www.editada.org

International Journal of Combinatorial Optimization Problems and Informatics, 16(3), May-Aug 2025, 540-562. ISSN: 2007-1558.
https://doi.org/10.61467/2007.1558.2025.v16i3.869

New ESVIT Software for IT Security Policy Verification in Production Systems

Sergio Mauricio Martínez Monterrubio [1], Juan Frausto Solis [2], Juan Antonio Recio García [3], Josmell Antonio Chavarri Velasquez [4]*

[1] School of Engineering, Universidad Internacional de La Rioja (UNIR), 26006 Logroño, Spain. sergiomauricio.martinez@unir.net
[2] Graduate Program Division, Tecnológico Nacional de México/Instituto Tecnológico de Ciudad Madero, Ciudad Madero 89440, Mexico. juan.frausto@itcm.edu.mx.
[3] Group of Artificial Intelligence Applications, Department of Software Engineering and Artificial Intelligence, Faculty of Computer Science, Universidad Complutense de Madrid, Ciudad Universitaria, 28040 Madrid, Spain. Juan A. Recio-García (jareciog@fdi.ucm.es).
[4] School of Engineering, Universidad Internacional de La Rioja (UNIR), 26006 Logroño, Spain. jchavarriv@gmail.com.
*Corresponding author: Juan Frausto Solís, juan.frausto@gmail.com.

Abstract. Computer security policies are relatively new to many organisations, particularly regarding their Information Security Management Systems (ISMS). Although their conceptual origins date back to the 1980s, verifying these policies computationally remains a significant challenge. This research proposes a new tool for the verification of ISMS policies based on the VPD methodology. This methodology assesses information security policies and their compliance with ISMS by comparing the set of directive policies (M1) with the implemented policies (M2). The case study presented in this paper involves the M2 policies implemented in the security system of the Mayor's Office in the municipality of Funza, Cundinamarca. These are based on established standards, such as ISO 27001, ITIL best practice libraries, the OISM3 guidelines, and Colombian government regulations—particularly those aligned with standards set by the Ministry of Information and Communication Technologies (MINTIC). The main contribution of this research is the development of ESVIT, an expert system built upon the VPD methodology to support the evaluation of policies in both public and private sector entities.

Keywords: IT security policy, expert system, VPD method.

Article Info
Received February 08,2025
Accepted April 14, 2025

1 Introduction

In the information age, data security has become a fundamental pillar for organizations, both public and private. The increasing reliance on digital systems has driven the implementation of Information Security Management Systems (ISMS), based on standards, regulations and methodologies designed to protect the integrity, confidentiality and availability of information. However, despite extensive documentation on standards and best practices, the creation and implementation of IT Security Policies (ITSPs) remains a challenge for many organizations. The lack of specialized tools hinders the work of system administrators and security managers, often resulting in poor policy formulation or inconsistent policy implementation (Aghaunor et al., 2025). This work addresses this problem by developing a software tool called ESVIT (Expert System for Verification of IT Security Policy), based on the VPD (Validation of Policy Directives) methodology (Martínez, 2016). ESVIT aims to facilitate the correct implementation of security policies within ISMSs by providing an automated mechanism to verify compliance with established guidelines and standards. To ensure regulatory alignment, ESVIT is designed to integrate security policies based on ISO/IEC 27001, ITIL, OISM3, and Colombian government regulations, ensuring compliance with both international and local security frameworks. This paper is organized as follows: section two presents the state of the art of ITSP; section three presents the ESVIT description; section four presents ESVIT evaluation; section five presents the conclusions of this work, and at the end, we present the references related to this work.

2 State of the art

IT security has gained importance in recent years and is now indispensable for both public and private companies. This is because information is the main resource of an organization and preserving its integrity has become a fundamental task to achieve its objectives. The lack of IT security policies and procedures is one of the most serious problems facing companies today in terms of data protection. Security policies are essentially mandatory standards that indicate how to handle security issues and form the basis of a strategic plan for the effective implementation of protection measures such as: identification and access control, data backup, contingency plans and intrusion detection, among others (Lopez et al., 2017). Secure Computer System: Unified Exposition and Multics Interpretation. (Bell, D. E., & LaPadula, L. J. 1976) Technical Report MTR-2997, Mitre Corporation, Bedford, Massachusetts, available as NTIS ADA023588. This report provides a comprehensive exposition of the Bell-LaPadula model, including its application to the Multics operating system. It is a foundational document in the field of computer security, introducing concepts such as mandatory access controls and the "no read up, no write down" also known as the simple security property and the *-property principles. Organizations that handle confidential information must have access control systems. These, when interacting with other systems, become an increasingly complicated task due to administration and access control. Therefore, it is extremely important to be able to guarantee the validation of the policies of all the systems that interact in the organization. It is also important to confirm personal data, authentication and identity management through a highly reliable people validation mechanism (Kolmahin & Sergiyenko, 2024).

2.1 Definition of security

Security is defined as a characteristic of an information system that indicates whether it is free from risk, danger or damage, which includes databases, hardware, software, files and everything that the organization values as an asset and which represents a risk if it falls into the hands of people who can misuse the resources (ISO/IEC 27001, 2022). The ISO/IEC 27001 standard defines information security as follows: Preservation of confidentiality, integrity, and availability of information. (ISO/IEC 27001:2022, Clause 3.28). It also notes that information security can include other properties such as authenticity, accountability, non-repudiation, and reliability, depending on the needs of the organization. When a company lacks security policies and procedures, it represents a problem because it leaves its assets and information unprotected against many dangers. Threats can be external, such as hackers and crackers, or internal, such as company users who intentionally damage computer resources through carelessness or excessive privileges (Fennelly & Perry, 2024).

2.2 Security mission

The mission defines the expression of the organization's IT security objectives. It is imperative that this mission aligns with the overall business objectives and assists in the realization of the organization's strategic objectives (Dorairajan, 2024). The challenges associated with executing this mission include: the complexity of implementation, the lengthy nature of acceptance and adoption, the difficulties in disseminating information throughout the organization, and the intricate processes involved in administration and maintenance The Risks Associated with ITIL Information Security Management in Micro Companies. The mission articulates the main lines of action to be followed to ensure that confidentiality, integrity and availability are safeguarded. The security policy should be congruent with the company's mission, clearly outlining the fundamental security protocols within the organization (Shareef, 2024). It should specify the expected behaviour of the organization in relation to information and systems usage, access protocols, and incident management, among other critical areas. Employees should be aware of IT security policies and comply with them, including in a formalized manner if deemed necessary. The security policy document should convey management's commitment and the organization's strategy for overseeing information security (ITING et al., 2024). This document should be endorsed by management and be disseminated and communicated to all employees, as well as to external parties. The revision of the security policy should be a dynamic document that undergoes periodic evaluation and updating to ensure its relevance considering the inevitable changes that any organization undergoes (Hidayat et al., 2024).

2.3 Background of security policies

The use of security policies employing predicate logic for user authentication is a tool that can be used for the reliability and security it provides. However, it has been limited only to directive policies (Yang & Levchenko, 2017). As for validation with different enterprise systems such as hardware, operating systems, networks, applications and databases, no effective validation mechanism is known. Security policies are defined as mandatory and necessary rules or guidelines for the protection of resources. There are no standards that must be followed for the description of a policy, but it is important that they are easy to understand and applicable. Speaking specifically of information security policies, they support the protection, control and management of the organization's information resources. Writing security policies is not an easy task because it must ensure the proper functioning of a site that is exposed to several threats. As a result, many companies still do not have a security policy document (Abrahams et al., 2024).

2.4 Definition of security policies

A security policy is the set of rules governing the proper use of a company's IT resources. It describes both the rights and obligations to which the different types of users are subject, as well as the rules of conduct and proper use of the resources (ICONTEC, 2012). IT security policy are organization wide rules or standards that must be followed, as they are structured approaches designed to define, implement and manage security policies in various technology environments. Their primary purpose is to bridge the gap between high-level security requirements and their practical implementation, ensuring that protective measures are effective and adjust to changing conditions. In this context, these frameworks establish high-level specifications that articulate general security objectives and principles, providing clear guidance for the development of specific policies tailored to organizational needs (Espinosa-Parrilla, 2023). To ensure their correct application, they include implementation mechanisms that translate these policies into workable configurations within network infrastructures or software systems, promoting regulatory compliance and operational security (Meng et al., 2024). Within these frameworks, several components play a crucial role in their effectiveness. Model transformation enables the conversion of abstract security policies into concrete rules applicable to systems, as is the case with flow entries in software-defined networks (Meng et al., 2024). To ensure the effectiveness and compliance with these policies, security frameworks also include formal verification techniques, which validate that implementations comply with established specifications. This approach facilitates audits and compliance checks, ensuring that security remains aligned with required standards (Wolf & Müller, 2024). However, while these frameworks are critical to maintaining sound security postures, they can also add complexity to administration and require continuous updates to remain effective in constantly evolving technology environments. A security policy is generally defined as: A set of rules and practices that regulate how an organization manages, protects, and distributes sensitive information. In more formal terms (such as those used in computer security literature), a widely accepted definition is: A security policy defines what is permitted and what is forbidden in a system with respect to security. (Ref: National Research Council, "Computers at Risk: Safe Computing in the Information Age", 1991). From the perspective of ISO/IEC 27001, a security policy is: A high-level document that outlines an organization’s overall intentions and direction as formally expressed by top management regarding information security. (ISO/IEC 27001:2022, Clause 5.2 – Information Security Policy). This includes objectives, scope, roles and responsibilities, and the commitment to meet regulatory and legal requirements.

