# IT Standardization in the Area of Information Security with a Focus on ISO/IEC 27001

Lazar Krstić and Marija Krstić
*Department of Higher Business School Leskovac, Academy of Applied Studies Southern Serbia, Partizanska Str. 7, 16000 Leskovac, Serbia*
*krstic.lazar@vpsle.edu.rs, krstic.marija@vpsle.edu.rs*

Keywords: Standard, Information Security, ISO/IEC 27000, ISO/IEC 27001, T-test.

Abstract: Due to the intensive use of information technologies, the protection and security of information have become a key challenge and imperative in the business environment. Threats to information security are constantly growing, and more and more organizations know that poor information security can be "expensive", regardless of whether their or their customers' confidential data is at risk. In this regard, various standards and guidelines for information security have been developed. In this paper, the focus is on the ISO/IEC 27000 family of standards for information security management, more precisely, the most well-known standard for information security and the fourth most widespread ISO standard - ISO/IEC 27001. The paper aims to analyze the current state of standardization in the field of information protection and security through the analysis of available sources of knowledge and to point out the importance of applying the ISO/IEC 27000 family of standards in practice and then use statistical analysis, specifically, using adequate T-test to examine whether the price of the most popular and, in practice, the most applied standard from the ISO/IEC 27000 family, the ISO/IEC 27001 standard, is statistically significantly different from the price of other published standards from the said family.

## 1 INTRODUCTION

Information technology (IT) is a broad term that includes designing, developing, implementing, supporting, studying, or managing computer information systems, hardware, and software applications. At its core, IT is concerned with improving diverse human problem-solving efforts through the design, development, and use of technology-based systems and processes that improve the efficiency and effectiveness of information and relevant knowledge in a variety of strategic, tactical, and operational situations [1].

Standardization in IT contributes to the more efficient establishment of information functions, their greater stability, and easier transition. Applying international, national, and internal standards creates the conditions for developing an efficient, economical, reliable, and secure software product [2].

Nowadays, the use of information defence technology is no longer enough. It is essential to implement an effective information security management system.

Implementing the ISO/IEC 27001 standard often poses significant financial and organizational challenges, especially for small and medium-sized enterprises. Costs arise from purchasing the standard, engaging experts and consultants, training employees, adapting business processes, upgrading technical infrastructure, and the certification and recertification processes. Therefore, analyzing the economic aspects of implementing the standard is as important as analyzing its security benefits.

The aim of the research is to analyze standardization in the field of information security, with a particular focus on the ISO/IEC 27001 standard, and to examine whether its cost differs statistically significantly from the costs of other standards in the ISO/IEC 27000 family. The methods used in the paper include analysis, comparison, and statistical testing, with a single-sample Student's t-test performed in IBM SPSS Statistics.

Table 1: Literature review.

| Title of work | Description |
|---|---|
| The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda | This paper is based on a systematic review of the existing literature. The identified research themes and sub-themes are organized around five overarching research perspectives: integration with other standards, underlying motivations, implementation-related challenges, potential outcomes, and relevant contextual factors. Through a structured analysis of the academic literature on ISO/IEC 27001, the study provides a comprehensive overview of current knowledge and establishes a solid foundation for further investigation. In addition, the paper highlights several directions for future research, with particular emphasis on interdisciplinary studies positioned at the intersection of information security and quality management [3]. |
| Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management | The research presented in this paper focuses on defining practical rules that organizations should establish to support cybersecurity objectives and ensure effective data protection, particularly for incidents caused by human error. These rules are derived from the ISO/IEC 27001 standard and are intended for use in everyday organizational practices. Their adoption can increase employee awareness of individual behavior in information systems, thereby reducing both the likelihood and the potential impact of human-related security incidents on organizational data and systems [4]. |
| A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard | The paper presents a model of the information security management system compliant with the NTC-ISO/IEC 27001:2013 standard. This model is valid for any organization and helps them understand their current information security status. The proposed model will enable organizations to implement systematic and appropriate controls, procedures, and policies necessary to preserve the integrity, confidentiality, and availability of information assets [5]. |
| Comparative Study Between the Integration of ITIL and ISO/IEC 27001 with the Integration of COBIT and ISO/IEC 27001 | The paper compares the integration of ITIL and ISO/IEC 27001 with the integration of COBIT and ISO/IEC 27001. Factors considered include the increased credibility of information security services, the cost of integrating the two standards, implementation time, the elimination of multiple processes, and improved understanding across parts of the organization. Various sources of literature are used as research methods. The research results can serve as a reference for organizations to determine which of the two information security standards is better to integrate [6]. |
| Significance of ISO/IEC 27001 in the Implementation of Governance, Risk and Compliance | In this research paper, the researchers established the relationship between ISO 27001:2013 and GRC and discussed the standard and GRC objectives. In organizations, 'Governance', 'Risk', and 'Compliance' (GRC) are among the most fundamental and robust pillars that work together to ensure organizations achieve their goals by effectively using available people, processes, and technology. ISO 27001:2013 covers all GRC objectives within its Information Security Management System (ISMS) through which a practical GRC framework can be established and maintained [7]. |

