3.4 Annex A Controls

Annex A of ISO 27001 provides a comprehensive list of *114 controls* grouped into *14 categories*. These controls are designed to address various aspects of information security. Below are some key categories and examples of controls:

1. **A.5 Information Security Policies:** Establishing and maintaining policies to manage information security (ISO, 2013).
2. **A.6 Organization of Information Security:** Defining roles and responsibilities for information security (ISO, 2013).
3. **A.8 Asset Management:** Identifying and classifying information assets to ensure appropriate protection (Soomro, Shah, & Ahmed, 2016).
4. **A.9 Access Control:** Restricting access to information based on business requirements (ISO, 2013).
5. **A.12 Operations Security:** Managing technical vulnerabilities and protecting against malware (ISO, 2013).
6. **A.16 Incident Management:** Establishing procedures for detecting, reporting, and responding to security incidents (ISO, 2013).

Each control is designed to address specific risks and ensure the confidentiality, integrity, and availability of information assets. These principles ensure that information is only accessible to authorized users (confidentiality), remains unaltered and protected from unauthorized modifications (integrity), and is available to authorized users when required (availability).

2.3.5 Implementation Process

Implementing ISO 27001 requires a structured approach, starting with defining the scope of the ISMS and conducting a thorough risk assessment (ISO, 2013). Organizations must then develop and implement policies, train employees, and establish monitoring mechanisms (Hinson, 2017). Achieving certification involves a rigorous external audit to verify compliance with the standard (NIST, 2020).

2.3.6 Importance of ISO/IEC 27001 in Information Security

Organizations that adopt ISO 27001 benefit from improved information security, reduced risk of data breaches, and enhanced compliance with regulatory requirements (Smith, 2022).

Certification also builds trust with customers and partners, providing a competitive edge in the marketplace (Brown, 2021).

Other research identifies the supreme significance of ISO/IEC 27001 in enhancing the security of organizations. According to Cherdantseva and Hilton (2018), implementing ISO/IEC 27001 significantly reduces exposure to cyber threats by creating a culture of security awareness and subjecting organizations to best practices for data protection.

A study by Fernández et al. (2020) discusses the economic benefits of implementation of ISO/IEC 27001, where entities that implement the standard experience fewer security incidents, less financial loss, and increased customers' and stakeholders' confidence. A study by Siponen and Willison (2020) also identifies how ISO/IEC 27001 enhances corporate reputation as it portrays commitment to risk management and cybersecurity.

2.3.7 Challenges of ISO/IEC 27001 Implementation

Despite its benefits, ISO 27001 implementation can be resource-intensive, particularly for small and medium-sized enterprises (Taylor, 2020). Critics also argue that the standard's focus on documentation may lead to a "tick-box" mentality, potentially overlooking practical security measures (Wilson, 2021).

Organizations are finding it difficult to implement ISO/IEC 27001, despite its usefulness. Based on a study carried out by da Veiga and Eloff (2019), limited resources, change resistance, and poor expertise are challenges to implementing it successfully. Furthermore, high implementation expenses and regular maintenance processes can be a challenge for small and medium-sized businesses (SMEs) (Tari et al., 2017).

The other problem is achieving compliance with new security threats, as cyber attackers continuously develop advanced attack methods. Companies need to review their ISMS periodically in order to counteract emerging threats and new vulnerabilities. (Jouini et al., 2020).

2.3.8 Alignment with Other Standards

ISO 27001 is designed to be compatible with other management system standards, such as ISO 9001 (Quality Management) and ISO 22301 (Business Continuity Management). This alignment allows organizations to integrate their ISMS with other management systems, reducing duplication of effort and improving overall efficiency (Green, 2022).

2.3.9 Future Trends in ISO 27001

As cybersecurity threats evolve, ISO 27001 is also adapting to address emerging challenges.

Key trends include:

- **Integration with Emerging Technologies:** Incorporating controls for cloud computing, IoT, and artificial intelligence (Harris, 2023).
- **Focus on Supply Chain Security:** Addressing risks associated with third-party vendors and suppliers (Clark, 2022).
- **Emphasis on Privacy:** Aligning with standards like ISO 27701 (Privacy Information Management) to address data protection requirements (Lee, 2023).

2.4 Cybersecurity knowledge and skills.

Cybersecurity, as a concept, is rooted in the convergence of two essential ideas: "cyber" and "security." The term "cyber" encompasses a broad range of digital technologies, including systems, networks, applications, and data that operate within cyberspace. Within this digital environment, cybersecurity focuses on protecting these elements from unauthorized access, disruption, or destruction. As highlighted by Aliyu (2022), cyberspace is increasingly integral to organizational functions, including learning, communication, data storage, and administration. Yet, this heavy reliance introduces complex vulnerabilities that, if not properly managed, can lead to significant institutional risks.

While many foundational definitions of cybersecurity emphasize technological dimensions such as hardware, software, and infrastructure protection, Aliyu's research draws attention to an often-overlooked aspect: the socio-cultural and organizational factors. These include institutional values, norms, and user behavior, which are critical in shaping the effectiveness of cybersecurity policies and practices. The study underscores the importance of integrating both technical and human-centered strategies into cybersecurity frameworks, especially in developing country contexts, where the lack of well-established cyber governance and awareness further heightens the threat landscape.

Cybersecurity in Palestinian security institutions, including the customs police, encompasses a range of knowledge and skills aimed at protecting sensitive information and critical infrastructure from cyber threats. These institutions focus on several key areas to ensure their cybersecurity resilience. Understanding the cyber threat landscape involves recognizing common threats such as malware, phishing, ransomware, and advanced persistent threats (APTs), as well as being aware of specific threats targeting governmental and security entities. Additionally, knowledge of regulatory and legal frameworks is crucial, including local and international cybersecurity laws, and data protection standards. (Al Najjar, Al Shobaki & El Talla, 2022).

Effective cybersecurity requires the development and implementation of robust security policies and governance frameworks. This includes crafting comprehensive cybersecurity policies and overseeing their enforcement through governance frameworks. Risk management is another critical area, involving the identification, assessment, and mitigation of cybersecurity

risks through regular risk assessments and vulnerability analyses. The practical application of cybersecurity skills is vital for incident response and management, where personnel detect, analyze, and respond to cybersecurity incidents. This includes implementing incident response plans and conducting post-incident analyses. Network and systems security skills are essential for securing networks, servers, databases, and other critical systems, utilizing firewalls, intrusion detection/prevention systems (IDS/IPS), and anti-malware solutions. (Otieno, 2020)

Encryption and cryptography play a key role in protecting data in transit and at rest, with the implementation of cryptographic protocols to secure communications and transactions. Access control and identity management involve managing user identities and access privileges, including multi-factor authentication (MFA) and single sign-on (SSO) solutions. Security awareness and training programs are conducted to educate staff on recognizing and responding to cyber threats, fostering a culture of cybersecurity awareness within the institution. Regular penetration testing and vulnerability assessments are performed to identify and remediate security weaknesses proactively. (Borky and Bradley, 2019)

Cyber-threat actors pose a significant threat to organizations, disrupting infrastructures, denying access to IT services, and stealing sensitive information. Research emphasizes situation awareness as critical for effective response. (Mohammed & etc., 2022)

Dawson and Thomson (2018) argue that while technical skills are essential in cybersecurity, they are no longer sufficient on their own. The future cybersecurity workforce must also possess non-technical competencies such as communication, teamwork, adaptability, ethical responsibility, and continuous learning. The authors emphasize the importance of integrating psychological and organizational factors like person-organization fit and personality traits into recruitment and training strategies. They propose a more holistic approach to workforce development that balances technical proficiency with human and social capabilities, ultimately enhancing cyber performance and resilience in complex, evolving environments.

Parsons et al. (2022) investigates how employees' awareness of general cybersecurity practices and specific organizational policies influences their cybersecurity behaviours. Through a survey of employees across various industries, the study finds that higher levels of

cybersecurity awareness are associated with more proactive and secure behaviours. Additionally, understanding specific organizational policies further enhances compliance and reduces risky actions. The authors recommend that organizations invest in comprehensive cybersecurity training programs and ensure that policies are clearly communicated and accessible to all employees.

Delso-Vicente et al. (2025) explores the behavioural and technological factors that influence employee compliance with information security policies (ISPs). Unlike earlier studies that focused primarily on technical defences, this research integrates behavioural theories such as the Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT) to understand how individual attitudes, awareness, and organizational culture affect compliance behaviour. Drawing from over 1,000 high-quality studies (2001–2023), the findings highlight that information security awareness (ISA), management support, and perceived policy effectiveness are pivotal for fostering secure behaviour. The study also underscores the importance of addressing the "knowing–doing gap," where awareness does not always translate into action. It concludes that a mix of intrinsic motivators (e.g., responsibility, self-efficacy) and extrinsic controls (e.g., sanctions, training, monitoring) are essential to strengthen cybersecurity culture in organizations.

El-Bably (2021) examines the critical role of human error in cybersecurity breaches and how organizations can mitigate these risks by implementing controls based on the ISO/IEC 27001 Information Security Management standard. The study underscores that while technological solutions are essential, the human element remains the weakest link in the cybersecurity chain, contributing significantly to incidents such as phishing attacks, misconfigurations, and data leaks. Findings from global reports show that distraction, fatigue, lack of training, and password reuse are leading causes of breaches, with internal actors whether through negligence or malicious intent posing a greater threat than external attackers. El-Bably (2021) proposes a set of practical strategies to strengthen institutional cybersecurity, including limiting access based on the principle of least privilege, routine employee awareness programs, monitoring physical access to sensitive systems, and enforcing strict data handling protocols. By aligning security practices with ISO/IEC 27001, organizations can establish a culture of accountability and reduce the frequency and impact of human-related security incidents. The paper highlights

the urgent need for organizations to move beyond technical defences and address behavioural and procedural vulnerabilities as a core part of their cybersecurity governance.

The conceptual framework titled "Three Pillars of Cybersecurity," as mentioned in (Rahman, Rohan, Pal & Kanthamanon, 2021) illustrating the interconnected relationships between three primary components: User, System, and Usability. Each component is represented by a circle, connected to the central triangular pillar, indicating their foundational role in cybersecurity. The User component is influenced by behavioral aspects, demographics, culture, and psychological factors, highlighting the importance of understanding the human element in cybersecurity practices. The System component encompasses technical aspects, functional aspects, legal aspects, and socio-technical aspects, emphasizing the multifaceted nature of system security. Usability is linked to user experience, scale development, and non-functional aspects, underscoring the need for systems to be both secure and user-friendly. The green arrows suggest a positive or supportive interaction between these components, while the red arrows may indicate areas requiring caution or balance. This framework underscores the comprehensive approach needed to address cybersecurity, integrating human factors, system robustness, and ease of use.