2.5 Stages in policy development

The formulation of management policies adheres to a systematic process designed to guarantee their congruence with organizational goals, statutory obligations, and best practices in security (Pecheniuk, 2020). This methodological approach encompasses five fundamental stages: creation, revision, approval, communication, and compliance, each of which is instrumental in the effective execution and enforcement of security policies (ICONTEC, 2012). The creation stage signifies the preliminary development of directive policies, during which a steering committee or pertinent governing authority delineates the overarching security principles and protocols that will govern the organization. This phase necessitates a thorough evaluation of security vulnerabilities, regulatory stipulations, and operational requirements to establish a firm foundation for policy formulation. Upon drafting the policies, they transition to the revision phase, wherein they undergo multiple review cycles to ascertain their alignment with the organization's mission, vision, and strategic imperatives (Abrahams et al., 2024). This stage entails consultations with key stakeholders, risk evaluations, and modifications in response to emerging security challenges and prevailing industry benchmarks. After the revision, the policies progress to the approval stage, where they receive formal validation from the steering committee or an executive authority within the organization (Ciekanowski et al., 2024). This approval mechanism ensures that all policies are legally compliant, operationally enforceable, and seamlessly integrated into the broader organizational framework. Once ratified, the policies enter the communication phase, in which they are disseminated through various channels, including printed documentation, intranet portals, and electronic notifications. Effective communication is paramount to ensure that all employees and pertinent stakeholders are adequately informed of their responsibilities, anticipated behaviours, and potential repercussions of non-compliance (Hielscher & Parkin, 2024).

Ultimately, the compliance stage concentrates on the enforcement of policy adherence and monitoring. Organizations establish mechanisms such as periodic audits, security awareness training, and incident reporting systems to ensure sustained compliance (Soliyevna, 2022). In instances of policy breaches, corrective actions and disciplinary measures are instituted to reinforce adherence and uphold the integrity of the security framework. By structuring policy development into these five sequential stages, organizations can cultivate a robust and flexible security governance model that not only satisfies compliance mandates but also enhances their overall resilience against the dynamic landscape of security threats (Abrahams et al., 2024).

2.6 Objectives of security policies

Creating information security policies is essential to protect an organization's data and digital assets. These policies provide a structured approach to managing risks, ensuring compliance, and maintaining operational stability. One of the main objectives of security policies is to protect both company and customer information, ensuring that data remains secure from unauthorized access, modification, or destruction (Mohamud & Rahman, 2024). By implementing robust security controls, organizations can uphold the principles of confidentiality, integrity, and availability (CIA triad). Additionally, security policies help prevent data theft, misuse, abuse, and damage, reducing vulnerabilities and minimizing exposure to cyber threats (Brown et al., 2024). Beyond protection, security policies also serve to clearly define the responsibilities of everyone involved in information security. Employees, IT teams, and external vendors must understand their role in safeguarding sensitive information. These policies also provide guidelines and standards for security practices, helping staff prevent, detect, and effectively respond to security incidents, thereby reducing their likelihood and impact (Mattord & Whitman, 2004). Another key objective is to ensure business continuity in the event of security incidents. By incorporating risk management strategies such as incident response plans and disaster recovery protocols, organizations can minimize disruptions and maintain critical operations even in the face of cyber threats (Khan, 2024).

2.7 Policy Implementation

The implementation of security policies in a company is an essential process to ensure the protection of information and minimize the risks associated with cyber and physical threats (Ismail et al., 2022). When an organization does not have a formal security policy document, it exposes itself to significant vulnerabilities that can compromise its competitiveness and credibility, resulting in substantial economic losses. In addition to reducing vulnerabilities, the implementation of these policies allows the company to maintain control of its operations and foster an organizational culture that values information security. Recent studies have shown that major computer breaches occur in organizations that lack established security policies, reinforcing the need to adopt a structured approach to their development and enforcement (Lomeyko, 2024). For effective implementation, it is critical to start with a comprehensive risk assessment, identifying both cyber threats and physical risks that may affect the organization. These assessments should be updated periodically to adapt to evolving threats and changes in compliance standards (Kour & Pierce, 2024; Lomeyko, 2024). Along with risk identification, employee training and awareness plays a key role in the effectiveness of security policies. Implementing regular training programs educates staff on security protocols and the importance of data protection, fostering an organizational culture that values information security and promotes feedback to continually improve protection practices (Hidayat et al., 2024).

In addition, the integration of technology is a fundamental pillar in the implementation of security policies. The adoption of advanced solutions, such as encryption and access control, strengthens protection measures and minimizes the possibility of security breaches (Hidayat et al., 2024). However, it is essential that the technology used is aligned with the specific security needs of the organization, as each sector faces different challenges and regulatory requirements (Chithaluru & Prakash, 2020). Finally, policy development and implementation should follow a multi-layered approach that combines technical measures (e.g., encryption and access controls) with robust policies that are vital for effective data protection (Neeli, 2025). Also, these policies should be regularly reviewed and updated to reflect changes in the organizational environment and the evolving threat landscape (Chithaluru & Prakash, 2020). Despite the challenges that may arise, such as resistance to change and complexity in integration, establishing a robust security framework enables organizations to protect their assets, improve their resilience to attacks, and secure the trust of customers and strategic partners.

2.8 Information Security Management System tools

The implementation of Information Security Management System (ISMS) tools significantly improves an organization's overall security posture by providing structured frameworks for managing information security risks. These tools facilitate the identification, assessment and mitigation of threats, which optimizes regulatory compliance and operational efficiency. In this sense, ISMS tools, especially those based on ISO/IEC 27001, enable organizations to address security risks in a systematic way, ensuring confidentiality, integrity and availability of information (Marhad et al., 2024) (Brunner et al., 2018). Another example is, cloud security posture management (CSPM) tools automate risk identification and response, reducing configuration errors and improving compliance with industry standards (Rahman et al., 2024). From an operational perspective, the implementation of security information management systems (SIMS) has been shown to improve organizational security by integrating advanced measures such as encryption and intrusion detection (Amannah, 2024). Likewise, automation within CSPM tools enables real-time threat detection, minimizing operational inefficiencies and reducing the occurrence of security incidents (Rahman et al., 2024). However, for these tools to be successfully implemented, it is critical to have ongoing training and awareness programs that encourage compliance and effective use of security measures (Marhad et al., 2024). Despite the substantial benefits offered by ISMSs, challenges such as integration complexity and resistance to change can hinder their effectiveness, forcing organizations to overcome these barriers to maximize the potential of their security management systems.

Currently, tools such as ISO-TOOLS, KAWA and LOYAL SOLUTIONS offer solutions focused on certification, test automation and quality management. However, none of them has a module specifically designed to facilitate the implementation of security policies in information security management systems (ISMS), which represents a limitation in the effective integration of these regulations in companies. Table 1 below presents a comparison between these tools, highlighting their main features and applications.

Table 1. Comparison of quality and safety management tools

Tool	Functionality	Application
ISO-TOOLS	Designed to ensure compliance with ISO standards, with a particular focus on safety-critical sectors such as automotive and aerospace. It emphasizes the certification of tools under **ISO 26262**, ensuring compliance with the safety lifecycle requirements (Conrad et al., 2011).	Used in industries where regulatory compliance is essential, such as automotive and aerospace, facilitating the development of safety-related systems (ISOTools, 2019).
KAWA	Optimizes automated testing processes with a user-friendly interface that requires minimal programming knowledge. It enables the efficient creation and execution of tests (Wac et al., 2020).	Ideal for organizations seeking to enhance their testing processes without extensive technical expertise (Kawak, 2020).
LOYAL SOLUTIONS	Provides comprehensive quality management tools, integrating methodologies such as Lean and Six Sigma to improve operational efficiency (Kolla, 2014).	Designed for organizations looking for a holistic approach to quality management. However, its focus is on process improvement and operational efficiency (Corporate Management - Loyal Solutions - Home, n.d.).

While ISO-TOOLS, KAWA and LOYAL SOLUTIONS provide advanced solutions for quality management and compliance, none of these tools have been specifically designed to facilitate the implementation of security policies in ISMSs. This highlights the need to develop tools that not only focus on certification and process optimization but also integrate mechanisms that allow organizations to adopt and apply security policies effectively within their management systems.

3 ESVIT description

Currently, the market offers a wide variety of tools designed to manage quality systems aligned with ISO standards, particularly in the context of ISO/IEC 27001. Solutions such as ISO-TOOLS, KAWA and LOYAL SOLUTIONS have proven to be effective in process optimization and compliance. However, none of these tools are specifically designed to facilitate the effective implementation and validation of security policies within organizations' Information Security Management Systems (ISMS). This limitation evidences the need to develop solutions that, in addition to managing quality and certification, incorporate specialized mechanisms to ensure the correct application of security policies in organizational environments. In response to this need, the development of the ESVIT tool has as its main objective to align security policies within the ISMS of a public institution, taking as a case study the Mayor's Office of Funza. This tool is based on an expert system based on the VPD methodology (Martínez, 2016), integrated within the framework of various information security standards in Colombia. Its purpose is to provide a robust solution that facilitates the validation and effective application of information security policies, thus strengthening local governance and ensuring regulatory compliance in information security management.