# 2 LITERATURE REVIEW

Few recent freely available works deal with the ISO/IEC 27000 family of standards, precisely the ISO/IEC 27001 standard. Table 1 provides an overview of works dealing with the issue of the ISO/IEC 27001 standard from various aspects. The table contains information about the year of publication of the work, the authors of the work, the title, and a short description.

# 3 INFORMATION SECURITY

The contemporary business landscape relies heavily on information technologies, as information itself represents a strategic resource that significantly influences organizational continuity and development. Irrespective of the medium in which it is stored or processed, information requires adequate protection. Achieving this level of protection assumes that users understand basic security principles and the measures required to implement them. In this context, maintaining the confidentiality, integrity, and availability of information remains a fundamental objective. Nevertheless, information security extends beyond the mere deployment of technical solutions provided by modern IT systems. Information security is the ability to safeguard information throughout its lifecycle (acquisition, processing, storage, transmission, and use) against diverse threats. The relevance of this issue has grown alongside the rapid expansion of computer technologies and the increasing interconnection of systems within

networked environments. As a result, information security has evolved into a broader concern that demands continuous attention and a comprehensive approach.

# 4 STANDARDIZATION AND IT

A standard represents a formally defined document that sets out requirements, recommendations, or characteristics intended to ensure that materials, products, processes, and services fulfill their intended purpose. Such documents are developed through a consensus-based process and are formally adopted by recognized standardization bodies. Their application is not limited to technologically advanced economies; standards are widely used across regions worldwide, including both developed and developing countries [8].

An IT standard is a rule, principle, technique, process, or pattern designed to ensure consistency in information technology services' planning, development, operation, and management [9]. IT standardization refers to making software, systems, and infrastructure used throughout an organization fully consistent and integrated. Once this is done, it is clear that the systems will more easily "talk" to each other, helping to perform business processes more efficiently and enabling jobs to be completed faster [10].

## 4.1 Organizations for Standardization

Standards are of great benefit and importance to consumers and users, as well as to trade, science, and the state, because they provide innovative technologies and increased safety for society [11]. There are three levels of standardization, i.e. standardization can take place at the international, European, or national levels. All three levels are interconnected, and all complement each other. This is ensured by the structure of standardization organizations and internal regulations [12]. The three levels of standardization are:

- International level (ISO);
- European level (CEN, CENELEC, ETSI);
- National level (National Standardization Bodies - NSBs).

The International Organization for Standardization - ISO and the International Electrotechnical Commission - IEC constituted the joint technical committee JTC 1, tasked with adopting standards in information technologies.

## 4.2 ISO/IEC 27000 Family of Standards and ISO/IEC 27001

To address increasingly sophisticated security challenges, organizations should take an integrated approach to information protection by implementing an Information Security Management System (ISMS) to protect the confidentiality, integrity, and availability of information assets. The ISO/IEC 27000 series provides an internationally recognized framework for information security management and organizational resilience, and certification to these standards will also prevent clients from conducting repeated audits. Among these, ISO/IEC 27001 (a joint effort by ISO and IEC) is a central and popular standard that sets out a structured set of security objectives and controls in Annex A. Recent updates to this standard have provided greater flexibility in its requirements, replacing a mandate to use specific controls with an organization's ability to choose controls that best suit its risk management process [13], [14].