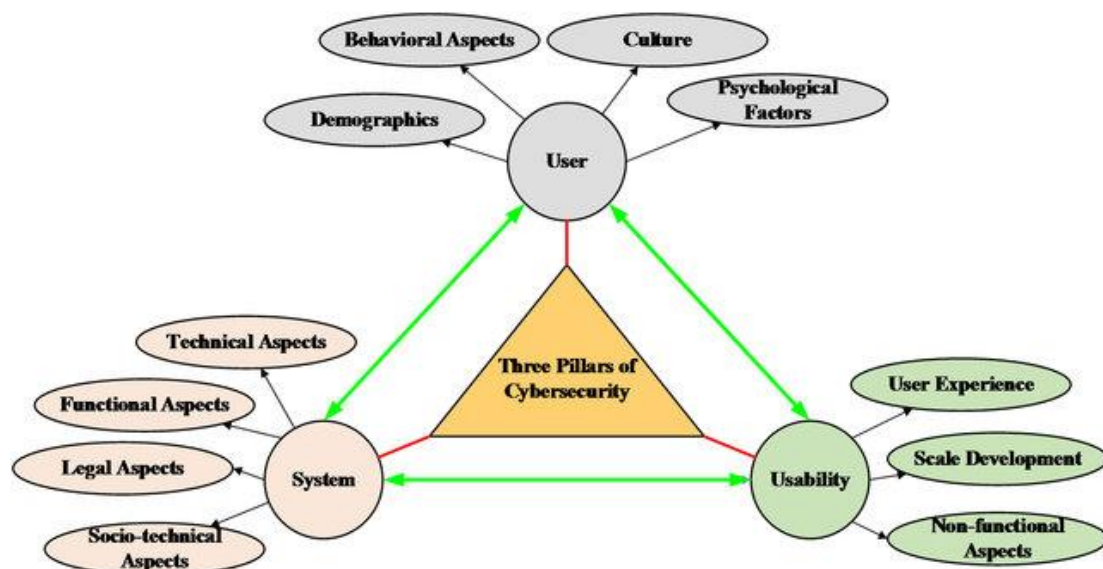


Figure 32: Three Pillars of Cybersecurity Adapted from (Palestinian Customs Police, 2023).

Ganin et al. (2020) propose a comprehensive Multicriteria Decision Analysis (MCDA) framework tailored for cybersecurity risk assessment and management. This framework

evaluates threats, vulnerabilities, and potential consequences through a structured set of criteria, aiming to provide a holistic assessment of cybersecurity risks. By integrating both quantitative and qualitative factors, the MCDA framework facilitates informed decision-making, enabling organizations to prioritize security measures effectively. The authors demonstrate the framework's applicability through case studies, highlighting its utility in real-world cybersecurity scenarios. This approach underscores the importance of a systematic and multidimensional evaluation in enhancing organizational resilience against cyber threats.

Sánchez-García et al. (2023) conducted a systematic mapping review (SMR) to explore tools that automate the cybersecurity risk assessment process. Their study reviewed 40 primary sources, identifying 35 distinct tools and classifying them by scope, methodology (qualitative vs. quantitative), and alignment with international standards like ISO/IEC 27000 and NIST. The authors highlighted that many tools lack comprehensive coverage of all sub-stages of risk assessment particularly risk evaluation and often fail to integrate key variables needed for accurate risk measurement. To address these gaps, the authors proposed a new integrated model that incorporates both qualitative and quantitative components and validated it with cybersecurity experts. Their findings underscore the need for standardized and holistic risk assessment tools tailored to organizational needs, particularly as automation becomes more central in cybersecurity operations.

Mizrak (2023) presents a comprehensive review exploring how cybersecurity risk management (CSRM) is increasingly integrated into strategic management frameworks within modern organizations. The study highlights a paradigm shift, wherein cybersecurity is no longer treated as a purely technical issue but as a core component of organizational resilience and strategic decision-making. The review emphasizes the significance of aligning CSRM with broader business objectives, particularly in the face of rapidly evolving cyber threats that can disrupt operations, damage reputations, and compromise competitive advantage. The author synthesizes methodologies such as vulnerability assessments, penetration testing, scenario analysis, and risk frameworks (e.g., NIST, ISO 27001), and discusses the need for proactive risk prioritization and cross-functional collaboration. Real-world cases like Amazon, JPMorgan Chase, and Google illustrate how major organizations align cybersecurity efforts with strategic goals to enhance operational continuity and digital trust. Ultimately, the article

underscores the importance of embedding CSRM into organizational culture to support long-term resilience and sustainable growth.

Kalinin, Krundyshev, and Zegzhda (2021) examine the cybersecurity risks associated with smart city infrastructures, focusing on the dynamic nature of interconnected systems such as IoT, IIoT, VANET, and WSN networks. The study highlights the vulnerability of these self-organizing networks to various cyberattacks, including DoS, DDoS, sinkhole, black hole, and Sybil attacks, which threaten the availability, integrity, and confidentiality of critical digital services. Traditional risk assessment methods qualitative, quantitative, and hybrid are found to be limited in adaptability and efficiency for smart city environments due to their complexity and rapidly evolving threat landscape. In response, the authors propose a novel neural network-based cybersecurity risk assessment model, which classifies risk levels with high accuracy using simulated smart city datasets. The model demonstrates significant potential in handling large-scale data, identifying hidden patterns, and enabling real-time dynamic risk analysis. This approach is especially valuable in environments with limited human oversight and rapidly changing topologies, such as modern urban digital infrastructures.

Kure et al. (2018) present a comprehensive cybersecurity risk management framework tailored for cyber-physical systems (CPS), which are highly integrated environments combining physical infrastructure with digital control. The article emphasizes that CPS used in critical sectors such as energy, healthcare, and transportation face growing vulnerabilities due to their interdependent and complex structures. Traditional risk management approaches often fail to account for cascading risks across interconnected components and lack adaptability to real-time threats. To address this gap, the authors propose an integrated risk management model that combines qualitative and quantitative assessments. This model includes the identification of critical assets, evaluation of vulnerabilities, modeling of cascading attack scenarios, and assignment of risk levels based on likelihood and impact. They incorporate standards such as ISO 31000, NIST, and NERC CIP, and demonstrate the framework through a case study involving Nigeria's power grid. The study concludes that an integrated, multi-layered approach enhances preparedness against cybersecurity threats in CPS environments by aligning technical, organizational, and operational risk factors.

Parsola (2022) explores the increasing importance of cybersecurity risk assessment and management in modern organizations amid the growing complexity of cyber threats. The article underscores the limitations of traditional security strategies, emphasizing the need for proactive and continuous risk management frameworks that include technical, organizational, and human dimensions. The study reviews key research contributions in cybersecurity, highlighting models such as the NIST Cybersecurity Framework and ISO/IEC 27001, and integrating methods like Bayesian networks and multidisciplinary qualitative and quantitative assessments. One of the core arguments is that effective cybersecurity involves not only technological controls but also strong governance, employee awareness, threat intelligence, and dynamic response mechanisms. Risk mitigation strategies such as access control, encryption, intrusion detection, training, and cyber insurance are discussed as essential components. The article concludes by proposing a comprehensive cybersecurity management framework that encompasses governance, continuous monitoring, third-party risk management, and a strong organizational security culture. This integrated approach is presented as essential to safeguarding data confidentiality, integrity, and availability in today's digital landscape.

Lubua and Pretorius (2019) address the critical need for robust cybersecurity policy frameworks in public sector organizations, particularly in developing countries like Tanzania. The study highlights that many institutions fail to meet international standards such as ISO 27001 due to the lack of formalized, comprehensive cybersecurity policies and clear procedures for policy formulation and review. Through qualitative methods including focus group discussions and structured interviews with IT professionals across 15 public organizations, the authors developed a seven-element policy framework, known as Lubua's Cybersecurity Policy Framework. This framework includes key domains such as data security, internet and network governance, physical security, incident handling, monitoring and compliance, and administrative policy issues. The findings revealed widespread procedural gaps: most organizations either lacked formal policies or had outdated ones with weak top-management endorsement. Additionally, many did not follow structured review cycles, failed to engage stakeholders, or relied on informal guidelines. The study emphasizes that cybersecurity policies must be reviewed at least every three years and must be approved by the organization's top authority to ensure enforceability. Overall, the authors argue for institutionalization of cybersecurity governance through formal policy development, stakeholder participation, and

adherence to international standards principles essential for safeguarding data and ensuring business continuity in the public sector.

Putri et al. (2024) explore cybersecurity risk management practices in ISO 27001-certified organizations to assess how international standards influence information security awareness and operational resilience. The study emphasizes that ISO 27001, as a globally recognized framework for Information Security Management Systems (ISMS), plays a critical role in helping organizations manage cybersecurity threats effectively through structured risk assessment, preventive controls, and continuous improvement mechanisms. The authors highlight that certified organizations demonstrate higher awareness and preparedness in mitigating risks such as malware, phishing, ransomware, and insider threats. The research identifies several key benefits of ISO 27001 implementation, including enhanced corporate reputation, improved operational efficiency, and reduced costs from security incidents. It also compares organizations with and without certification, finding that ISO compliant entities tend to have more defined cybersecurity procedures, stronger response protocols during attacks, and greater alignment with international data protection laws. The study concludes that ISO 27001 not only strengthens internal cybersecurity governance but also improves stakeholder confidence by demonstrating a commitment to protecting sensitive information.

Ramadhanty (2024) presents a comprehensive study on the implementation of the NIST Cybersecurity Framework and ISO/IEC 27001 as dual strategies for managing cybersecurity risks in organizations. The article highlights the increasing severity of cyber threats in Indonesia, including phishing, ransomware, and malware, particularly in sensitive sectors like banking and healthcare. The study emphasizes that many organizations still lack integrated cybersecurity strategies, often due to weak infrastructure and inadequate staff training. The study systematically compares the two frameworks, outlining their five core components: identify, protect, detect, respond, and recover. ISO/IEC 27001 is credited for its focus on information security governance and structured risk management, while NIST is praised for its operational adaptability and detection capabilities. Case studies discussed in the article demonstrate how these frameworks enhance organizational preparedness, especially in incident response and recovery. Ramadhanty (2024) concludes that adopting both standards can significantly strengthen cybersecurity governance, improve awareness among employees, and

enable organizations to proactively manage complex cyber risks. Key recommendations include regular employee training, continuous auditing, and embedding security policies into corporate culture.

Qusef and Alkilani (2022) investigate how the ISO/IEC 27001 standard can enhance the implementation and governance of Open-Source Intelligence (OSINT) in digital forensic investigations. OSINT, which involves gathering publicly available data from online sources for intelligence purposes, is increasingly used in cybersecurity, criminal investigations, and organizational risk assessments. However, the authors highlight that despite its effectiveness, OSINT often lacks standardized integration with formal security practices. To address this, they propose aligning OSINT techniques with ISO/IEC 27001 clauses to improve the reliability, legality, and procedural transparency of data collection and analysis. The study reveals that ISO/IEC 27001 provides a structured framework for managing sensitive data and information systems, enhancing privacy, authenticity, and accessibility. They argue that combining OSINT with ISO 27001 improves data governance, strengthens digital evidence procedures, and supports compliance with international privacy regulations. The authors also emphasize the growing need for digital forensic investigators to incorporate social media and OSINT tools systematically, especially in complex cybercrime investigations. Their research recommends the development of an integrated OSINT toolkit aligned with ISO standards to support lawful and effective digital forensics.