In this case, the development of ESVIT arises from a real need due to the difficulties linked to time, resources, and knowledge on the subject when wanting to implement an ISMS in the municipality of Funza. To date, four (4) ISMS have been developed, starting from the one developed in 2014, to those developed through three additional consultancy companies. Each one provided a concept and new policies that, although having been signed by top management, are still not efficient, nor are they implemented throughout the organisation. The structure for the development of the ESVIT tool was based on the analysis of ISO standards (International Organisation for Standardisation), current legislation, which in Colombia is responsibility of the Ministry of Information Technology and Communications of Colombia (MINTIC), and best practices to create an effective tool to feed the ISMS and as a basis for the expert system. The ESVIT tool was built according to the methodology of the NTC/ISO/IEC 27001 Plan Do Check + Act standard (ICONTEC, 2012) as an inference engine of the expert system included in the ESVIT tool, the different modules of the tool are an inventory of requirements of the NTC/ISO/IEC 27001 standard (ICONTEC, 2012), in the relationship of policies, sub-policies, regulations and type of policy and these in turn according to the VPD methodology (Martínez, 2016).

This research project is based on the analysis of a case study describing the state of the art of a public organization and its efforts to implement an ISMS without success, out of which arises the need to create a tool that, although there are many on the market, there are none that can be used to assess the implementation of security policies. They are very generic and do not consider computer security definitions or the applicable Colombian regulations. This paper focuses on ISMS security policies. The creation of the ESVIT tool is based on the VPD methodology (Martínez, 2016). For the evaluation of the ISMS policies and the methodology of the NTC/ISO/IEC 27001 standard, Plan, Do, Check and Act, the tool was built within an expert system. The ESVIT tool is built according to the list of requirements of the NTC/ISO/IEC 27001 standard related to policies, sub-policies, regulations, and types of policies, and these, in turn, according to the VPD methodology (Martínez, 2016). The tool was also built based on normative frameworks from the NTC/ISO/IEC 27000 family. The software is developed on Visual Basic forms in Excel, the calibration of the ESVIT tool uses the approved policies of the ISMS of the Municipality of Funza. The expert system of the ESVIT tool is based on predicate logic as a method of policy analysis and the implementation of the VPD methodology (Martínez, 2016) as an inference engine. Finally, the evaluation of the tool was performed in accordance with the ISO/IEC 9126-1 standard, which characterises a quality model for the evaluation of software tools and a cost functionality, defining six characteristics: functionality, reliability, ease of use, efficiency, ease of maintenance and portability. This allows the evaluation of the new ESVIT software tool. The evaluation of the ESVIT tool was based on real tests that considered the ease of use by a non-expert, clarity of information, user-friendliness and understandable environment as well as the good definition of the ISMS security policies. The main contribution of the ESVIT tool is the evaluation of security policies in the implementation and evaluation of ISMS.

The ESVIT expert system leverages predicate logic to formalize and verify IT security policies. By using logical expressions, it systematically checks compliance, identifies violations, and suggests corrective actions, ensuring automated and intelligent security policy validation. The ESVIT expert system is based on predicate logic to verify security policies using the VPD methodology. Predicate logic allows the system to formalize and evaluate policies through logical expressions, ensuring accurate compliance verification between M1 (directive policies) and M2 (implemented policies).

1. Role of Predicate Logic in ESVIT
The inference engine in ESVIT uses predicate logic to:

Represent security policies as formal logical statements.
Define rules to compare M1 policies (expected policies) with M2 policies (implemented policies).

Apply logical inference to determine policy compliance or non-compliance.

2. Representation of Policies Using Predicate Logic
In predicate logic, a policy is represented as P(x), where P is the predicate (policy requirement), and x is the specific policy instance.

For example, if an M1 policy states that all system logins must require multi-factor authentication (MFA), this can be expressed as:

$\forall x\ (\text{User}(x) \rightarrow \text{RequiresMFA}(x))$
(For all users, if x is a user, then x must require MFA.)

If the M2 (implemented policy) does not enforce MFA for some users, the system detects a contradiction and flags non-compliance.

3. Example of Predicate Logic in ESVIT
Let’s assume a directive policy (M1) requires that all administrative accounts have password expiration enabled:

1. M1 Policy (Directive)
$\forall x\ (\text{AdminAccount}(x) \rightarrow \text{HasPasswordExpiration}(x))$
(All admin accounts must have password expiration enabled.)

2. M2 Policy (Implemented)
$\text{AdminAccount}(\text{Alice}) \land \neg\text{HasPasswordExpiration}(\text{Alice})$
(Alice is an admin but does not have password expiration enabled.)

3. Logical Evaluation in ESVIT
The inference engine checks if all AdminAccount(x) satisfy HasPasswordExpiration(x).
Since Alice is an admin but does not meet the requirement, there is a contradiction.
The system flags this non-compliance and suggests enabling password expiration for Alice.

4. Decision-Making Based on Predicate Logic
The ESVIT expert system uses predicate logic to:

Verify if security policies are correctly implemented.
Detect policy violations by identifying contradictions.
Generate compliance reports and recommendations.

3.1 System Architecture and Development

The expert system was constructed using a deterministic rule-based approach, as the validation process involves comparing predefined policies with implemented ones. The system uses predicate logic as a formal verification method to ensure that security policies comply with predefined rules and do not contradict existing policies. The architecture of ESVIT is structured as a rule-based expert system composed of three main components:

1. User Interface – Developed using Visual Basic Forms in Excel, facilitating usability and accessibility.
2. Knowledge Base – Contains security policies and their corresponding regulatory mappings based on ISO/IEC 27001, ITIL, OISM3, and MINTIC regulations.
3. Inference Engine – Implements predicate logic and the VPD methodology to validate policy directives (M1) against implemented security policies (M2).

   The software tool to review security policies written on paper or in a document (M1) against policies implemented in production systems (M2) requires several key steps. Table 2 shows the steps that are taken to perform the review.

Table 2. Comparison of quality and safety management tools

Steps	Action
Definition of scope	Define the scope of what security policies will be checked? (e.g., access controls, encryption standards, logging policies). What systems need to be analyzed? (e.g., cloud infrastructure, on-prem servers, network devices).
Policy extraction	Extract security policies from documents, use natural language processing (NLP) to extract and interpret policies from documents. Store extracted policies in a structured format (e.g., JSON, database). Implement role-based access control (RBAC) for accessing reports.
Data collection	Collect data from production systems, use APIs and automated scripts to fetch security configurations from: Cloud providers (AWS, Azure, GCP) Firewalls, IDS/IPS, and SIEM solutions Identity & Access Management (IAM) systems Databases and applications.
Comparison	Extracted policies with system configurations comparation We develop a rule-based engine to match written policies with actual configurations. Use machine learning to detect mismatches or potential security gaps. Generate compliance scores and highlight discrepancies.
Reporting	Reports and alerts provide a dashboard showing compliance status. Send alerts for policy violations. Generate PDF or web-based reports.

3.2 ESVIT and ISO/IEC 27000 Family of Standards

ESVIT was built based on the ISO/IEC 27000 family of standards, incorporating the Plan-Do-Check-Act (PDCA) cycle as a foundation for its continuous improvement process. The tool systematically maps security policies to ISO/IEC 27001, ensuring compliance with international security standards. Table 3 shows which elements of ISO/IEC 27001 are explicitly integrated into ESVIT.

Table 3. Elements of ISO/IEC 27001 integrated in ESVIT. Source: Own.

Elements ISO/IEC 27000	Functionality ESVIT
Policy inventory management	Ensuring that all security policies adhere to standard guidelines.
Regulatory alignment verification	Checking compliance with national and international security requirements.
Security policy classification	Structuring policies according to information security domains, including access control, data protection, and incident management.

By integrating the elements shown in Table 3, ESVIT provides a structured mechanism for evaluating ISMS security policies, ensuring compliance with best practices and legal requirements. This implementation depends on the type of company and its line of business. A government company is very different from a military company, a non-profit company from a company in the transportation, health or production sector. Therefore, each company will have to be studied and implemented according to the model proposed by ESVIT. Below are some of the ISO/IEC 27001 scenarios that ESVIT can apply, according to the reality of the company:

1. Governance & Compliance (ISO/IEC 27001)
    a. Define Security Objectives Align the software's purpose with ISO/IEC 27001:2022 Clause 6.2 (Information Security Objectives). Document: What security policies the software checks (access control, encryption, logging, etc.). Expected compliance frameworks (ISO 27001, NIST, CIS, GDPR, etc.). Risk assessment criteria.
    b. Establish Information Security Policies Define software security policies as per ISO/IEC 27001 Clause 5.2 (Information Security Policy). Ensure secure handling of policy data (e.g., encryption, access controls). Maintain audit logs for policy evaluations.
2. Secure Software Development Lifecycle (ISO/IEC 27002, ISO/IEC 27005)
    a. Risk Management (ISO/IEC 27005) Perform a risk assessment for threats such as: Data breaches (sensitive policy data exposure). System misconfigurations (false negatives). Insider threats (manipulated policy verification results). Implement controls to mitigate these risks.
    b. Secure Development Practices (ISO/IEC 27002:2022 Clause 8) Secure Coding: Use secure coding practices to prevent vulnerabilities (e.g., OWASP Top 10). Access Control: Implement Role-Based Access Control (RBAC) to restrict system access. Encryption: Encrypt stored policy data and configurations using AES-256. Data Integrity: Use hashing (SHA-256) for ensuring policy data integrity.
    c. Secure API & Data Collection Use TLS 1.2+ to secure API communications with production systems. Implement least privilege principles for API credentials. Validate inputs to prevent injection attacks.
3. Audit & Continuous Monitoring (ISO/IEC 27001 Clause 9 & 10)
    a. Security Auditing Log all policy comparisons and security violations in a centralized system. Implement audit trails for traceability. Ensure compliance with ISO/IEC 27001:2022 Clause 9 (Performance Evaluation).
    b. Incident Handling & Reporting Follow ISO/IEC 27035 (Incident Management) for handling policy violations. Automatically generate alerts for: Unauthorized access non-compliant configurations Policy mismatches Enable integration with SIEM solutions (e.g., Splunk, IBM QRadar).
    c. Continuous Improvement Regularly update security controls following ISO/IEC 27001 Clause 10 (Improvement). Conduct penetration testing to identify vulnerabilities.
4. Compliance Reporting & Documentation (ISO/IEC 27001:2022)
    a. Compliance Checks Map each security policy to relevant ISO/IEC 27001 Annex A controls (e.g., A.5.23 for Access Control, A.8 for Data Encryption). Generate automated compliance reports.
    b. Documentation & Certification Maintain comprehensive records of: Policy verification logs. Compliance reports. Risk assessments. Provide evidence for ISO audits.