The ISO/IEC 27000 family of standards provides a comprehensive framework for information security management, with ISO/IEC 27001 at its core, specifying requirements for an ISMS that integrates people, processes, and IT systems. Applicable to organizations of all sizes and sectors, these standards help manage the security of critical assets, including financial data, intellectual property, employee information, and third-party data. As technology and organizational environments evolve, the family continues to expand, offering guidance to address changing information security needs worldwide. ISO/IEC 27001 is an international standard for information security (in Serbia, SRPS ISO/IEC 27001:2014) that specifies requirements for an ISMS. As part of the ISO 27000 series, it provides a framework for organizations to establish, implement, operate, monitor, review, and continuously improve their information security management system [15].

ISO 27001 helps organizations set clear responsibilities for information. Implementing information security standards ensures that security becomes part of the organization's culture and resilience against cyber threats. ISO 27001 is a standard that an organization should maintain by conducting risk assessments, which enables management and key stakeholders to maintain information security risks. The safeguards (or controls) that an organization must implement are usually policies, procedures, and technical implementation (such as software and hardware). However, in most cases, organizations already have

all the necessary security controls in place, but they are not always implemented correctly. Since such an implementation will require the management of many policies, procedures, people, and resources, ISO 27001 describes how to link all these elements together in an ISMS. Therefore, the whole concept of ISMS is not only about IT security (like firewalls and antivirus). These are process management, legal protection, human resource management, physical asset protection, and more [16].

The ISO/IEC 27001 standard is comprehensive, as it treats information security from three aspects [17]:

- IT - analyzing and defining the performance of IT equipment, access rights, encryption, passwords, protocols, and policies from the aspect of data and information security risks;
- administrative - defining clear instructions, policies, and procedures for the generation of information, its distribution, and preservation (storage);
- physical - physical access control, employee records, video surveillance, protection of work premises.

The advantages of the information security management system are [2]:

- Meeting legal requirements - there are more and more laws, regulations, and contractual requirements related to information security, most of which can be addressed by applying ISO/IEC 27001 - this standard provides the perfect methodology to comply with them all.
- Gaining a marketing advantage - if an organization gets certified and competitors don't, it gives them an advantage in the eyes of customers sensitive to their data protection.
- Lower costs - the underlying philosophy of ISO/IEC 27001 is to prevent security incidents, and every incident, big or small, costs money. Therefore, the organization will save a lot of money by preventing incidents.

Better organization - fast-growing organizations often do not have time to stop and define their processes and procedures. The consequence is that employees often do not know what, when, and who should do it. Implementing ISO/IEC 27001 helps solve such a situation because it encourages organizations to write their core processes (even those unrelated to security), which allows them to reduce losses and optimize employees' working time.

### 4.3 IEEE Standardization in the Field of Cybersecurity and Privacy

IEEE (Institute of Electrical and Electronics Engineers) is the world's largest technical professional organization dedicated to advancing technology through technology standard setting and educational activities [18]. IEEE standards are developed within its societies and coordination committees through a consensus-based process approved by the American National Standards Institute. This process brings together volunteers representing diverse perspectives, who contribute without compensation, to produce the final standard. While IEEE oversees the development process and ensures fairness, it does not test, evaluate, or verify the technical accuracy of the information contained in the standards [19].

The IEEE Cybersecurity and Privacy Standards Committee is responsible for standardizing cybersecurity and privacy standards in the IEEE. Cyber security focus is but not limited to cryptographic techniques, cyber incident management, identity management, IT system security assessment, information security management systems, network security, security automation, continuous monitoring, supply chain risk management, software, and system assurance safety engineering standards. On the other hand, privacy includes, but is not limited to, standardization related to privacy risk identification and mitigation methods and technology [20].