Renvall (2018) explores the importance of enhancing cybersecurity in small and medium-sized enterprises (SMEs) through the adoption and implementation of the ISO/IEC 27001 standard. The thesis emphasizes that as digitalization accelerates and cyber threats become increasingly sophisticated, SMEs despite their limited resources must adopt systematic approaches to information security. The study outlines the core components of ISO/IEC 27001, including the Information Security Management System (ISMS), risk assessment, and the CIA triad (confidentiality, integrity, availability). Renvall presents a detailed overview of current cyber threats such as phishing, ransomware, social engineering, and denial-of-service attacks, and argues that these risks are not limited to large corporations but are equally relevant to SMEs. The thesis highlights that implementing ISO/IEC 27001 offers SMEs a structured path to assess risks, define security policies, and build a culture of cybersecurity awareness. Furthermore, the

research points out the challenges SMEs face without a formal security framework, including higher vulnerability to data breaches and operational disruptions. Certification to ISO/IEC 27001 is not only seen as a technical necessity but also a strategic asset that enhances trust and market credibility.

Folorunso et al. (2024) investigate how ISO/IEC security standards, particularly ISO/IEC 27001, contribute to strengthening cybersecurity posture in organizations across various sectors. The study emphasizes that with the rising complexity of cyber threats such as ransomware, phishing, and insider attacks there is a growing need for structured, internationally recognized frameworks to guide organizations in protecting their digital infrastructure. The ISO/IEC 27000 family of standards offers such a framework, with ISO/IEC 27001 providing a comprehensive system for implementing and maintaining an Information Security Management System (ISMS). Folorunso et al. (2024) outlines how ISO standards improve cybersecurity by fostering risk-based thinking, encouraging management involvement, enhancing incident response, and promoting a security-first organizational culture. The standards also align with regulatory requirements such as GDPR and HIPAA, ensuring legal compliance and stakeholder trust. Through real-world case studies in finance, healthcare, and cloud technology, the authors demonstrate how ISO implementation significantly reduces data breaches and improves organizational resilience. Despite these advantages, the paper also discusses challenges in adopting ISO standards, especially for small and medium-sized enterprises (SMEs). These challenges include high costs, resource limitations, resistance to change, and the ongoing need for updates. However, the authors argue that the long-term benefits of ISO compliance such as improved risk management, greater operational efficiency, and competitive advantage outweigh the difficulties. The study concludes by emphasizing the evolving role of ISO standards in addressing emerging threats from AI, IoT, and blockchain technologies, underscoring the importance of global collaboration and continual adaptation.

2.5 Conclusion

This literature review has provided an in-depth exploration of the critical role that cybersecurity knowledge, skills, and frameworks particularly the ISO/IEC 27001 standard play in enhancing the operational security and institutional capacity of law enforcement bodies, with a special focus on the Palestinian Customs Police (PCP). The review traced the historical development,

current functions, and strategic vision of the PCP, emphasizing its shift toward digital transformation, risk management, and international cooperation as outlined in its 2023–2028 strategy.

The ISO/IEC 27001 framework emerged throughout the reviewed literature as a cornerstone of effective cybersecurity governance. Studies demonstrated its value in providing structured approaches to managing information security risks, ensuring regulatory compliance, improving stakeholder trust, and aligning cybersecurity practices with broader organizational objectives. ISO 27001 emphasis on continuous improvement, risk-based thinking, and multi layered controls was found to be applicable not only to large corporations but also to small and medium-sized institutions like the PCP, especially as cyber threats become more complex and frequent.

Moreover, the review highlighted that technical defenses alone are insufficient; cybersecurity effectiveness is deeply influenced by human factors such as employee awareness, institutional culture, leadership involvement, and compliance behavior. Research consistently underscored the need for a holistic cybersecurity strategy one that integrates policy frameworks, workforce development, behaviorally informed training, and continuous evaluation. Models such as the Multicriteria Decision Analysis (MCDA) framework and human-centered approaches like the "Three Pillars of Cybersecurity" further reinforced the importance of bridging the gap between technology, policy, and human factors.

In conclusion, while the Palestinian Customs Police have made significant strides in aligning with modern cybersecurity standards, this review reveals the necessity of further capacity building, training, and standardized governance practices. (Calder & Watkins, 2019) Adopting and internalizing global best practices like ISO/IEC 27001 will not only mitigate operational risks but also strengthen institutional resilience, contributing to national security and sustainable digital governance in Palestine.

Chapter 3: Methodology

3.1 Introduction

The previous chapter explained in details a theoretical bases of the knowledge and skills that are being applied in Palestinian security institutions (a case study: customs police). While, this chapter shows a detailed discussion about the research process design that used to answer the research questions which has been clarified previously in chapter one. This chapter will illustrate the research method, instruments applied, internal validity and reliability, population, sample, data collection and analysis procedures.

3.2 Study Design

The researcher employs a quantitative research design, utilizing **survey** to collect data from personnel within the Palestinian Customs Police (PCP). This approach is well-suited to objectively measure the level of knowledge and skills being applied, assess patterns, and identify gaps across specific domains such as information security, risk management, and institutional competence. The use of statistical analysis will allow for precise interpretation of the findings and support data-driven conclusions and recommendations.

3.3 Population

The study targets representatives from officer, and non-commissioned officer. This diverse study population ensures a comprehensive range of perspectives on Cybersecurity Knowledge and Skills Applied in the Palestinian Customs Police: A Case Study. The population of this study consists of 150 customs police staff in the Northern governorates.

3.4 Sampling

A survey was employed to select individuals directly involved, specifically targeting members of officers, and non-commissioned officers in customs police in the Northern governorates of Palestine. Due to the population size, the researcher distributed (150) questionnaires on the targeted population, the researcher retrieved (146) questionnaires about (97%) of the population size, valid for statistical analysis.

3.5 Instrument of study and validation indicators

Study Instruments: An online cross-sectional questionnaire was employed as the primary study instrument, encompassing both closed questions. These questions were centred around nine dimensions providing a structured yet flexible framework for respondents to share their

insights about the knowledge and skills that are being applied in Palestinian security institutions among customs police officers and non-commissioned officers. The questionnaire was designed as a Google Form, chosen for its user-friendly interface, accessibility, and ease of distribution and response collection. This platform facilitated efficient primary data collection while accommodating the diverse technological proficiencies of respondents. To accommodate our diverse respondent base and ensure the utmost clarity in communication, the questionnaire was distributed in Arabic, the mother tongue of the participants. This decision not only respects the linguistic preferences of the respondents but also enhances the accuracy of the data collected by mitigating potential language barriers. The questionnaire has to be designed in a way that it can precisely measure the dependent and independent variables in this research.

Likert scale allows the respondent to choose the degree of agree or disagree with each item, when it comes to the stimulus purpose, the different items were measured on 5- point Likert scale to check the participant's degree of convenient with the statement or not, as below: We will use the following scale to assess the level to assess the knowledge and skills that are being applied in Palestinian security institutions among officers, and non-commissioned officers in customs police in the Northern governorates of Palestine, this scale depends on interval length=range/number of intervals, interval length= $(5-1)/3=1.33$. The following scale represents the result: 1- less than 2.33 is low, (less than 46.4%); 2.33- less than 3.66 between (46.4% and less than 73.2%) is medium and 3.66-5 (73.2% and more) is high.

3.6 Ethical approval

Ethical considerations will be paramount throughout the research process. This includes obtaining informed consent from all participants, ensuring confidentiality and anonymity, and minimizing any potential harm or discomfort. The research will adhere to the ethical guidelines set forth by relevant institutions and professional bodies.

- the soft copy of electronic questionnaire was distributed among officers, and non-commissioned officers in customs police in the Northern governorates of Palestine.
- Completed questionnaires were collected electronically.
- The data was collected, and treated as (SPSS, 28), for statistical analysis.

3.7 Tool Validity

3.7.1 Virtual Validity

Validity is “the accuracy of an assessment” in another word it means, does the used instruments measure what supposed to measure? to have the confidence about the validity of the questionnaire before distribute it to the last respondent (Oluwatayo, 2012), content validity of the instrument ensured through valid previous studies. The data collection tool translated to Arabic language, and then content validity reviewed by experts in the field from Palestinian Universities to ensure that it is highly valid.

3.7.2 Exploratory Data Analysis (Construct Validity)

Exploratory data analysis is the set of steps that quantitative researcher follows in exploring a new area of social or psychological life, which researcher did by collecting ended questions to generate new concepts and generalizations about that area. The most efficacious exploratory data analysis leaves these investigators as much scope as possible for the discovery of new concepts and generalizations.

In order to examine the construct validity, the tool applied to an exploratory sample of (15) questionnaires distributed among officers, and non-commissioned officers in customs police in the Northern governorates of Palestine. It was distributed among participants from the study population and returned back to population due the small size. The purpose of the exploratory sample to make the questionnaire achieve the greatest degree of accuracy, and to identify the extent to which the respondents understand the paragraphs of the questionnaire, and detect any problems that appear during the conduct of the study, also, to examine the possibility of its application to obtain information related to the validity of the tool, through the exploratory sample, a Pearson correlation coefficient of the items and the total score of the related dimension was calculated, it was compared with the standard approved for accepting the item according to what was stated in (Garcia, 2011) if greater than (.40), the items are statistically acceptable, in order to confirm the consistency of the items. Table (3-1) shows the result.

Table 3-1: Pearson correlation coefficient between the items and the total score of the related to aspects

Implementation and Compliance Information Policies		Roles and Responsibilities and with Security		Asset and Management (Equipment) and Inventory	
item	Pearson correlation	Item	Pearson correlation	item	Pearson correlation
1	0.74**	30	0.82**	52	0.84**
2	0.52**	31	0.88**	53	0.80**
3	0.68**	32	0.89**	54	0.89**
4	0.79**	33	0.71**	55	0.87**
5	0.77**	34	0.74**	56	0.88**
6	0.89**	35	0.77**	57	0.77**
7	0.71**	Total score=0.88**		58	0.92**
8	0.74**	Employee Competence		59	0.87**
9	0.89**	36	0.88**	60	0.88**
10	0.71**	37	0.82**	61	0.82**
Total score=0.81**		38	0.75**	62	0.77**
Risk Management and Assessment		39	0.77**	63	0.89**
11	0.89**	40	0.80**	Total score=0.91**	
12	0.71**	41	0.68**	Information Access	
13	0.68**	Total score=0.85**		64	0.89**
14	0.79**	Confidentiality and Information Protection		65	0.71**
15	0.89**	42	0.89**	66	0.74**
16	0.74**	43	0.71**	67	0.89**
17	0.89**	44	0.74**	68	0.71**
18	0.71**	45	0.89**	69	0.79**
Total score=0.90**		46	0.71**	Total score=0.89**	
Risk Management and Incident Response		47	0.71**	Physical Access Controls	
19	0.71**	48	0.68**	70	0.80**
20	0.74**	49	0.79**	71	0.89**
21	0.77**	50	0.77**	72	0.74**
22	0.80**	51	0.71**	73	0.85**
23	0.87**	Total score=0.90**		Total score=0.88**	
24	0.88**				
25	0.82**				
26	0.77**				
27	0.89**				
28	0.71**				
29	0.74**				
Total score=0.90**					

** Statistically significant (p<0.01)

It is noted from table (3.1) that the values of Pearson correlation coefficients ranged between (0.52-0.92). according to Garcia and Gonzalez (2006), these values are considered acceptable and statistically significant.