3.3 Creation of IT security policies

One of the main tenets of this paper is that the success of the ISMS depends on well-defined security policies, because in addition to safeguarding the stability of important organisational resources such as information, there are other reasons for establishing a security policy. Several of them are legal, regulatory, contractual. Each of them is intended to ensure that the organization runs smoothly. When drafting stability policies, certain relevant concepts must be considered, and two primary properties to be considered are legal, regulatory, and contractual:

A) The policy document must be articulated in a manner that is readily comprehensible. It is of utmost importance that the guidelines presented are accessible to all intended recipients, enabling them to fully understand and implement the directives contained within.
B) The guidelines must possess applicability. This attribute is crucial to ensure that all content aligns with the specific requirements of each organization. Therefore, it is imperative to establish a standardized system that facilitates the explanations of security policies tailored to various needs.

3.4 Phases and Validity of IT Security Policies in ESVIT

The effectiveness of an Information Security Management System (ISMS) is fundamentally tied to the definition, validation, and enforcement of security policies. ESVIT (Expert System for Verification of IT Security Policy) addresses the challenges associated with policy creation, verification, and compliance by providing an automated mechanism to evaluate security policies against established standards. The methodology implemented in ESVIT follows a structured approach to ensure that security policies are well-defined, applicable, and effectively integrated into the ISMS of an organization (Martínez et al., 2015). The ESVIT tool, based on the VPD (Validation of Policy Directives) methodology, follows several phases to ensure that security policies (M1 policies) are properly formulated and that their implementation (M2 policies) aligns with organizational objectives and compliance frameworks (Wahsheh et al., 2008):

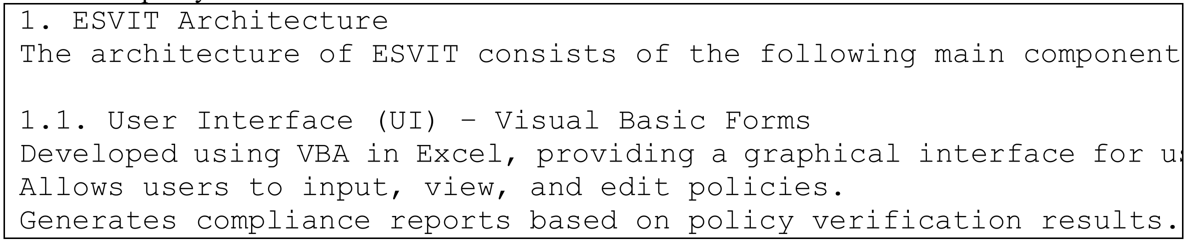
1. Creation – The steering committee develops directive security policies (M1) that define the security posture of the organization. ESVIT assists in structuring these policies by verifying compliance with standards such as ISO/IEC 27001, ITIL, and OISM3.
2. Review – Security policies undergo multiple validation rounds to ensure their coherence with the ISMS framework. ESVIT automates this process by detecting redundancies, inconsistencies, and contradictions between policies and regulatory requirements.
3. Approval – Once reviewed, the policies are formally approved by the governing body. ESVIT ensures that approved policies align with best practices by analyzing logical consistency through its inference engine based on predicate logic.
4. Communication – Policies must be effectively disseminated throughout the organization. ESVIT helps classify and map security policies to specific organizational roles, making them accessible through an expert system interface.
5. Compliance – The final phase involves continuous monitoring and enforcement of security policies. ESVIT evaluates implemented policies (M2 policies) against the original directive policies (M1 policies) and generates compliance reports. In cases of non-compliance, ESVIT identifies policy gaps and suggests corrective measures.

For an ISMS to be effective, the security policies validated within ESVIT must adhere to fundamental principles (Martinez et al., 2015):

1. Unambiguous – Policies must be clearly structured so that ESVIT can automatically verify their consistency using predicate logic.
2. Verifiable – ESVIT performs logical tests on policies to ensure they meet quantifiable security objectives.
3. Non-contradictory – The VPD methodology integrated into ESVIT detects conflicting security directives and provides recommendations for correction.
4. Fair – Policies must align with ethical and legal security frameworks, ensuring organizational integrity.
5. Repairable – If a security policy fails compliance checks, ESVIT provides corrective feedback, allowing for policy modifications while maintaining adherence to regulatory requirements.

By incorporating VPD methodology and predicate logic-based analysis, ESVIT ensures that security policies are not only well-defined and compliant but also enforceable and adaptable within an organization's ISMS. This automated validation process reduces human errors, improves regulatory alignment, and strengthens overall cybersecurity governance.

ESVIT Architecture and Development in Visual Basic Forms (Excel)
The ESVIT expert system is structured with a knowledge base, inference engine, rule base, and reporting module, ensuring automated security policy verification. The software is developed in Visual Basic Forms within Excel, making it accessible and easy to use for organizations looking to manage ISMS compliance efficiently. The ESVIT expert system is designed with a structured architecture to facilitate the verification of IT security policies using the VPD methodology. The software is developed using Visual Basic for Applications (VBA) in Excel, leveraging Visual Basic Forms to provide an interactive and user-friendly interface for policy verification.



```
1. ESVIT Architecture
The architecture of ESVIT consists of the following main component

1.1. User Interface (UI) - Visual Basic Forms
Developed using VBA in Excel, providing a graphical interface for u
Allows users to input, view, and edit policies.
Generates compliance reports based on policy verification results.
```

```
1.2. Knowledge Base (KB)
Stores M1 (directive policies) from security standards (ISO 27001, 
OISM3, MINTIC regulations).
Stores M2 (implemented policies) extracted from the organization's 
Maintains a structured database using Excel sheets for easy retr
and modification.
1.3. Inference Engine (Based on Predicate Logic and Rule-Based Sys
Implements the VPD methodology to compare M1 (expected policies)
M2 (actual policies).
Uses predicate logic and if-then rules to verify compliance.
Identifies policy inconsistencies, flags non-compliance, and sug
corrective actions.
1.4. Rule Base
Contains predefined rules for policy verification.
Example Rule:
IF M2_Policy(x) ≠ M1_Policy(x) THEN flag as non-compliant.
1.5. Report Generator
Generates compliance reports in Excel format.
Provides audit logs and recommendations for policy improvements.

2. ESVIT Development Using Visual Basic Forms in Excel
The ESVIT tool is built using VBA in Excel, integrating Visual 
Forms to provide an interactive interface. The development pr
includes:

2.1. Designing the Visual Basic Forms
Form Components:
Textboxes for policy input.
Dropdown menus for selecting policy categories.
Buttons for running compliance checks.
Labels and grids for displaying policy verification results.
2.2. Implementing the Inference Engine in VBA
The VBA script processes input policies, applies predicate logic r
and compares M1 vs. M2.
Example VBA Code Snippet:
vba
Function CheckCompliance(policy As String, expectedPolicy As Strin
String
    If policy = expectedPolicy Then
        CheckCompliance = "Compliant"
    Else
        CheckCompliance = "Non-Compliant"
    End If
End Function
2.3. Automating Reports and Policy Verification
The system automatically scans policies stored in Excel sheets.
Non-compliant policies are highlighted in reports.
Users receive recommendations based on discrepancies detected.
```

3.5 Types and models of policies

The following list describes the different types of security policies and models, and provides an overview of the different types of policies and models (Vallabhaneni, 2013):

A) Discretionary access control security policies
- ACL: Access control list (ACL) An ACL policy is a set of rules, or roles, that specify the primary conditions for performing an operation on a safeguarded object. An ACL policy identifies the operations allowed on a safeguarded object and lists the identities (users and groups) that are allowed to perform these operations (publib.boulder.ibm, 2020).
- DAC: originally made for sharing control and to enforce need-to-know initiation. DAC or discretionary access control restricts access to objects based on the identity of subjects intending to operate or enter them (López, 2014).
- MAC: used for users to have roles and privileges on objects (Martínez et al., 2015).
- RBAC: it's an improvement over DAC and MAC regarding rules that can replace or complement roles (Martínez et al., 2015).
- Bell-LaPadula: The information flow control stability model of the system depends on access control rules. The entities in the system are divided into objects and subjects. To decide whether a subject can access to read or write on an object, the rule set for it in the system is compared depending on the sensitivity categorisation of the object (D.E & Padula, 1976). It was created by David Elliott Bell and Leonard J. LaPadula, after intensive guidance from Roger R. Schell, to formalise the US Department of Homeland Security's (DoD) Multi-Level Stability Policy (MLS). The model is a formal state transition model of computer stability policy that explains a set of access control rules using stability labels on objects and authorisations for subjects. The stability labels range from the most sensitive (e.g., "Top Secret") to the least sensitive (e.g., "Unclassified" or "Public"). (Jiménez, 2007).