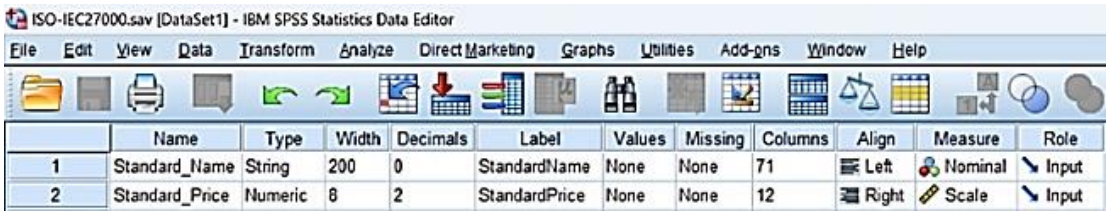
## 5 RESEARCH METHODOLOGY

Basic methods, including analysis, synthesis, concretization, and generalization, as well as general scientific methods, analytical-deductive and comparative, were applied in the work. Basic methods (analysis, synthesis, concretization, and generalization) were used to have a more superficial understanding of concepts from the theory of information security, standardization in that area, ISO/IEC and IEEE standards, i.e., interpretation of T-test results, and conclusion. The analytical-deductive method was used to operationalize appropriate analytical procedures of a qualitative-quantitative character, making adequate conclusions. The comparative method was used when comparing scientific and professional papers dealing with similar

issues to those with which this paper deals. Also, the paper used an appropriate statistical method for hypothesis testing, while the sample description was presented with the help of descriptive statistics indicators.

The research problem investigates whether the price of the ISO/IEC 27001 standard differs statistically from the average price of other standards in the ISO/IEC 27000 family. Since the objective is to compare the sample mean with a predefined reference value, a one-sample t-test was applied. The essence of the one-sample Student's t-test is to determine whether the sample mean differs statistically significantly from a predefined reference value, allowing assessment of whether the observed difference is due to random variation or is statistically significant. Statistical analysis was conducted using IBM SPSS Statistics, a software tool for statistical data processing. The dataset included published standards from the ISO/IEC 27000 family, obtained from the official website of the International Organization for Standardization (ISO), where each row corresponds to a single standard and its price.

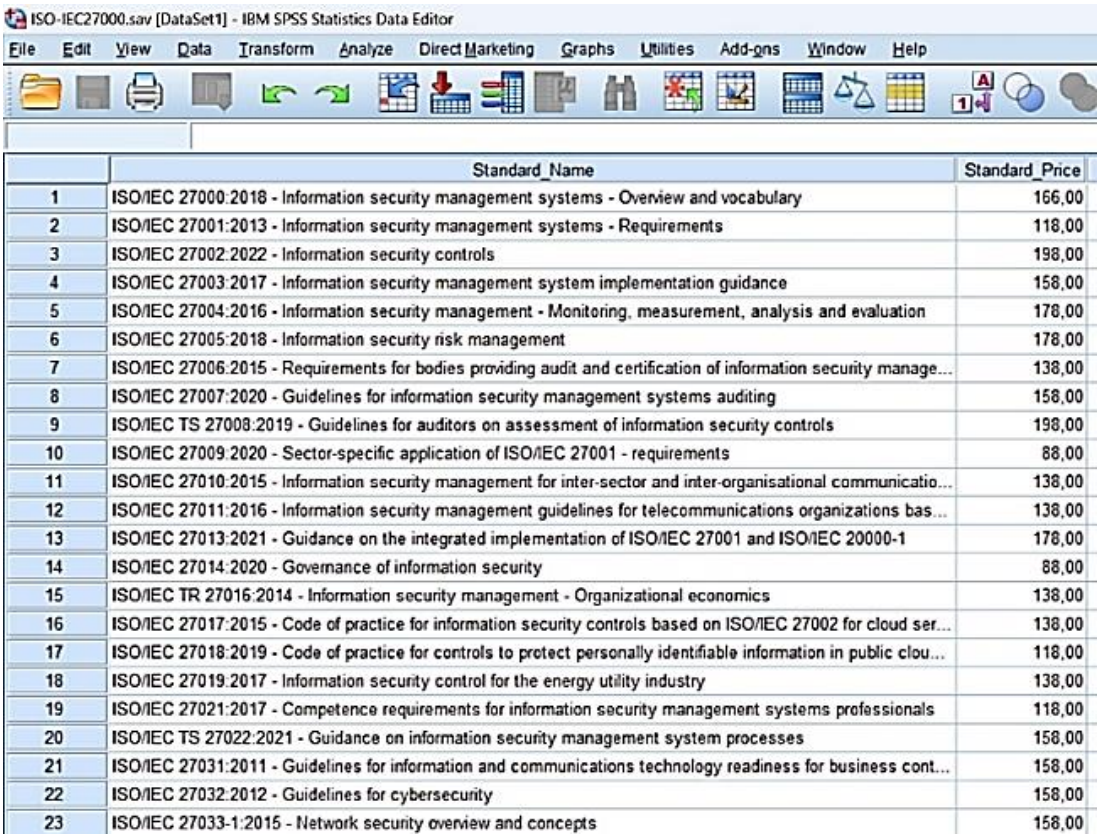
In the statistical analysis, two variables were used: Standard_Name, a nominal variable for standard identification, and Standard_Price, a continuous numerical variable representing the price of each standard. Figure 1 presents the variables used in the analysis, highlighting the nominal variable (Standard_Name) and the continuous dependent variable (Standard_Price), while Figure 2 illustrates the dataset employed for the statistical analysis.