3.8 Reliability

To find out the reliability degree of the questionnaire, the reliability coefficient (Cronbach alpha) is calculated as an indicator of the homogeneity to the level of the instrument. An accepted level would be more than (70%) (Fraenkel & Wallen, 2003). Table (3.2) summarizes the Cronbach's alpha values of the exploratory sample.

Table 3-2: Cronbach's Alpha values for the exploratory sample among employees distributed by aspects

Aspect	Number of items	Cronbach's Alpha
Implementation and compliance with information security policies	10	0.92
Risk management and assessment	8	0.85
Risk management and incident response	11	0.91
Roles and responsibilities	6	0.86
Employee competence	6	0.92
Confidentiality and information protection	10	0.91
Asset and inventory management (equipment)	12	0.93
Information access	6	0.73
Physical access controls	4	0.87
The tool	73	0.98

Table (3.2) shows that Cronbach's Alpha for all aspects ranged between (0.73-0.93) and more than 0.70, the reliability for the whole instrument equals 0.98, which means the consistency of assessment, all items of the instrument measure the same construct, if we distribute the instrument again among the sample after a period of time exceed 4 weeks.

3.9 Statistical analysis

Data from the questionnaires will be analysed using descriptive and inferential statistics (SPSS, 28). Descriptive statistics will summarize the data (e.g., frequencies, percentages, means), while inferential statistics (e.g., T-tests, ANOVA) will be used to test hypotheses and identify significant relationships between variables. SPSS will be used for statistical analysis.

3.10 Conclusion

This chapter has identified the methodological approach selected for this thesis study. The researcher identified the research instrument that applied to test the hypothesis to reach the final results which explore the complex issue of knowledge and skills application within the Palestinian Customs Police (PCP). The internal validity and reliability of the questionnaire were used to make the necessary modifications on the instrument. Moreover, the researcher identified the population, the targeted research sample and explained the procedures used to conduct the data collection and analysis.

Chapter 4: Results and Data Analysis

4.1 Introduction

The overall purpose of this research is to explore the complex issue of knowledge and skills application within the Palestinian Customs Police (PCP), and to examine the significant mean differences among officers and non-commission officers of Customs Police (PCP), according to hypothesis. The researcher presents analysis using (SPSS, 28) to answer the questions and reject or fail to reject the hypothesis. This chapter is divided into three parts: demographic analysis, descriptive analysis, and testing hypothesis respectively.

4.2 Socio-Demographic Analysis

Table 4-1: Socio-Demographic characteristics among officers and non-commission officers of Customs Police (PCP) (n=150)

Variable	Level	Count	Percentage
Gender	Male	134	92%
	Female	12	8%
Age	Between 20 and less than 30 years	36	25%
	Between 30 and less than 40 years	78	53%
	40 years and more	32	22%
Service experience	Less than 5 years	11	8%
	Between 5 and less than 10 years	32	22%
	Between 10 and less than 15 years	44	30%
	15 years or more	59	40%
Qualification level	Diploma or less	34	23%
	Bachelor's Degree	100	68%
	Master's Degree or higher	12	8%
Job title	Customs Officer	131	90%
	Non-commissioned Officer	15	10%
Division you work in	Central operations	19	13%
	Administrative affairs	24	16%
	Sub-Governorates	89	61%
	Information technology	14	10%

Table (4.1) shows the following:

- Gender: the highest percentage (92%) related to males' respondents, (8%) females.

Age: the highest age period related to between 30 and less than 40 years with (53%), while the lowest related to the age period between (40 years and more) with (22%).

- Service experience: 15 years or more has the highest percentage of the sample size with (40%), while less than 5 years is the lowest with (8%).

- Qualification level: the education level for the sample was distributed as (68%) related to bachelor's degree, (8%) master's degree or higher.

- Job title: The highest percentage equals (90%) related to Customs Officer, while the lowest (10%) related to non-commissioned officer.
- Division you work in: the highest percentage is (61%) related to sub-governorates, the lowest percentage (10%) related to information technology.

4.3 Descriptive Statistics:

The descriptive analysis part describes the gathered numerical data. Its results show the mean, percentage and standard deviation for each statement to determine the items that has the highest and lowest mean in each aspect. The purpose of this analysis to identify the central tendency of the responses through mean results and the spread of a set of observations through the standard deviation results which means, when the standard deviation is low, it expressed most of the respondents has the same opinion (concentrated) toward the same statement, on the other hand, if the score of the standard deviation is high it means that the respondents has a different opinion toward the same statement (Cicenaite, et al. 2012).

First question: what is the level of knowledge and skills that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means percentages and standard deviations are calculated to find the level of knowledge and skills that are being applied in Palestinian security institutions (a case study (PCP)).

Table 4-2: Descriptive statistics of the level of knowledge and skills that are being applied in Palestinian security institutions (a case study (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
Implementation and compliance with information security policies	4.08	0.60	81.6	High
Risk management and assessment	4.05	0.53	81.0	High
Risk management and incident response	4.01	0.62	80.2	High
Roles and responsibilities	4.00	0.66	79.9	High
Employee competence	4.07	0.70	81.4	High
Confidentiality and information protection	4.14	0.61	82.7	High
Asset and inventory management (equipment)	4.18	0.56	83.6	High
Information access	3.81	0.67	76.2	High

Physical access controls	4.10	0.67	82.0	High
Total average	4.06	0.52	81.2	High

According to table (4.2) it is clear that the total average of the level of knowledge and skills that are being applied in Palestinian security institutions (a case study (PCP)) represents the high level with (4.06, 81.2%), the statements mean located between (3.81, 76.2%) related to **information access** with a high level and (4.18) related to "**asset and inventory management (equipment)**" with a high level.

Sub-Questions

Question1: What is the level of implementation and compliance with information security policies that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the implementation and compliance with information security policies that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

Table 4-3: Descriptive statistics of implementation and compliance with information security policies that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
To guarantee compliance, the Cabinet's decision about information security management is conveyed in a transparent and thorough manner	4.22	0.74	84.4	High
The service offers a comprehensive breakdown of the steps involved in carrying out the Cabinet's information security management decision	4.16	0.72	83.2	High
The service is committed to fully implementing the Cabinet's decision on managing information security	4.15	0.70	83.0	High
The service ensures compliance with cybersecurity instructions in all its activities	4.29	0.63	85.8	High

Through workshops and training sessions, the service educates staff members on its information security rules	3.94	0.97	78.8	High
The security service has the necessary infrastructure to ensure cybersecurity and effectively implement information security policies	4.00	0.82	80.0	High
The security service has adequate human resources to ensure cybersecurity and effectively implement information security policies	3.95	0.89	79.0	High
The security service provides the required technologies to ensure cybersecurity and effectively implement information security policies	4.01	0.78	80.2	High
Effective monitoring mechanisms are in place by relevant authorities to ensure compliance with the Cabinet's decision on managing information security	3.99	0.85	79.8	High
Monitoring authorities promptly take corrective actions to ensure the protection of information	3.99	0.78	79.8	High
Total average	4.07	0.60	81.4	High

According to table (4.3) it is clear that the total average of implementation and compliance with information security policies that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.07, 81.4%), the statements mean located between (3.94, 78.8%) related to "through workshops and training sessions, the service educates staff members on its information security rules" with a high level and (4.29, 85.8%) related to "the service ensures compliance with cybersecurity instructions in all its activities" with a high level.

Question 2: What is the level of risk management and assessment in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the risk management and assessment in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

Table 4-4: Descriptive statistics of risk management and assessment in Palestinian security institutions (a case study Palestinian Customs Police (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
Non-compliance with security instructions places the institution in an unstable position	4.40	0.67	88.0	High
The efficiency of the regulations in place can be seen by the low risks that arise from ignoring cybersecurity instructions	3.79	0.96	75.8	High
The service has clear and systematic procedures for identifying potential risks	3.94	0.82	78.8	High
Staff are skilled and capable of distinguishing between threats and potential risks, enhancing their response effectiveness	3.99	0.76	79.8	High
Relevant authorities regularly analyse threats and risks to ensure safety and security	4.03	0.74	80.6	High
Authorities can analyse the potential consequences resulting from emerging threats and risks	4.01	0.71	80.2	High
Any suspicions regarding threats or risks are reported to the appropriate authorities within the service	4.12	0.76	82.4	High
Reports related to threats and risks are addressed immediately to identify and effectively resolve them	4.15	0.69	83.0	High
Total average	4.05	0.53	81.0	High

According to table (4.4), it is clear that the total average of risk management and assessment in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.05, 81.0%), the statements mean located between (3.79, 75.8%) related to "The efficiency of the regulations in place can be seen by the low risks that arise from ignoring cybersecurity instructions" with a high level and (4.40, 88.0%) related to "non-compliance with information security instructions places the institution in an unstable position" with a high level.

Question 3: What is the level of risk management and incident response in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the risk management and incident response in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

Table 4-5: Descriptive statistics of risk management and incident response in Palestinian security institutions (a case study Palestinian Customs Police (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
The service has a comprehensive plan for addressing information security risks, based on risk assessments and data recovery in disaster scenarios	3.88	0.90	77.6	High
To guarantee that the measures taken are effective, officers take part in creating the plan to address risks	3.93	0.86	78.6	High
Officers are informed about the results of risk management to ensure transparency and accountability	3.86	0.91	77.2	High
Officers are provided with information related to the threats and risks facing the institution	3.86	0.89	77.2	High
Officers are required to report any event related to information systems, such as virus attacks, data breaches, denial of service, or other risks	4.35	0.72	87.0	High

Officers are informed when the effect of a potential risk or threat has ended to ensure clarity of the security situation	4.09	0.87	81.8	High
The service has written procedures for handling information security incidents to ensure effective response	4.03	0.84	80.6	High
The service documents all incidents and vulnerabilities to ensure effective response	4.05	0.73	81.0	High
The service employs an information security professional to guarantee ongoing security measure monitoring	4.12	0.89	82.4	High
The service relies on external information security experts when necessary to strengthen protection	3.71	1.06	74.2	High
The service keeps backup copies of data to ensure recovery in emergency situations	4.23	0.76	84.6	High
Total average	4.01	0.62	80.2	High

According to table (4.5), it is clear that the total average of risk management and incident response in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.01, 80.2%), the mean of statements located between (3.71, 74.2%) related to "The service relies on external information security experts when necessary to strengthen protection" with a high level and (4.35, 87.0%) related to "Officers are required to report any event related to information systems, such as virus attacks, data breaches, denial of service, or other risks" with a high level.

Question4: What is the level of roles and responsibilities that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the roles and responsibilities that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

Table 4-6: Descriptive statistics of roles and responsibilities that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
The service is committed to outlining the duties associated with information security	4.12	0.69	82.4	High
A sufficient number of personnel is available to effectively handle information security issues	3.73	0.94	74.6	High
The person responsible for information security can be easily accessed at any time	4.11	0.87	82.2	High
The information security specialist is committed to reacting promptly to possible dangers and threats	4.01	0.97	80.2	High
Information security specialists possess high competencies in their fields	3.99	0.85	79.8	High
Regular reviews of roles and responsibilities are conducted to ensure alignment with ongoing developments in information security	4.03	0.80	80.6	High
Total average	4.00	0.66	79.9	High

According to table (4.6), it is clear that the total average of roles and responsibilities that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.00, 79.9%), the mean of statements located between (3.73, 74.6%) related to "A sufficient number of personnel is available to effectively handle information security issues" with a high level and (4.12, 82.4%) related to "the service is committed to outlining the duties associated with information security" with a high level.