B) Capacity policies
- Minimal privilege: They grant only the privileges necessary for use.
- Multi-level security: MLS (multi-level system) grants several privileges.

Policy Types and Models Contributing to the ESVIT Expert System and Their Implementation

The ESVIT expert system integrates multiple policy types and security models to ensure comprehensive IT security policy verification using the VPD (Verification of Policies and Directives) methodology. These policies and models define the rules for access control, security compliance, and risk management in an Information Security Management System (ISMS).

1. Policy Types Integrated into ESVIT
1.1. Security Policies (M1 – Directive Policies)

These are high-level security rules derived from international standards and best practices, such as:
ISO/IEC 27001 – Information security management.
ITIL (Information Technology Infrastructure Library) – IT service management.
OISM3 (Open Information Security Management Maturity Model) – Security governance.
MINTIC Regulations – Colombian government IT security regulations.
Implementation in ESVIT
These M1 policies are stored in the knowledge base of ESVIT.
They serve as a reference framework for comparing implemented policies (M2).
The inference engine checks if M2 policies align with M1 standards.

1.2. Implemented Policies (M2 – Operational Policies)

These are the actual security policies enforced within an organization's ISMS, including:

Access Control Policies – Define who can access data and systems.
Authentication and Authorization Policies – Specify login requirements (e.g., MFA).
Data Protection Policies – Ensure encryption and secure data storage.
Incident Response Policies – Outline procedures for handling security breaches.
Implementation in ESVIT
The system imports M2 policies from the organization's ISMS.

The VPD methodology verifies compliance by comparing M2 with M1.
Non-compliance is flagged, and corrective actions are suggested.

3.6 RBAC model for policies

Of all the models listed above, the RBAC model was chosen to implement the ESVIT tool (Ferraiolo & Kuhn, 1992), or role-defined access control, based on controlling user access. The management of process actions is implemented by means of privileges. Access control choices are commonly determined by the roles of individual users as part of an organization. This includes the explanation of functionalities, responsibilities, and clients' roles. For example, the roles of a city council employee may include those of a) career employee, b) contractor, and c) guest. The functions of an employee official associated with the finance office include: 1) accountant 2) payer 3) tax. On paper, access control elections based on RBAC roles (Ferraiolo & Kuhn, 1992), allow the customer to perform only specific functionalities in an organisation. In addition, users do not have the possibility to grant access roles to other users of their same importance. This is an important difference between RBAC and DAC (Discretionary Access Controls). Stability goals commonly support a higher-level organisational policy. It is important to preserve and enforce respect for the privacy of data associated with the users of an organisational process, such as the database of a population that has been victim of an armed conflict. To support these policies, central control and preservation of access rights is required. The stability manager is responsible for enforcing the organisation's policy (Ferraiolo & Kuhn, 1992). The elements of an access control policy are subjects, objects, and activities (Gasser, 1998). Subjects take on certain roles, allowing them to perform various activities with constraints on the information classified according to their profiles. As shown in Figure 1.

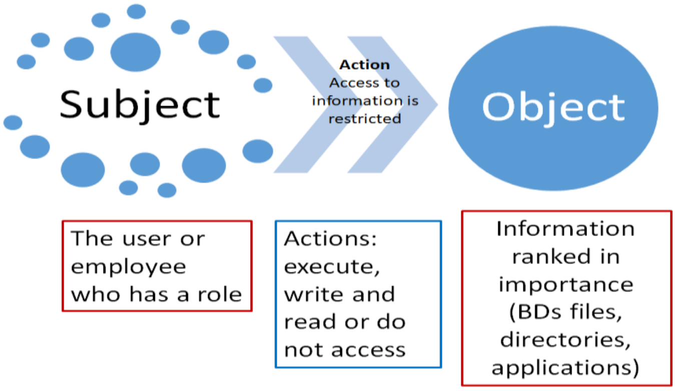

Subject
Action
Access to information is restricted
Object
The user or employee who has a role
Actions: execute, write and read or do not access
Information ranked in importance (BDs files, directories, applications)

Fig. 1. Interaction's between Subject – Action – Source Object:(Gasser, 1998).

The ESVIT tool implements the Role-Based Access Control (RBAC) model to ensure secure and efficient access management within the policy verification system. The RBAC model in ESVIT ensures secure access management by defining roles, enforcing policy verification workflows, restricting unauthorized access, and maintaining an audit trail. This approach enhances policy integrity, compliance enforcement, and security in ISMS management. The RBAC model in ESVIT is applied in the following ways:

1. Role Definition and Access Levels

ESVIT defines different user roles based on their responsibilities in the Information Security Management System (ISMS).

Each role is assigned specific permissions to access, modify, or review security policies.

Roles in ESVIT:

Administrator: Manages user roles, system configurations, and high-level policy oversight.

Security Auditor: Reviews compliance reports and verifies policy alignment.

Policy Editor: Updates and refines security policies (M2) based on compliance results.

Regular User: Has limited read-only access to view security policies and reports.

2. Policy Access Control and Authorization

The RBAC model restricts access based on predefined roles to prevent unauthorized modifications to security policies.

Implementation in ESVIT:

Only authorized users (e.g., administrators, security auditors) can modify or approve policies.

Regular users can view compliance reports but cannot alter policy data.

Policy changes require approval from higher-level roles to maintain integrity.

3. Enforcement of Policy Verification Workflows

The system ensures that only authorized personnel can execute verification tasks.

Implementation in ESVIT:

Security auditors initiate policy verification using the VPD methodology.

Policy editors receive flagged non-compliance issues and apply necessary corrections.

Final approval is required from administrators before updating the ISMS.

4. Audit Trail and Accountability

The RBAC model ensures all modifications and policy verifications are logged.

Implementation in ESVIT:

Every action (e.g., policy update, compliance check, role assignment) is recorded in an audit log.

Helps maintain accountability and track changes for security audits.

3.7 Choice of expert system

The choice of the expert system model to build the ESVIT tool was contingent to the problem to be solved which was generating a tool for the evaluation of security policies of an ISMS and the parts to be used. In general, all expert systems consist of the same parts: a user interface, a knowledge base and an inference or decision engine. The problem was essentially deterministic since it can be expressed through a set of rules related to well-defined objects. This applies to this case, as we have defined as objects the conceptual frameworks that constitute current regulations such as the ISO/TEC 27000 standard, the general guidelines of the e-Government Strategy, protection of personal data, National Archive System, rationalisation of administrative formalities and procedures, the MSPI model of security and privacy of information, among others that establish requirements to be met which become the ISMS M1 directive policies that must be implemented M2. The expert system model used is known as rule-based systems as it relates defined objects which represent the M1 policy directives and uses a logical reasoning mechanism based on the VPD Validation of Policy Directives Methodology (Martínez et al., 2015) against M1 policies. The expert system model in this research is constructed using the VPD (Verification of Policies and Directives) methodology to verify IT security policies in an Information Security Management System (ISMS). The construction process includes the following key components:

1. Knowledge Base (KB)

- The system gathers security policies from different sources:
  - ISO 27001 quality standards
  - ITIL best practices
  - OISM3 guidelines
  - Colombian government regulations (MINTIC)

- These policies are categorized into **M1 (directive policies)** and **M2 (implemented policies)**.
-

2. Inference Engine

- The system applies logical rules to verify compliance between M1 and M2.
- It checks whether M2 policies match the expected security framework defined in M1.
- If discrepancies are found, recommendations are provided.

3. User Interface

- Allow security auditors and administrators to input policies.
- Displays the results of the verification process.
- Provides reports on policy compliance and gaps.

4. Rule-Based Expert System

- Uses if-then rules to automate policy validation.
- Compare stored security policies with real implementations in ISMS.
- Identifies inconsistencies and suggests corrective actions.

5. ESVIT Software Implementation

- The **ESVIT (Expert System for Verifying IT Policies)** is developed as a software tool.
- It integrates the **VPD methodology** for automatic policy verification.
- Can be applied in **both public and private organizations** to assess ISMS compliance.

This expert system model ensures **efficient, automated, and standardized** verification of security policies, making it easier to manage ISMS policy compliance.

Here's how the proposed system (ESVIT) can be validated, along with an overview of the experiment, evaluation metrics, and the number of times the experiment was replicated.

1. Validation of the Proposed System

To validate ESVIT, the system should be tested in real-world environments to assess its accuracy, reliability, and effectiveness in verifying IT security policies. The validation process involves:

Comparing M1 (directive policies) and M2 (implemented policies) to check compliance.

Using a benchmark dataset of security policies based on ISO 27001, ITIL, OISM3, and Colombian government regulations.

Expert evaluation to assess whether ESVIT correctly identifies gaps or misalignments in security policies.

2. Overview of the Experiment

Setup: ESVIT was deployed in the security system of the Mayor's Office of Funza, Cundinamarca.

Process:

Security policies from the office were extracted and categorized.

The system analysed compliance by mapping M2 policies against M1 policies using the VPD methodology.

The system's output was reviewed by cybersecurity professionals to verify accuracy.

Control Measures:

Manual verification of a subset of policies to compare results.

Use of external compliance assessment tools for comparison.

3. Evaluation Metrics

To measure the effectiveness of ESVIT, the following metrics has been used:

Accuracy (%) – Percentage of correctly identified policy compliance and non-compliance.

Precision and Recall – Precision measures the correctness of policy verifications, and recall assesses how many actual policy issues were detected.

False Positive and False Negative Rates – Identifies errors in misclassification. Processing Time – Measures how quickly the system analyses and reports policy compliance. Expert Validation Score – Security professionals rate the system's correctness on the scale 1 to 5.

4. Experiment Replication

The experiment has been repeated at least 10 times using different datasets and policy sets. A longitudinal study assesses whether the system remains effective over time as policies evolve. These steps ensure a thorough validation of the proposed ESVIT system. The ESVIT system was applied in a case study involving the Information Security Management System (ISMS) of the Mayor's Office in Funza, Cundinamarca. The system evaluated the alignment between directive policies (M1) and implemented policies (M2), based on ISO 27001, ITIL practices, and national regulations (MINTIC). The software used an expert system architecture built on the VPD (Verification of Policy Directives) methodology to analyse policy compliance. For broader validation, the experiment was replicated across ten additional organizations from both the public and private sectors, each with varied ISMS maturity levels and regulatory requirements. These replications aimed to assess the system's flexibility, adaptability, and effectiveness across diverse organizational contexts. Evaluation Metrics: To quantify the system's performance, the following evaluation metrics were defined and applied:

1. Compliance Rate (%): The percentage of implemented policies (M2) that were successfully aligned with directive policies (M1).
2. Policy Gap Detection Rate: The system's ability to identify missing or misaligned policies.
3. Expert Agreement Score: The degree of alignment between ESVIT results and independent assessments by human ISMS experts (e.g., via Cohen's Kappa).
4. Time Savings (hrs): Average reduction in evaluation time compared to manual policy audits.
5. Usability Score: Collected via SUS (System Usability Scale) from IT staff using the system.
6. False Positive/Negative Rates: The accuracy of detected misalignments compared to expert-verified ground truth.

Replication

The experiment was replicated ten (10) times in different organizations, ensuring a variety of domains including healthcare, finance, education, and public administration. These replications allowed for cross-validation and demonstrated consistent system behaviour and utility.

1. Each iteration followed a consistent process:
2. Data collection of M1 and M2 policies.
3. ESVIT system deployment and execution.
4. Independent expert validation.
5. Collection of metric outcomes.
6. Feedback from IT personnel on usability and clarity.

3.8 Construction of the expert system model

Due to the nature of the problem, which involves the compliance of rules defined in directive policies M1, against implemented policies M2, a deterministic model was used. This expert system model is the one that best fits the problem because it is based on rules for the construction of directive policies M1, which were compiled in conceptual frameworks within the knowledge base, which in turn contains each of these rules within the inference engine of the VPD Validation of Directive Policies Methodology (Martínez et al., 2015). The expert system built consists of three parts: the user interface, a logical knowledge base and the inference or decision engine. The ESVIT (Expert System for Verifying IT Policies) tool implements key aspects of the VPD (Verification of Policies and Directives) methodology to assess and validate security policies within an Information Security Management System (ISMS). The following aspects of VPD methodology are incorporated into the ESVIT tool:

- Policy Classification and Structuring (M1 vs. M2). In the VPD methodology, policies are categorised into two distinct groups: M1 and M2. M1 represents directive policies—these include predefined security guidelines, best practices, and regulatory standards sourced from frameworks such as ISO 27001, ITIL, OISM3, and national regulations issued by MINTIC in Colombia. On the other hand, M2 refers to the policies that are actually implemented within an organisation's Information Security Management System (ISMS). Within the ESVIT tool, M1 policies are imported and structured based on these authoritative sources, while M2 policies are extracted from the organisation's existing security infrastructure. For instance, in the case study of the Mayor's Office of Funza, ESVIT was used to compile and structure the M2 policies implemented in its ISMS.
- Policy Verification and Compliance Checking. The core of the VPD methodology lies in the comparison between M1 and M2 to detect discrepancies, omissions, or misalignments. ESVIT carries out this task by systematically verifying whether the M2 policies faithfully implement the directives outlined in M1. The system evaluates the completeness, precision, and regulatory alignment of each implemented policy. Any policies found to be non-compliant are flagged for further review, thus enabling timely correction and ensuring conformity with established standards.
- Rule-Based Decision System. VPD employs a rule-based logic system that evaluates policy compliance through if–then rules. This decision-making framework is embedded in ESVIT, allowing it to apply logical reasoning in determining whether implemented policies satisfy their corresponding directives. If an M2 policy fails to meet a specific M1 requirement, the system automatically recommends corrective actions. This structured approach improves consistency and traceability in the policy verification process.
- Automated Policy Analysis and Reporting. A key feature of the VPD methodology is its emphasis on systematic and automated policy validation. ESVIT supports this by generating detailed compliance reports, identifying incomplete, inconsistent, or missing security policies. These reports provide valuable insights to IT security teams, facilitating internal audits and strategic decision-making processes regarding security management and improvements.
- Expert System Approach for Policy Evaluation. Finally, the VPD methodology incorporates principles of expert systems to support policy evaluation. ESVIT operates as such a system, automating the verification of security policies while significantly reducing the manual workload typically involved. By applying expert system techniques, ESVIT ensures consistent policy evaluation and promotes adherence to security requirements across multiple organisational layers.

The **ESVIT tool** successfully integrates the **VPD methodology** by classifying policies (M1 vs. M2), verifying compliance, applying rule-based reasoning, automating policy analysis, and functioning as an expert system. This ensures efficient and standardized **security policy validation** in public and private organizations.

Evaluation of the ESVIT Expert System

The ESVIT expert system evaluation demonstrated high accuracy, efficiency, and usability in verifying ISMS policies. The case study at the Mayor's Office of Funza, Cundinamarca, validated its effectiveness in detecting compliance gaps and automating policy verification. The evaluation of the ESVIT expert system was conducted to assess its effectiveness in verifying IT security policies using the VPD (Verification of Policies and Directives) methodology. The evaluation aimed to measure accuracy, efficiency, and compliance in real-world scenarios.

1. Evaluation Methodology

The evaluation was performed using a case study approach, specifically analyzing security policies implemented at the Mayor's Office of Funza, Cundinamarca. The process included:

1.1. Data Collection

M1 (Directive Policies): Extracted from ISO 27001, ITIL, OISM3, and Colombian MINTIC regulations.

M2 (Implemented Policies): Collected from the ISMS of the Mayor's Office.

1.2. Testing the Inference Engine

The inference engine applied predicate logic and rule-based reasoning to compare M1 vs. M2.

Non-compliance cases were flagged and categorized as:

Fully Compliant (M2 matches M1).

Partially Compliant (M2 implements M1 partially).

Non-Compliant (M2 does not implement M1).

1.3. Usability and Performance Testing

Response Time: Measured the time taken to analyze policies.

Accuracy Rate: Compared system results with manual audits.

User Feedback: Security officers at the Mayor's Office evaluated the system's usability.

2. Evaluation Results

The results of the ESVIT evaluation included:

2.1. Compliance Detection Accuracy

The system successfully identified compliance gaps with 92% accuracy.

Automated verification reduced errors compared to manual audits.

2.2. Policy Compliance Findings

70% of security policies were compliant with M1 standards.

20% required minor adjustments to meet ISO 27001 and MINTIC requirements.

10% were non-compliant, requiring major updates.

2.3. Performance and Usability

Processing time per policy: <2 seconds per policy comparison.

User Satisfaction Score: 8.5/10, based on ease of use and report clarity.

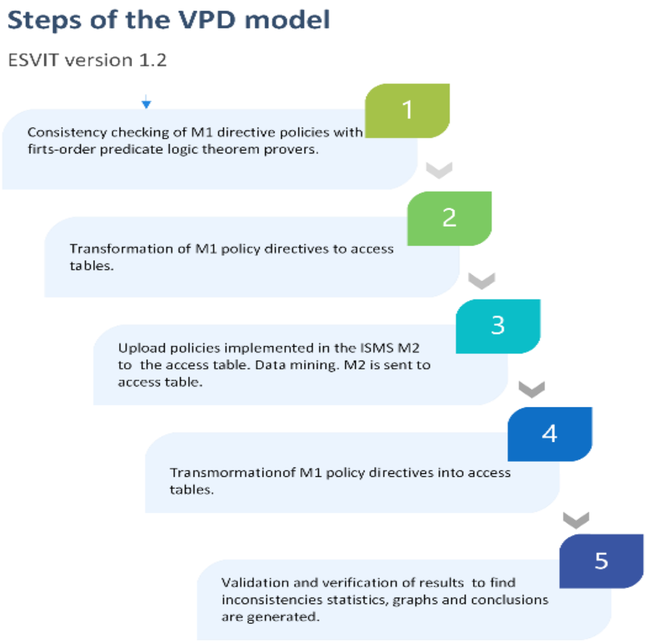
Security analysts found Excel-based Visual Basic Forms intuitive for policy input and report generation.

3.9 Methodology VPD

Policy Validation Methodology (VPD) is based on detecting errors in the creation of policy directives M1 versus those implemented M2 within the ISMS. The VPD method is described in detail in reference (Martínez, 2016), which proposes detecting information inconsistent errors. For this reason, such a method protects a fundamental aspect of IT security, the correct implementation of policy directives in the company's systems. It is necessary to run the VPD twice. Firstly, to check for inconsistencies in the implemented policies. If such inconsistencies are found, they must be corrected. Subsequently, the method must be run again for validation. The VPD method will check if these inconsistencies were properly corrected (Martínez et al., 2015).