Question5: What is the level of employee competence in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the employee competence in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

**Table 4-7: Descriptive statistics of employee competence in Palestinian security institutions
(a case study Palestinian Customs Police (PCP))**

Statement	Mean	Standard Deviation	Percentage %	Level
The service ensures the training and qualification of officers to enhance their competence in information security	4.07	0.91	81.4	High
The service evaluates the competence of officers based on education, training, and practical experience	3.97	0.91	79.4	High
IT department staff possess specialized certifications in cybersecurity	4.05	0.85	81	High
Corrective or remedial actions are taken when necessary to improve employee performance	4.12	0.75	82.4	High
The necessary technical support is provided by specialists when needed to ensure effective implementation of procedures	4.15	0.74	83	High
The service educates employees on best practices for using equipment owned by the security service	4.08	0.81	81.6	High
Total average	4.07	0.70	81.4	High

According to table (4.7) it is clear that the total average of employee competence in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.07, 81.4%), the mean of statements located between (3.97, 79.4%) related to "The service evaluates the competence of officers based on education, training, and practical experience" with a high level and (4.15, 81.0%) related to "The necessary technical support is provided by specialists when needed to ensure effective implementation of procedures" with a high level.

Question6: What is the level of confidentiality and information protection in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the level of confidentiality and information protection in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

Table 4-8: Descriptive statistics of confidentiality and information protection in Palestinian security institutions (a case study Palestinian Customs Police (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
The service requires employees not to disclose any information obtained during their work, even after their service ends	4.23	0.86	84.6	High
The principle of confidentiality is applied to all employees without distinction between positions and authorities	4.10	0.88	82	High
The service has a specific penalty system for violating security policies, ensuring that every employee knows the consequences of their actions.	4.14	0.78	82.8	High
Confidentiality policies are reviewed regularly to ensure compatibility with legal and technological developments	4.03	0.75	80.6	High
The service uses technologies to protect information systems, such as antivirus programs, network security, and intrusion detection systems	4.14	0.78	82.8	High
The service employs licensed firewalls in all governorates and imposes restrictions on the use of removable media (e.g., USB drives, CDs) to protect data	3.97	1.05	79.4	High
Officers are aware of the security risks associated with the misuse of information systems.	4.18	0.87	83.6	High
The institution classifies data and information based on their level of confidentiality	4.16	0.79	83.2	High
Data transfer lines are separated from internet lines	4.12	0.85	82.4	High

to ensure the security and safety of information				
Employees are prohibited from modifying or downloading software on their desktop or portable devices without consulting the IT department	4.09	0.86	81.8	High
Total average	4.34	0.77	86.8	High

According to table (4.8), it is clear that the total average of confidentiality and information protection in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.34, 86.8%), the mean of statements located between (3.97, 79.4%) related to "The service employs licensed firewalls in all governorates and imposes restrictions on the use of removable media (e.g., USB drives, CDs) to protect data" with a high level and (4.18, 83.6%) related to "Officers are aware of the security risks associated with the misuse of information systems" with a high level.

Question7: What is the level of asset and inventory management (equipment) that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the level of asset and inventory management (equipment) that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

Table 4-9: Descriptive statistics of asset and inventory management (equipment) that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
Information security assets (devices) are centrally managed	4.23	0.71	84.6	High
Information security assets (devices) are managed locally within governorates	4.01	0.87	80.2	High
These assets (devices) are updated periodically based on the institution's needs	4.19	0.79	83.8	High
The service has a documented policy for controlling access to	4.15	0.78	83	High

assets (devices), reviewed regularly to ensure effectiveness				
Access policies are reviewed regularly to maintain effectiveness	4.14	0.71	82.8	High
The institution has clear procedures for transferring assets	4.1	0.71	82	High
Data related to individuals responsible for asset transfer is documented to ensure transparency and accountability	4.16	0.75	83.2	High
There is an administrative process for requesting new assets	4.23	0.64	84.6	High
The security service maintains a record for documenting issues occurring with equipment and devices	4.1	0.84	82.0	High
Measures are taken to ensure that repaired devices are not tampered with or manipulated	4.3	0.70	86.0	High
The security service has a specialized maintenance department with sufficient expertise to handle malfunctions and issues	4.34	0.63	86.8	High
Physical access to devices and equipment is restricted to authorized personnel only	4.19	0.73	83.8	High
Total average	4.18	0.56	83.6	High

According to table (4.9), it is clear that the total average of asset and inventory management (equipment) that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.18, 83.6%), the mean of statements located between (4.01, 80.2%) related to "Information security assets (devices) are managed locally within governorates" with a high level and (4.34, 86.8%) related to "The security service has a specialized maintenance department with sufficient expertise to handle malfunctions and issues" with a high level.

Question8: What is the level of information access that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the level of information access that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

Table 4-10: Descriptive statistics of information access that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
In order to protect sensitive data, the security service categorizes the information that users can access according to their work requirements	4.27	0.63	85.4	High
The dangers of revealing or exchanging organizational information with outside parties without the proper authority are well known to officers	3.97	0.99	79.4	High
Visitors are allowed access to the institution's network (Wi-Fi) according to specific regulations	3.41	1.30	68.2	Medium
Officers can access the institutional network remotely via VPN in accordance with approved security policies	3.6	1.18	72	Medium
Service providers or equipment suppliers are permitted external network access via VPN or software such as Any Desk or TeamViewer under controlled conditions	3.53	1.10	70.6	Medium
The use of wired and wireless internet while working is governed by explicit rules to maintain security and compliance with institutional regulations	4.1	0.84	82	High
Total average	3.81	0.67	76.2	High

According to table (4.10), it is clear that the total average of information access that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (3.81, 76.2%), the mean of statements located between (3.41, 68.2%) related to "Visitors are allowed access to the institution's network (Wi-Fi) according to specific regulations" with a medium level and (4.27, 85.4%) related to "In order to protect sensitive data, the security service categorizes the information that users can access according to their work requirements" with a high level.

Question9: What is the level of physical access controls that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

To answer this question, means, percentages and standard deviations are calculated to find the level of physical access controls that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)).

Table 4-11: Descriptive statistics of physical access controls that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))

Statement	Mean	Standard Deviation	Percentage %	Level
The security service has written and published controls to regulate access to high-security areas	4.12	0.82	82.4	High
Entry and exit from high-security areas are documented in a special log	4.03	0.82	80.6	High
The security service confirms each visitor's identity before allowing them entry	4.17	0.71	83.4	Medium
Access permissions are properly and systematically specified and documented for both employees and individuals	4.07	0.80	81.4	Medium
Total average	4.10	0.67	82.0	High

According to table (4.11), it is clear that the total average of physical access controls that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.10, 82.0%), the mean of statements located between (4.03, 80.6%) related to "Entry and exit from high-security areas are documented in a special log" with a high level and (4.17, 83.4%) related to "The security service confirms each visitor's identity before allowing them entry" with a high level.

Chapter 5: Conclusion and Recommendations

5.1 Introduction

The purpose of this study is to investigate the Cybersecurity Knowledge and Skills Applied in the Palestinian Customs Police: A Case Study. This chapter introduces a holistic discussion of the study results and assesses their theoretical and practical implications. It also outlines recommendations, exposes limitations and makes suggestions for future research.

5.2 Discussion of Results

The study findings are interpreted in the light of the literature reviewed in chapter two, alongside the results derived from the primary data analysis presented in chapters three and four. Results of the theoretical and empirical review as discussed comprehensively in chapter two can be summarized in the following highlights:

1. Digital Competencies as a Strategic Imperative

In the evolving landscape of national security, digital competencies have emerged as a strategic necessity, especially for institutions like the Palestinian Customs Police. Theoretically, digital skills encompass a range of abilities including data literacy, cybersecurity awareness, and the use of digital tools for operational efficiency. These competencies are no longer optional but foundational, given the increased reliance on digital communication, surveillance, and coordination systems. Empirical research underlines that the integration of digital competencies allows for enhanced institutional responsiveness and strategic alignment with modern border security practices.

2. Integration of Digital Tools into Daily Operations

Digital technologies are now embedded in the daily routines of Customs Police officers. Theoretical models of digital transformation suggest that effective integration occurs when technology is used not just for data management but as a tool for strategic decision-making. Empirically, field observations within Palestinian Customs Police reveal the use of electronic tracking systems, digital inspection checklists, and mobile apps for real-time data collection. This integration reduces manual errors, speeds up customs procedures, and allows for accurate threat assessments at border points.

3. Cybersecurity Awareness and Institutional Preparedness

As digital systems become central to security operations, vulnerabilities to cyber threats also increase. Theoretically, cybersecurity readiness involves both technical defence mechanisms and human vigilance. In practice, the Palestinian Customs Police have begun adopting cybersecurity protocols, including the encryption of sensitive data, secure communication platforms, and threat detection systems. Empirical evaluations show that while technical infrastructure is gradually improving, continued investment in awareness campaigns and simulation-based training is crucial to maintain institutional resilience against cyberattacks.

4. The Role of Education and Continuous Digital Training

The theoretical literature supports the idea that digital skills are best developed through sustained education and hands-on training. The Customs Police in Palestine have initiated digital literacy programs as part of their professional development framework. Empirical findings highlight that workshops, certification courses, and e-learning modules contribute significantly to skill acquisition, especially in areas like database management, digital forensics, and network security. These initiatives are critical in ensuring that personnel remain competent and updated on the latest technological advancements.

5. Institutional Policies Supporting Digital Transformation

The successful application of digital competencies is also shaped by the presence of supportive institutional policies. Theoretically, digital transformation in security agencies is guided by governance frameworks that prioritize innovation, security, and accountability. In the Palestinian context, the Ministry of Interior and related bodies have developed digital governance strategies aimed at standardizing procedures, securing digital infrastructure, and promoting interoperability across departments. Empirical reviews indicate that where policies are clear and well-implemented, there is a measurable improvement in the quality and consistency of digital operations.

6. Measuring the Impact of Digital Competencies on Security Performance

Finally, the theoretical approach to performance measurement in digital security emphasizes both quantitative and qualitative metrics. Empirically, internal assessments within the Palestinian Customs Police have tracked improvements in operational speed, accuracy of customs processing, and responsiveness to threats post-digitization. Moreover, digital reporting tools now allow for better tracking of smuggling attempts, resource allocation, and inter-agency communication. These indicators confirm that digital competencies, when effectively taught

and applied, contribute meaningfully to the broader goals of security, efficiency, and institutional integrity. The study also introduced results of the primary data analysis. These results and their implications are discussed hereafter.

As the first step was to determine the level of knowledge and skills that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)). The level of knowledge and skills that are being applied in Palestinian security institutions (a case study (PCP)) represents the high level with (4.06, 81.2%), the statements mean located between (3.81, 76.2%) related to information access with a high level and (4.18) related to "asset and inventory management (equipment)" with a high level.

From the researcher's perspective, the high level of knowledge and skills applied in the Palestinian Customs Police (PCP), reflected by an overall mean score of (4.06, 81.2%), indicates a mature and structured institutional environment where professional competencies are well-developed and strategically implemented. Notably, the domain of "information access" achieved a mean of (3.81, 76.2%), which reflects strong capabilities in utilizing digital platforms, retrieving operational data, and ensuring timely flow of information—an essential component in modern security operations. Moreover, the statement regarding "asset and inventory management (equipment)" recorded an even higher mean of (4.18), suggesting that the PCP exhibits robust logistical management and operational control over its physical resources. These results collectively justify the classification of the knowledge and skills level as high, as they demonstrate the institution's effectiveness in aligning staff competencies with operational goals, supported by structured training, digital integration, and effective administrative practices.

The researcher discusses the sub-questions derived from the main first question as indicated below:

Question1: What is the level of implementation and compliance with information security policies that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

The results showed the level of the implementation and compliance with information security policies that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.07, 81.4%), the statements mean located between (3.94, 78.8%) related to "through workshops and training sessions, the service educates staff members on its information security rules" with a high level and (4.29, 85.8%)

related to "the service ensures compliance with cybersecurity instructions in all its activities" with a high level.

From the researcher's point of view, the findings indicating a high level of implementation and compliance with information security policies in the Palestinian Customs Police (PCP), with an overall mean of (4.07, 81.4%), reflect a commendable institutional commitment to cybersecurity and risk management practices. This level suggests that information security is not only prioritized but also embedded in the operational culture of the organization. The relatively high mean score of (3.94, 78.8%) for the statement concerning the use of workshops and training sessions to educate staff on information security rules highlights the proactive efforts made to raise awareness and foster compliance through continuous learning. Meanwhile, the even higher score of (4.29, 85.8%) for the statement related to ensuring compliance with cybersecurity instructions across all activities demonstrates a strong enforcement mechanism and accountability within the institution. Together, these results justify the classification of the overall level as high, showing that the PCP not only develops comprehensive information security policies but also effectively translates them into practice through training, monitoring, and policy enforcement across all functional levels.

Question 2: What is the level of risk management and assessment in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

According to table (4.4) it is clear that the total average of risk management and assessment in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.05, 81.0%), the statements mean located between (3.79, 75.8%) related to "The efficiency of the regulations in place can be seen by the low risks that arise from ignoring cybersecurity instructions" with a high level and (4.40, 88.0%) related to "non-compliance with information security instructions places the institution in an unstable position" with a high level.

From the researcher's perspective, the overall result indicating a high level of **risk management and assessment** in the Palestinian Customs Police (PCP), with a total average of **(4.05, 81.0%)**, reflects a strategic and structured approach to managing security-related risks, especially those associated with information security. The statement with the mean score of **(3.79, 75.8%)**, which emphasizes that *"the efficiency of the regulations in place can be seen by the low risks that arise from ignoring cybersecurity instructions"*, demonstrates that the current regulatory framework is functioning effectively in minimizing vulnerabilities, even if continuous improvement is still needed. Meanwhile, the highest statement mean of **(4.40,**

88.0%), stating that *"non-compliance with information security instructions places the institution in an unstable position"*, strongly underscores a widespread awareness among personnel of the potential consequences of security lapses. This high perception of risk awareness indicates that the institution successfully integrates risk recognition into its daily operations. Collectively, these findings justify the classification of risk management and assessment at a high level, as the institution appears to not only identify and assess risks systematically but also instil a culture of accountability and prevention among its members.

Question 3: What is the level of risk management and incident response in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

The total average of risk management and incident response in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.01, 80.2%), the mean of statements located between (3.71, 74.2%) related to "The service relies on external information security experts when necessary to strengthen protection" with a high level and (4.35, 87.0%) related to "Officers are required to report any event related to information systems, such as virus attacks, data breaches, denial of service, or other risks" with a high level.

From the researcher's perspective, the high total average score of (4.01, 80.2%) in the domain of risk management and incident response reflects the Palestinian Customs Police's (PCP) strong institutional commitment to identifying, addressing, and mitigating cybersecurity threats in a timely and effective manner. The statement with the lower end of the mean range, (3.71, 74.2%), indicating that "the service relies on external information security experts when necessary to strengthen protection", shows a pragmatic recognition of the need to engage specialized expertise when internal resources require reinforcement. This suggests a mature understanding of risk complexity and the value of collaboration in enhancing institutional resilience.

On the other hand, the highest scoring item, (4.35, 87.0%), "officers are required to report any event related to information systems, such as virus attacks, data breaches, denial of service, or other risks", highlights a culture of proactive incident reporting and early threat detection. This indicates a well-established internal protocol and awareness among personnel regarding their responsibilities in safeguarding information systems. The consistency of high scores across both external collaboration and internal response practices validates that the institution not only prepares for potential threats but also reacts to incidents with clarity and accountability. These findings collectively justify the classification of this domain at a high level, demonstrating that

the PCP has embedded both preventative and reactive elements of cybersecurity into its operational fabric.

Question4: What is the level of roles and responsibilities that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

According to table (4.6), it is clear that the total average of roles and responsibilities that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.00, 79.9%), the mean of statements located between (3.73, 74.6%) related to "A sufficient number of personnel is available to effectively handle information security issues" with a high level and (4.12, 82.4%) related to "the service is committed to outlining the duties associated with information security" with a high level.

From the researcher's standpoint, the high total average score of (4.00, 79.9%) in the area of roles and responsibilities clearly reflects the institutional clarity and organizational discipline maintained by the Palestinian Customs Police (PCP) in managing information security. The statement with the highest mean, (4.12, 82.4%), which emphasizes that "the service is committed to outlining the duties associated with information security," indicates a strong organizational framework in which responsibilities are clearly defined and communicated. This alignment ensures that all personnel are aware of their roles, which in turn enhances accountability and consistency in implementing cybersecurity policies.

Additionally, the lowest scoring item in this domain, (3.73, 74.6%), which states that "a sufficient number of personnel is available to effectively handle information security issues," still falls within the high level, suggesting that while staffing may face certain limitations, there is still a relatively adequate human resource base to maintain security functions. This finding may also point to the potential for further investment in specialized personnel to support growing digital needs. Nonetheless, the overall high rating demonstrates that the PCP has established a solid foundation of structured responsibilities, which is essential for managing cybersecurity effectively. The commitment to assigning and enforcing specific duties serves as a critical pillar in fostering a secure digital environment across the institution.

Question5: What is the level of employee competence in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

According to table (4.7), it is clear that the total average of employee competence in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.07, 81.4%), the mean of statements located between (3.97, 79.4%) related to "The

service evaluates the competence of officers based on education, training, and practical experience" with a high level and (4.15, 81.0%) related to "The necessary technical support is provided by specialists when needed to ensure effective implementation of procedures" with a high level.

From the researcher's perspective, the high total average score of (4.07, 81.4%) for employee competence in the Palestinian Customs Police (PCP) strongly reflects the institution's dedication to cultivating a highly skilled and professionally capable workforce. The statement with the highest mean, (4.15, 81.0%), which asserts that "the necessary technical support is provided by specialists when needed to ensure effective implementation of procedures," highlights the organization's proactive approach in equipping its personnel with expert assistance to maintain operational efficiency, especially in critical and technical areas related to information systems and cybersecurity.

Meanwhile, the statement with the lowest mean, (3.97, 79.4%), emphasizing that "the service evaluates the competence of officers based on education, training, and practical experience," still falls well within the high-level range. This indicates that PCP not only values academic and professional qualifications but also systematically assesses and builds upon its officers' competencies through structured evaluation mechanisms.

Overall, the results demonstrate that employee competence is not left to chance but is supported through a comprehensive system that combines formal assessment, ongoing training, and timely technical support. This integrated strategy enhances institutional readiness, promotes continuous professional development, and ensures that employees are well-equipped to perform their roles effectively, particularly in an evolving security environment.

Question6: What is the level of confidentiality and information protection in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

According to table (4.8), it is clear that the total average of confidentiality and information protection in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.34, 86.8%), the mean of statements located between (3.97, 79.4%) related to "The service employs licensed firewalls in all governorates and imposes restrictions on the use of removable media (e.g., USB drives, CDs) to protect data" with a high level and (4.18, 83.6%) related to "Officers are aware of the security risks associated with the misuse of information systems" with a high level.

From the researcher's perspective, the high total average score of 4.34 (86.8%) in confidentiality and information protection within the Palestinian Customs Police (PCP) can be justified by the data presented in table (4.8), which demonstrates that the service's approach to security is robust.

The mean scores for individual statements such as the use of licensed firewalls across all governorates and the restrictions on removable media like USB drives (with a mean of 3.97 or 79.4%)—reflect a proactive and preventive approach to safeguarding data. The implementation of these measures suggests a high level of concern for data integrity and security, minimizing potential risks related to unauthorized access or data breaches.

The score of 4.18 (83.6%) for the awareness of officers regarding security risks associated with misuse of information systems reinforces the importance of knowledge-based security practices. This indicates that officers are well-informed and trained on the implications of poor information security practices, further supporting the overall high level of confidentiality and information protection within the institution.

Together, these findings indicate that the Palestinian Customs Police have established strong security protocols, with both technological tools (e.g., firewalls and media restrictions) and personnel awareness contributing to a comprehensive, high-level approach to confidentiality and data protection.

Question7: What is the level of asset and inventory management (equipment) that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

According to table (4.9), it is clear that the total average of asset and inventory management (equipment) that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.18, 83.6%), the mean of statements located between (4.01, 80.2%) related to "Information security assets (devices) are managed locally within governorates" with a high level and (4.34, 86.8%) related to "The security service has a specialized maintenance department with sufficient expertise to handle malfunctions and issues" with a high level.

From a researcher's perspective, the justification for the high total average score of 4.18 (83.6%) in asset and inventory management within the Palestinian Customs Police (PCP) can be derived from the responses related to specific statements about the management of equipment. The statement regarding the local management of information security assets (e.g.,

devices) with a mean score of 4.01 (80.2%) reflects a structured and localized approach to managing assets within the various governorates. This score indicates that each governorate is actively involved in the management of its own security devices, ensuring that local units have the necessary tools and resources for effective operation and security, which is crucial for decentralized operations. Furthermore, the higher score of 4.34 (86.8%) for the presence of a specialized maintenance department with sufficient expertise underscores the PCP's commitment to maintaining the functionality and reliability of its equipment. This indicates that the organization has implemented a dedicated and skilled team to handle malfunctions and other technical issues, ensuring that the equipment remains operational and efficient, which is essential for maintaining security operations without unnecessary interruptions. These findings justify the overall high score in asset and inventory management, as they demonstrate that both localized management of assets and specialized maintenance procedures are being effectively implemented to enhance the operational readiness of the Palestinian Customs Police. These practices ensure that equipment is well-maintained, properly managed, and ready for use when needed, reflecting a high level of competency in asset and inventory management.

Question 8: What is the level of information access that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

According to table (4.10), it is clear that the total average of information access that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (3.81, 76.2%), the mean of statements located between (3.41, 68.2%) related to "Visitors are allowed access to the institution's network (Wi-Fi) according to specific regulations" with a medium level and (4.27, 85.4%) related to "In order to protect sensitive data, the security service categorizes the information that users can access according to their work requirements" with a high level.