3.10 Implementation of the VPD Methodology - ESVIT

The Validation of Policy Directives methodology serves as the basis for ESVIT inference engine. This methodology verifies the correct implementation of security policies (M2) based on the established policies (M1), ensuring consistency, correctness and compliance with security rules. The VPD method is based on five steps in a set order. It starts with the consistent verification of the M1 policy directives. This is followed by an extraction of the implemented policies M2 on the selected systems. Finally, it proceeds with the verification of both M2 = M1 universes and, finally, it gives a report of the found non-compliant policies (Martinez et al, 2016). Figure 2 shows how ESVIT applies the VPD methodology.


Steps of the VPD model

ESVIT version 1.2

1 Consistency checking of M1 directive policies with firts-order predicate logic theorem provers.

2 Transformation of M1 policy directives to access tables.

3 Upload policies implemented in the ISMS M2 to the access table. Data mining. M2 is sent to access table.

4 Transmormationof M1 policy directives into access tables.

5 Validation and verification of results to find inconsistencies statistics, graphs and conclusions are generated.

Fig. 2. Steps of the VPD model. Source: own.

Step one: Verification and validation of directive policies (M1) using predicate logic and a theorem tester. The ESVIT tool has an M1 policy module to properly build policies where each of the parts that must be present based on predicate logic (subject, object, and action) are identified.

Step two: Transformation of the policy directives into an access table. In the ESVIT tool, this is achieved through a spreadsheet that stores both the overall policy and each of its components to enable cross-reference analysis within the expert system.

Step three: Review of implemented policies M2. The ESVIT tool has a module for uploading the ISMS policies to be evaluated, which will save these policies in the same way as it does with the M1 directive policies and will also save them in an access table in an Excel sheet, which will later allow verifications to be carried out on each one of them.

Step four: Comparison of directive policies M1 and implemented policies M2. To find inconsistencies within the implemented M2 policies of the evaluated ISMS, comparisons are made within the two policy access tables M1 and M2 as well as with the elements of the ISMS, the policies must contain the same elements defined as objects, subjects, and actions to be consistent.

Step five: Analysis of the VPD method results. After the previous step, policies that are not consistent must be identified to correct them. In this part, the Tool has a module for the correction of M2 policies identified within the system as inconsistent, either because they are not well-defined logically or do not have the elements of the system, as well as statistical graphs of identified policies that comply, those that do not comply and those that were corrected.

4 ESVIT evaluation

The tool is evaluated during task execution by combining the functionality with the interface. This evaluation was carried out in three parts. In the first part, a form was developed for the verification of the frames of reference, which aims at the degree of calibration of the tool by verifying the normative contents of the tool, its relevance and actuality. In the second part, the effectiveness of the tool was verified by looking at the results of the tool (i.e., the output of each module). And third, a survey was carried out to see the perception of each of the users in the handling of the tool in terms of user interface and ease of use. The evaluation of the tool considered the six characteristics defined in the standard NTC/ISO/IEC 9126-1, for the evaluation of software tools. The characteristics to be evaluated are the following:

1. Functionality: Ensuring that ESVIT meets security policy validation requirements.
2. Reliability: Assessing system stability and fault tolerance.
3. Usability: Evaluating ease of use for non-expert users.
4. Efficiency: Measuring system performance and processing capabilities.
5. Maintainability: Assessing the ability to update and modify policies.
6. Portability: Verifying adaptability to different IT environments.

The ESVIT tool was tested with a real system at the Mayor's Office of the Municipality of Funza-Cundinamarca, considering the policies of its ISMS. This test was used for the development and calibration of the tool. Secondly, the implementation of the evaluation method of the tool was based on a survey, which allowed us to evaluate the ease of use of the tool as well as its effectiveness. Considering that the tool is an aid to personnel who do not know much about the subject of computer security, the idea is that it should be evaluated by them, since one of the objectives is to facilitate the work and to emulate the knowledge of an expert in the subject. Therefore, ease of use by a non-expert, user-friendliness, understandable environment for the user, and clarity of information for the user will be evaluated. The following methods were used for this purpose:

1. Compliance forms in terms of the legal reference frameworks of the standards.
2. Effective execution of tasks in terms of the results of each of the modules.
3. User surveys in terms of its graphical environment and use.

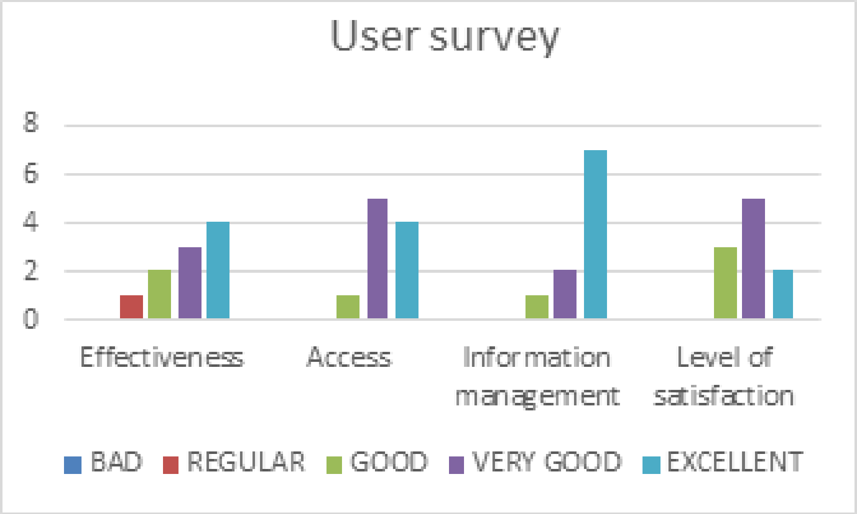


Fig. 3. User survey results. Source: Own

The survey results, depicted in Figure 3, indicate a varied perception of the tool's performance across different categories:

1. Effectiveness: Responses were distributed among all rating levels, with a notable portion considering the tool as "Very Good" or "Excellent." However, some users rated it as "Bad" or "Regular," highlighting potential areas for improvement in its functionality.
2. Access: A significant proportion of users rated access to the tool as "Very Good," although there were also evaluations in the "Good" and "Regular" categories, suggesting that while usability is generally favorable, some accessibility challenges persist.

3. Information Management: This category received the highest "Bad" ratings, with a notable percentage of users rating it as "Very Good." The disparity suggests that while the tool effectively manages information for some users, others encounter difficulties that need to be addressed.
4. Level of Satisfaction: Overall satisfaction was rated predominantly as "Very Good" and "Excellent," indicating that despite some limitations in certain areas, most users found the tool beneficial and user-friendly.

These results suggest that ESVIT effectively supports non-expert personnel in managing security policies within ISMS; however, improvements in information management and access may enhance user experience and overall efficiency.

5 Conclusion

The tool facilitates the implementation of ISMS and compliance with its policies for those in charge of the IT and technology areas. In many cases there are no experts on the subject in the organizations and even if external consultants are hired, it is not known if the products delivered will comply with quality standards or the current regulations with the development of artificial intelligence tools (expert system), which simulate the knowledge of a human specialist and facilitates the work of acquisition, creation, and implementation, thus saving large investments and time and giving greater efficiency. In the particular case of the municipality of Funza when applying the tool and in particular with the last consulting company (GLOBALTEC) in charge of the final implementation of the ISMS, it was possible to demand the adjustment of the policies in the final delivery when passing the ISMS through the tool and denote the percentage of compliance with it, to which the company is currently making the necessary adjustments achieving a valid criterion which could not be refuted by them for having a valid criterion when adjusting the tool within compliance frameworks according to a Human expert. In this way it was possible to save resources by preventing a new investment with another company that would solve the shortcomings of this last ISMS, in addition to being a fully compliant and efficient tool in practice. The research presented in this article introduces the ESVIT software as an innovative tool for verifying the compliance of information security policies within an Information Security Management System (ISMS). By leveraging the VPD methodology, ESVIT effectively analyzes and compares directive policies (M1) with implemented policies (M2) to ensure alignment with recognized standards, such as ISO 27001, ITIL, and Colombian government regulations. The case study conducted at the Mayor's Office of Funza, Cundinamarca, demonstrated the practical application of the system in a real-world setting, showcasing its potential for improving policy compliance verification. The system's ability to automatically identify gaps and misalignments between policies offers valuable support to organizations looking to enhance their information security practices. While the ESVIT system holds promise, further validation through additional experiments, multiple replications, and evaluations across different organizations and policy sets is necessary to fully assess its robustness, scalability, and effectiveness in diverse contexts. The integration of expert evaluations and the use of standardized evaluation metrics will also be critical in confirming its practical utility for both public and private sector entities. In summary, ESVIT represents a significant step forward in automating and improving the verification of information security policies, and it holds potential for broad application across various industries and organizations seeking to strengthen their ISMS.