From a researcher's perspective, the justification for the findings in the study, where the total average score of information access in Palestinian security institutions (specifically the Palestinian Customs Police, PCP) is 3.81 (76.2%), can be reflects a balanced and thoughtful approach, indicating that while there is room for improvement, the existing practices are functioning at a relatively high level when it comes to regulating and protecting information access. The statement regarding visitor access to the institution's network (Wi-Fi), with a mean score of 3.41 (68.2%), indicates that while visitors can access the network, this is done under regulated conditions. The medium score suggests that the regulations surrounding visitor access are in place but may not be as stringent or comprehensive as those for internal users.

This could reflect a balance between facilitating external interactions and ensuring that access does not pose a security risk. The medium level points to potential areas for tightening controls or enhancing the guidelines on what visitors can access. The statement about categorizing information access based on work requirements, with a high mean score of 4.27 (85.4%), strongly supports the idea that the PCP is prioritizing security. By categorizing information and ensuring that users can only access the data necessary for their roles, the PCP is safeguarding sensitive information. This reflects a high level of security awareness and a well-structured access control policy that ensures personnel are only able to view or use data pertinent to their duties. Such measures are fundamental to protecting the integrity and confidentiality of sensitive data within security institutions. The overall findings suggest a structured, tiered approach to information access. While general access (such as visitor Wi-Fi) is regulated with moderate restrictions, there is a strong focus on controlling access to sensitive information based on role-specific needs. This ensures that those within the institution can only access the information relevant to their work, while limiting the exposure of sensitive data.

Question9: What is the level of physical access controls that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP))?

According to table (4.11), it is clear that the total average of physical access controls that are being applied in Palestinian security institutions (a case study Palestinian Customs Police (PCP)) represents the high level with (4.10, 82.0%), the mean of statements located between (4.03, 80.6%) related to "Entry and exit from high-security areas are documented in a special log" with a high level and (4.17, 83.4%) related to "The security service confirms each visitor's identity before allowing them entry" with a high level.

From a researcher's perspective, the findings indicating that the total average of physical access controls in Palestinian security institutions, specifically the Palestinian Customs Police (PCP), is at a high level (4.10, 82.0%) reflect a strong institutional commitment to safeguarding its physical infrastructure. This high average suggests that the PCP has implemented comprehensive and effective physical security measures that align with best practices in secure facility management. These measures are essential for controlling access to sensitive areas, protecting personnel and resources, and preventing unauthorized entry that could compromise operations.

The statement "Entry and exit from high-security areas are documented in a special log" received a high mean score of 4.03 (80.6%), which indicates that the PCP maintains proper

monitoring and traceability of movements within critical zones. This documentation practice enhances accountability and ensures that any access to high-risk areas is recorded and can be audited if necessary. It is a key aspect of risk management that supports investigation and response efforts in the event of security breaches or incidents. Meanwhile, the higher score of 4.17 (83.4%) for the statement "The security service confirms each visitor's identity before allowing them entry" reflects a strict adherence to identity verification protocols, which are crucial in preventing unauthorized access and maintaining a secure environment.

Overall, the high ratings across these indicators demonstrate that the PCP has adopted a proactive and structured approach to physical access control. By consistently applying these measures such as maintaining detailed access logs and enforcing visitor identity checks—the institution minimizes vulnerabilities and enhances its operational resilience. These practices not only protect physical assets and sensitive areas but also contribute to the overall security culture within the organization, ensuring that all personnel understand and support the importance of controlled access in maintaining institutional integrity.

3.5 Recommendations

Based on the results of the study, the researcher presents some invaluable recommendations:

1. **Enhance Technical Safeguards:** The Palestinian Customs Police (PCP) should continue upgrading and maintaining licensed firewalls and other security technologies across all governorates to ensure robust protection of confidential information and prevent unauthorized access.
2. **Limit Use of Removable Media:** Further restrictions should be placed on the use of removable media (such as USB drives and CDs) by implementing stricter usage policies and promoting the use of encrypted or centrally monitored alternatives.
3. **Promote Ongoing Training and Awareness:** Regular training programs should be conducted to strengthen officers' awareness of security risks, particularly regarding the misuse of information systems, emerging cyber threats, and best practices in information protection.
4. **Improve Visitor Network Access Controls:** The institution should revise its visitor access policies by enforcing more stringent regulations for temporary access to the internal network (e.g., Wi-Fi) to ensure that it does not compromise system security.

5. Strengthen **Role-Based Access to Information**: The PCP should regularly evaluate and update access permissions to ensure that employees can only access data relevant to their specific job roles, thereby minimizing the risk of internal data breaches.

6. **Upgrade Physical Access Systems**: While current measures are effective, the PCP is advised to adopt modern technologies such as biometric systems and electronic logging tools to further improve the security of high-risk areas and streamline the visitor identification process.

5.6 Future Research

Depending on the findings of the current study, the researcher suggests for future research the following subjects or topics:

1. **Comparative Analysis Across Security Sectors**: Future research could conduct a comparative study between different Palestinian security institutions to identify variations in asset management, information access, and physical security controls, highlighting sector-specific strengths and areas for improvement.
2. **Impact of Digital Transformation**: Investigate the effects of digital transformation and automation on confidentiality and information protection within security institutions, focusing on how new technologies (e.g., AI, cloud storage, digital surveillance) influence data security and operational efficiency.
3. **Evaluation of Training Programs**: Explore the effectiveness of ongoing security awareness and training programs on employees' adherence to information protection policies, and how such programs contribute to reducing security breaches.
4. **Cybersecurity Challenges in Security Institutions**: Study the growing cybersecurity threats facing Palestinian security institutions and assess the readiness and resilience of their current digital infrastructure to detect, prevent, and respond to cyberattacks.
5. **User Experience and Compliance**: Investigate how employees and visitors perceive and interact with physical and digital access control systems, and how user satisfaction or resistance influences overall compliance with security protocols.

References

- صدی نیوز. (2018، 1 يوليو). 450 جريمة إلكترونية مقدمة للشرطة الفلسطينية منذ بداية العام. تم الاسترجاع من <http://www.sadaa.ps/43722.html>
- Abu Al-Rab, N. (2019). Cybercrime in the State of Palestine: Reality and Challenges. The 13th ICT Day Conference (Technology and Law). Ramallah: Al-Quds Open University.
- Adhikari, C. (2017, November 9). Cybersecurity challenges in developing countries. ICT Frame. Retrieved from <https://ictframe.com/cybersecurity-challenges-in-developing-countries/>
- Al Najjar, M., Al Shobaki, M., & El Talla, S. (2022). The extent of cyber security application at the Ministry of Interior and National Security in Palestine. *International Journal of Academic Information Systems Research (IJAIRS)*, 6(5), 46–71.
- Aliyu, J. M. (2022). Development of framework for prevention of cyber attack in an organization [Doctoral dissertation, Selinus University].
- Amro, B. (2018). Cybercrime as a matter of the art in Palestine and its effect on individuals. *International Journal of Wireless and Microwave Technologies (IJWMT)*, 8(5), 19–26. <https://doi.org/10.5815/ijwmt.2018.05.03>
- Borky, M., & Bradley, H. (2019). Protecting information with cybersecurity. In *Effective Model-Based Systems Engineering* (pp. 345–404).

- Brown, R. (2021). ISO 27001 certification and its impact on organizational trust. *International Journal of Information Security*, 15(3), 78–92.
- Calder, A., & Watkins, S. (2019). *IT governance: An international guide to data security and ISO 27001/ISO 27002*. Kogan Page.
- Clark, P. (2022). Supply chain security and ISO 27001: Addressing third-party risks. *Journal of Supply Chain Security*, 8(3), 67–72.
- Cox, L. (2017, August 8). Developing countries: A hotbed for cybercrime. Disruption Hub. Retrieved from <https://disruptionhub.com/developing-countries-hotbed-cybercrime/>
- Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9, 744. <https://doi.org/10.3389/fpsyg.2018.00744>
- Delso-Vicente, A. T., Diaz-Marcos, L., Aguado-Tevar, O., & García de Blanes-Sebastián, M. (2025). Factors influencing employee compliance with information security policies: A systematic literature review. *Future Business Journal*, 11(28). <https://doi.org/10.1186/s43093-025-00452-7>
- El-Bably, A. Y. (2021). Overview of the impact of human error on cybersecurity based on ISO/IEC 27001. *Journal of Information Security & Cybercrimes Research*, 4(1), 95–102. <https://doi.org/10.26735/WLPW6121>
- Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*, 24(1), 2582–2595. <https://doi.org/10.30574/wjarr.2024.24.1.3169>

- Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, 40(1), 183–199. <https://doi.org/10.1111/risa.12891>
- Green, M. (2022). Aligning ISO 27001 with ISO 9001 and ISO 22301. *Integrated Management Systems Review*, 14(2), 33–40.
- Halder, D., & Jaishankar, K. (2012). Definition, typology and patterns of victimization. In I. Management Association (Ed.), *Cyber Crime: Concepts, Methodologies, Tools and Applications* (Vol. 1, pp. 1016–1042). USA: Information Resources Management Association.
- Harris, T. (2023). Emerging technologies and ISO 27001: Adapting to the future. *Future Cybersecurity Trends*, 5(1), 55–60.
- Hinson, G. (2017). *ISO 27001 controls – A guide to implementing and auditing*. IT Governance Publishing.
- International Organization for Standardization. (2013). *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*.
- ISACA. (2021). *Implementing ISO 27001 in financial institutions: A case study*. IT Governance UK. (n.d.). What is ISO 27001? Retrieved from <https://www.itgovernance.co.uk/iso27001>
- Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, 9(4), 78. <https://doi.org/10.3390/machines9040078>

- Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & Security*, 24(3), 246–260.
- Kshetri, N. (2010). Diffusion and effects of cybercrime in developing economies. *Journal of Global Information Technology Management*, 13(2), 1057–1075.
- Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, 8(6), 898. <https://doi.org/10.3390/app8060898>
- Lee, S. (2023). Privacy and ISO 27001: The role of ISO 27701. *Privacy and Data Protection Journal*, 12(1), 88–95.
- Lubua, E. W., & Pretorius, P. D. (2019, July). Cyber-security policy framework and procedural compliance in public organisations. In *Proceedings of the International Conference on Industrial Engineering and Operations Management*, Pilsen, Czech Republic, July 23–26, 2019.
- Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Research Journal of Business and Management (RJBM)*, 10(3), 98–108. <https://doi.org/10.17261/Pressacademia.2023.1807>
- National Institute of Standards and Technology. (2020). NIST cybersecurity framework and ISO 27001: A comparative analysis.
- OECD. (2019). *Governance for Youth, Trust and Intergenerational Justice: Fit for All Generations?* OECD Publishing.
- Otieno, D. (2020). Cyber security challenges: The case of developing countries. In *Promoting Creativity, Innovation and Productivity for Sustainable Development*.

- Otieno, D. O. (2020). Cybersecurity challenges: The case of developing countries. *Proceedings of the International Conference on Information Security and Cyber Threats*, 1(1), 1–12.

- Palestinian Customs Police. (2023). *Network Architecture, Security, and Surveillance Report*. Internal Technical Report.

- Palestinian Customs Police. (2023–2028). الدوائر أهداف [Goals of the Departments]. Internal Strategy Document.