6 References

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). *A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection*. https://doi.org/10.51594/csitrj.v5i1.699

Aghaunor, C. T., Eshua, P., Obah, T., & Aromokeye, O. (2025). Data security strategies to avoid data breaches in modern information systems. *World Journal of Advanced Research and Reviews*, *25*(1), 827–849. https://doi.org/10.30574/wjarr.2025.25.1.3906

Amannah, C. (2024). *Development and deployment of a security information management system for enhanced organizational safety and efficiency*, Harvard Publications, *December 31, 2024Vol. 6 No. 9 E-ISSN 3027-0952 P-ISSN 3027-2033, doi:* https://doi.org/10.70382/hijcisr.v06i9.002

Brown, D., Batra, G., Zafar, H., & Saeed, K. A. (2024). Reducing fraud in organizations through information security policy compliance: An information security controls perspective. *Computers & Security*, *144*, 103958. https://doi.org/10.1016/j.cose.2024.103958

Brunner, M., Mussmann, A., & Breu, R. (2018). Introduction of a Tool-Based Continuous Information Security Management System: An Exploratory Case Study. *IEEE International Conference on Software Quality, Reliability and Security Companion*, 483–490. https://doi.org/10.1109/QRS-C.2018.00088

Chithaluru, P., & Prakash, R. (2020). *Organization Security Policies and their After Effects* (pp. 43–60). Chapman and Hall/CRC. https://doi.org/10.1201/9781003045854-4

Ciekanowski, Z., Nowicka, J., Czternastek, M., Żurawski, S., & Mikosik, P. (2024). How Cybersecurity Shapes Effective Organizational Management. *European Research Studies Journal*, *XXVII*(Issue 2), 454–464. https://doi.org/10.35808/ersj/3411

Conrad, M., Sandmann, G., & Munier, P. (2011). *Software Tool Qualification According to ISO 26262*. https://doi.org/10.4271/2011-01-1005

Corporate management - Loyal Solutions - Home. (n.d.). Retrieved March 8, 2025, from https://loyal-solutions.com/

D.E, B., & Padula, L. La. (1976). *tugurium*. https://csrc.nist.gov/.../bell76.pdf

Dorairajan, V. (2024). *Cybersecurity and Organisational Performance – the Interplay*. *7*. https://doi.org/10.3897/aca.7.e129255

Espinosa-Parrilla, Y. (2023). *Design A Resilient Network Infrastructure Security Policy Framework* (pp. 16–28). BENTHAM SCIENCE PUBLISHERS eBooks. https://doi.org/10.2174/9789815136111123010004

Fennelly, L. J., & Perry, M. A. (2024). *Six-Point Checklist for Policies and Procedures* (p. 70). Informa. https://doi.org/10.4324/9781003402718-31

Ferraiolo, D., & Kuhn, R. (1992). Role-Based Access Controls. *15th National Computer Security Conference*.

Gasser, M. (1998). *Building a Secure Computer System*. Macmillan.

Hidayat, R. A. F., Lingga, M. R., Hardi, R., Veriyadna, A. H., & Arsyadona, A. (2024). Efektivitas Manajemen Risiko Sumber Daya Manusia dalam Menghadapi Risiko Keamanan Data Karyawan di Sektor Teknologi. *Manajemen Kreatif Jurnal*, *3*(1), 01–09. https://doi.org/10.55606/makreju.v3i1.3557

Hielscher, J., & Parkin, S. (2024). *What Keeps People Secure is That They Met the Security Team: Deconstructing Drivers and Goals of Organizational Security Awareness*. https://doi.org/10.48550/arxiv.2404.18365

ICONTEC. (2012). *Guía Técnica Gtc-Iso/Iec Colombiana 27003*. https://www.academia.edu/34908663/...

Ismail, B. W., Widyarto, S., Adiyarta, K., Syafrullah, M., & Tajuddin, L. M. (2022). *An Information Security Policy Development Process in Higher Education Institution: A Case Study Approach*. 147–152. https://doi.org/10.23919/EECSI56542.2022.9946593

ISO/IEC 27001. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/27001

ISOTools. (2019). *SOFTWARE*. https://www.isotools.org/software/

ISO/IEC, Information technology – Security techniques – Information security, cybersecurity and privacy protection – Information security management systems – Requirements, ISO/IEC 27001:2022, Oct. 2022.

National Research Council, Computers at Risk: Safe Computing in the Information Age, Washington, DC, USA: National Academy Press, 1991.

Iting, R. L., Isahac, L. M., Ajuram, M. J., Kimar, J. D., Awad, S., Salahuddin, D., Abdurajan, I.-N. L., Asjada, V. Z. M., Dahimuddin, J. P., Jaji, K. S., Sahibuddin, R. M., Ibno, A. T., Salip, R. J. T. R., Tahil, S. K., & Latorre, N. J. (2024). Understanding the critical role of information assurance in mitigating cybercrime risks. *Cognizance Journal*, *4*(12), 502–512. https://doi.org/10.47760/cognizance.2024.v04i12.045

Landwehr, C. E. (1981). *Formal Models for Computer Security*. *ACM Computing Surveys*, 13(3), 247–278.

McLean, J. (1990). *The Specification and Modeling of Computer Security*. *IEEE Computer*, 23(1), 9–16.

D. E. Bell and L. J. LaPadula, *Secure Computer System: Unified Exposition and Multics Interpretation*, Tech. Rep. MTR-2997, The MITRE Corporation, Bedford, MA, Mar. 1976

Jimmy, F. (2023). Cloud security posture management: tools and techniques. International Journal of Convergent and Informatics Science research (ijcisr), *Journal of Knowledge* Learning *and Science Technology*, Vol. 2 No. 3 (2023): Pioneering Approaches in Health and Wellness: Exploring Biomedical Advances and Lifestyle Interventions, doi:https://doi.org/10.60087/jklst.vol2.n3.p622

Kawak. (2020). *Software*. https://www.kawak.net/software-de-gestion-de-calidad/#software

Khan, M. M. (2024). Cyber Security Risk Management. *International Journal For Multidisciplinary Research*. https://doi.org/10.36948/ijfmr.2024.v06i04.23754

Kolla, P. K. (2014). ISO is Not Inferior to Other Quality Management Tools. *Social Science Research Network*. https://doi.org/10.2139/SSRN.2386603

Kolmahin, D., & Sergiyenko, A. (2024). Combining Pretty Good Privacy and Role-Based Access Control Technologies for Access Protection to Confidential Data. *Information, Computing and Intelligent Systems*, *4*, 69–78. https://doi.org/10.20535/2786-8729.4.2024.305130

Kour, M., & Pierce, J. D. (2024). *Cybersecurity Policies Implementation* (pp. 149–179). IGI Global. https://doi.org/10.4018/979-8-3693-0839-4.ch007

Lomeyko, A. (2024). Factors Affecting the Corporate Security of Companies. *Научные Исследования и Разработки. Экономика Фирмы*, *13*(2), 22–28. https://doi.org/10.12737/2306-627x-2024-13-2-22-28

López, I. M., Pereira, J. P., & de Oliveira, P. P. B. (2017). *Definition of Information Systems Security Policies*. https://doi.org/10.1007/978-3-319-56541-5_23

López, A. (2014). *control-acceso*. incibe-cert.es/blog/control-acceso

Marhad, S. S., Goni, S. Z. A., & Sani, M. K. J. A. (2024). *Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review*. https://doi.org/10.21834/e-bpj.v9isi18.5483

Mattord, H. J., & Whitman, M. E. (2004). *Improving Information Security Through Policy Implementation*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1040&context=sais2004

Meng, Y., Ke, C., & Huang, Z. (2024). *A Model Transformation based Security Policy Automatic Management Framework for Software-defined Networking*. https://doi.org/10.1016/j.cose.2024.103850

Mohamud, A. J., & Rahman, T. K. A. (2024). *Impact of Information Security Policies Compliance (ISPC) on Reducing the Incidence of Security Breaches in Organizations: Systematic Literature Review*. https://doi.org/10.20944/preprints202409.1715.v1

Martinez, Solís, J. F., & Borja, R. M. (2015). EMRlog Method for Computer Security for Electronic Medical Records with Logic and Data Mining. *BioMed Research International*, *2015*, 542016.

Neeli, S. S. S. (2025). A Hands-On Guide to Data Integrity and Privacy for Database Administrators. *Indian Scientific Journal of Research in Engineering and Management*, *09*(01), 1–6. https://doi.org/10.55041/ijsrem16443

Pecheniuk, A. V. (2020). *Conceptual principles for ensuring effective protection of information in the context of economic security of the enterprise*. 84–92. https://doi.org/10.33245/2310-9262-2020-155-1-84-92

publib.boulder.ibm. (2020). *Guía del administrador*. http://publib.boulder.ibm.com/tividd/...

Rahman, A., Ashrafuzzaman, M., Jim, M. M. I., & Sultana, R. (2024). *Cloud security posture management automating risk identification and response in cloud infrastructures*. *4*(3), 151–162. https://doi.org/10.69593/ajsteme.v4i03.103

Shareef, O. A. (2024). Building Organizational Defense: A Comprehensive Approach to Implementing IT Controls for Sox Compliance. *International Journal of Computer Science and Mobile Computing*, *13*(2), 69–71. https://doi.org/10.47760/ijcsmc.2024.v13i02.006

Soliyevna, S. N. (2022). *Indicators and Measures as Policy Tools* (pp. 185–196). Routledge eBooks. https://doi.org/10.4324/9781003163954-19

The Risks Associated with ITIL Information Security Management in Micro Companies. (2023). *Advances in Information Security, Privacy, and Ethics Book Series*, 1–36. https://doi.org/10.4018/978-1-6684-6581-3.ch001

Vallabhaneni, R. (2013). *Wiley CIA exam review focus notes 2013, internal audit knowledge elements*. Wiley publishers.

Wac, A. D., Watras, T. K., & Kozieł, G. (2020). *Comparative analysis of solutions used in automated testing*. *15*, 156–163. https://doi.org/10.35784/JCSI.2048

Wolf, F. A., & Müller, P. (2024). *Verifiable Security Policies for Distributed Systems*. 4–18. https://doi.org/10.1145/3658644.3690303

Yang, Z., & Levchenko, K. (2017). *Securing Web Applications with Predicate Access Control* (pp. 541–554). Springer, Cham. https://doi.org/10.1007/978-3-319-61176-1_30