- Parsola, J. (2022). Cybersecurity risk assessment and management for organizational security. *NeuroQuantology*, 20(5), 5330–5337.
<https://doi.org/10.48047/nq.2022.20.5.nq22815>

- Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2022). The role of cybersecurity and policy awareness in shifting employee cybersecurity behavior. *Computers in Human Behavior*, 130, 107–115.
<https://doi.org/10.1016/j.chb.2022.107115>

- Putri, S. R. M., Bernandy, M. P., Aulia, C., Fikri, M. G. R., & Jasmine, J. (2024). Cybersecurity risk management practices: Insights from an ISO 27001 certified organization. *Journal of Digital Business and Innovation Management*, 3(2), 101–113.
<https://doi.org/10.26740/jdbim.v3i2>

- PwC. (2020). The value of ISO 27001 certification in cybersecurity. Retrieved from <https://www.pwc.com>

- Qusef, A., & Alkilani, H. (2022). The effect of ISO/IEC 27001 standard over open-source intelligence. *PeerJ Computer Science*, 8, e810. <https://doi.org/10.7717/peerj-cs.810>

- Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021, June). Human factors in cybersecurity: a scoping review. In *Proceedings of the 12th International Conference on Advances in Information Technology* (pp. 1–11).

- Ramadhanty, N. (2024). Implementasi kerangka keamanan NIST dan ISO/IEC 27001 dalam menghadapi ancaman risiko siber. *Journal of Indonesian Management*, 4(4), 1–9. <https://doi.org/10.53697/jim.v4i4.1973>

- Renvall, A. (2018). Improving cybersecurity through ISO/IEC 27001 information security standard in the context of SMEs (Master's thesis). Helsinki Metropolia University of Applied Sciences. Retrieved from <https://www.theseus.fi/handle/10024/157277>

- Safarini, B. (2017, August 30). Cybercrime: the other face of the digital world. Retrieved October 05, 2020 from <http://www.asdaapress.com/?ID=26387>

- Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2023). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences*, 13(1), 395. <https://doi.org/10.3390/app13010395>

- Smith, J. (2022). The role of ISO 27001 in modern cybersecurity. *Journal of Cybersecurity Research*, 10(1), 22–35.

- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs a holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215–225.

- Tartir, A. (2015). The evolution and reform of Palestinian security forces 1993–2013. Stability: International Journal of Security & Development, 4(1).
<https://doi.org/10.5334/sta.fk>
- Taylor, L. (2020). Resource challenges in ISO 27001 implementation for SMEs. Cybersecurity Today, 7(2), 45–50.
- Wilson, K. (2021). Critiquing ISO 27001: A focus on practical security. Security and Privacy Journal, 9(4), 12–18.

Appendix A: Survey

Al-Quds Open University
Faculty of Graduate Studies and Scientific Research
Master's Program in Information Technology



Dear Officer,

Dear Non-Commissioned Officer,

In the name of God, the Most Compassionate, the Most Merciful

The researcher is working on a project titled "**Cybersecurity Knowledge and Skills Applied in the Palestinian Customs Police: A Case Study**" in order to fulfill the requirements for Al-Quds Open University Master of Information Technology degree.

In order to accomplish this, the researcher has reviewed a range of standards in this field.

This questionnaire has been prepared in line with the study's objectives. We respectfully ask for your cooperation and support in order to complete this questionnaire precisely, carefully, and objectively. Note that any information gathered will be handled in the greatest confidentiality and used only for research purposes.

We truly appreciate your hard work and constructive feedback which will help this study succeed.

With the highest regard and appreciation,

Supervisor: Dr. Waleed Awad

Researcher: Loai Basem Mohammad Shalash

Part One: Demographic Information

Please mark (✓) in the box that matches you:

Gender

☐ Male ☐ Female

Age Group

☐ Under 20 ☐ 20 to less than 30 ☐ 30 to less than 40 ☐ 40 and above

Years of Service

☐ Less than 5 years ☐ 5 to less than 10 years ☐ 10 to less than 15 years ☐ 15 years or more

Educational Qualification

☐ Diploma or less ☐ Bachelor's Degree ☐ Master's Degree or higher

Job Title

☐ Officer ☐ Non-Commissioned Officer

Department

☐ Central Operations ☐ Administrative Affairs ☐ Governorates ☐ Information Technology

Part Two: Implementation and Compliance to Information Security

Policies

This section attempts to assess the degree of application and compliance to information security rules, as well as their execution, and to provide insight into the actual state of these policies within security establishments. This study specifically focuses on the Customs Police in order to learn how these policies are used, evaluate their compliance, and offer suggestions to improve the state of information security regulations as they exist today. It also looks at how efficient these institutions are to handle upcoming technological difficulties.

NO	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Field One: Implementation and Compliance with Information Security Policies						
1.	To guarantee compliance, the Cabinet's decision about information security management is conveyed in a transparent and thorough manner.					
2.	The service offers a comprehensive breakdown of the steps involved in carrying out the Cabinet's information security management decision.					
3.	The service is committed to fully implementing the Cabinet's decision on managing information security.					
4.	The service ensures compliance with cybersecurity instructions in all its activities.					
5.	Through workshops and training sessions, the service educates staff members on its information security rules.					
6.	The security service has the necessary infrastructure to ensure cybersecurity and effectively implement information security policies.					
7.	The security service has adequate human resources to ensure cybersecurity and effectively implement information security policies.					
8.	The security service provides the required technologies to ensure cybersecurity and effectively implement information security policies.					
9.	Effective monitoring mechanisms are in place by relevant authorities to ensure compliance with the Cabinet's decision on managing information security.					
10.	Monitoring authorities promptly take corrective actions to ensure the protection of information.					
Field Two: Risk Management and Assessment						
11.	Non-compliance with information security instructions places the institution in an unstable position.					

12.	The efficiency of the regulations in place can be seen by the low risks that arise from ignoring cybersecurity instructions.					
13.	The service has clear and systematic procedures for identifying potential risks					
14.	Staff are skilled and capable of distinguishing between threats and potential risks, enhancing their response effectiveness.					
15.	Relevant authorities regularly analyze threats and risks to ensure safety and security.					
16.	Authorities can analyze the potential consequences resulting from emerging threats and risks.					
17.	Any suspicions regarding threats or risks are reported to the appropriate authorities within the service					
18.	Reports related to threats and risks are addressed immediately to identify and effectively resolve them.					
Field Three: Risk Management and Incident Response						
19.	The service has a comprehensive plan for addressing information security risks, based on risk assessments and data recovery in disaster scenarios.					
20.	To guarantee that the measures taken are effective, officers take part in creating the plan to address risks.					
21.	Officers are informed about the results of risk management to ensure transparency and accountability.					
22.	Officers are provided with information related to the threats and risks facing the institution.					
23.	Officers are required to report any event related to information systems, such as virus attacks, data breaches, denial of service, or other risks.					
24.	Officers are informed when the effect of a potential risk or threat has ended to ensure clarity of the security situation.					
25.	The service has written procedures for handling information security incidents to ensure effective response.					
26.	The service documents all incidents and vulnerabilities to ensure effective response.					

27.	The service employs an information security professional to guarantee ongoing security measure monitoring.					
28.	The service relies on external information security experts when necessary to strengthen protection.					
29.	The service keeps backup copies of data to ensure recovery in emergency situations.					
Field Four: Roles and Responsibilities						
30.	The service is committed to outlining the duties associated with information security.					
31.	A sufficient number of personnel is available to effectively handle information security issues.					
32.	The person responsible for information security can be easily accessed at any time.					
33.	The information security specialist is committed to reacting promptly to possible dangers and threats.					
34.	Information security specialists possess high competencies in their fields.					
35.	Regular reviews of roles and responsibilities are conducted to ensure alignment with ongoing developments in information security.					
Field Five: Employee Competence						
36.	The service ensures the training and qualification of officers to enhance their competence in information security.					
37.	The service evaluates the competence of officers based on education, training, and practical experience.					
38.	IT department staff possess specialized certifications in cybersecurity.					
39.	Corrective or remedial actions are taken when necessary to improve employee performance.					
40.	The necessary technical support is provided by specialists when needed to ensure effective implementation of procedures					
41.	The service educates employees on best practices for using equipment owned by the security service.					
Field Six: Confidentiality and Information Protection						
42.	The service requires employees not to disclose any information obtained during their work, even after their service ends.					

43.	The principle of confidentiality is applied to all employees without distinction between positions and authorities.					
44.	The service has a specific penalty system for violating security policies, ensuring that every employee knows the consequences of their actions.					
45.	Confidentiality policies are reviewed regularly to ensure compatibility with legal and technological developments.					
46.	The service uses technologies to protect information systems, such as antivirus programs, network security, and intrusion detection systems.					
47.	The service employs licensed firewalls in all governorates and imposes restrictions on the use of removable media (e.g., USB drives, CDs) to protect data.					
48.	Officers are aware of the security risks associated with the misuse of information systems.					
49.	The institution classifies data and information based on their level of confidentiality.					
50.	Data transfer lines are separated from internet lines to ensure the security and safety of information.					
51.	Employees are prohibited from modifying or downloading software on their desktop or portable devices without consulting the IT department.					
Field Seven: Asset and Inventory Management (Equipment) Assets: are the resources owned by the organization to support its operations and achieve its objectives, including equipment, tools and devices. Inventory: are assets given to employees for temporary use within the framework of their work, and they must maintain them and return them in good condition.						
52.	Information security assets (devices) are centrally managed.					
53.	Information security assets (devices) are managed locally within governorates.					
54.	These assets (devices) are updated periodically based on the institution's needs.					
55.	The service has a documented policy for controlling access to assets (devices), reviewed regularly to ensure effectiveness.					

56.	Access policies are reviewed regularly to maintain effectiveness.					
57.	The institution has clear procedures for transferring assets.					
58.	Data related to individuals responsible for asset transfer is documented to ensure transparency and accountability.					
59.	There is an administrative process for requesting new assets.					
60.	The security service maintains a record for documenting issues occurring with equipment and devices.					
61.	Measures are taken to ensure that repaired devices are not tampered with or manipulated.					
62.	The security service has a specialized maintenance department with sufficient expertise to handle malfunctions and issues.					
63.	Physical access to devices and equipment is restricted to authorized personnel only.					
Field Eight: Information Access						
64.	In order to protect sensitive data, the security service categorizes the information that users can access according to their work requirements.					
65.	The dangers of revealing or exchanging organizational information with outside parties without the proper authority are well known to officers.					
66.	Visitors are allowed access to the institution's network (Wi-Fi) according to specific regulations.					
67.	Officers can access the institutional network remotely via VPN in accordance with approved security policies.					
68.	Service providers or equipment suppliers are permitted external network access via VPN or software such as AnyDesk or TeamViewer under controlled conditions.					
69.	The use of wired and wireless internet while working is governed by explicit rules to maintain security and compliance with institutional regulations.					
Field Nine: Physical Access Controls						
70.	The security service has written and published controls to regulate access to high-security areas.					

71.	Entry and exit from high-security areas are documented in a special log.					
72.	The security service confirms each visitor's identity before allowing them entry.					
73.	Access permissions are properly and systematically specified and documented for both employees and individuals.					