ISO-IEC27000.sav [DataSet1] - IBM SPSS Statistics Data Editor

File Edit View Data Transform Analyze Direct Marketing Graphs Utilities Add-ons Window Help

| | Name | Type | Width | Decimals | Label | Values | Missing | Columns | Align | Measure | Role |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Standard_Name | String | 200 | 0 | StandardName | None | None | 71 | Left | Nominal | Input |
| 2 | Standard_Price | Numeric | 8 | 2 | StandardPrice | None | None | 12 | Right | Scale | Input |

Figure 1: Presentation of the variables used in the statistical analysis.


ISO-IEC27000.sav [DataSet1] - IBM SPSS Statistics Data Editor

File Edit View Data Transform Analyze Direct Marketing Graphs Utilities Add-ons Window Help

| | Standard_Name | Standard_Price |
|---|---|---|
| 1 | ISO/IEC 27000:2018 - Information security management systems - Overview and vocabulary | 166,00 |
| 2 | ISO/IEC 27001:2013 - Information security management systems - Requirements | 118,00 |
| 3 | ISO/IEC 27002:2022 - Information security controls | 198,00 |
| 4 | ISO/IEC 27003:2017 - Information security management system implementation guidance | 158,00 |
| 5 | ISO/IEC 27004:2016 - Information security management - Monitoring, measurement, analysis and evaluation | 178,00 |
| 6 | ISO/IEC 27005:2018 - Information security risk management | 178,00 |
| 7 | ISO/IEC 27006:2015 - Requirements for bodies providing audit and certification of information security manage... | 138,00 |
| 8 | ISO/IEC 27007:2020 - Guidelines for information security management systems auditing | 158,00 |
| 9 | ISO/IEC TS 27008:2019 - Guidelines for auditors on assessment of information security controls | 198,00 |
| 10 | ISO/IEC 27009:2020 - Sector-specific application of ISO/IEC 27001 - requirements | 88,00 |
| 11 | ISO/IEC 27010:2015 - Information security management for inter-sector and inter-organisational communicatio... | 138,00 |
| 12 | ISO/IEC 27011:2016 - Information security management guidelines for telecommunications organizations bas... | 138,00 |
| 13 | ISO/IEC 27013:2021 - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 | 178,00 |
| 14 | ISO/IEC 27014:2020 - Governance of information security | 88,00 |
| 15 | ISO/IEC TR 27016:2014 - Information security management - Organizational economics | 138,00 |
| 16 | ISO/IEC 27017:2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud ser... | 138,00 |
| 17 | ISO/IEC 27018:2019 - Code of practice for controls to protect personally identifiable information in public clou... | 118,00 |
| 18 | ISO/IEC 27019:2017 - Information security control for the energy utility industry | 138,00 |
| 19 | ISO/IEC 27021:2017 - Competence requirements for information security management systems professionals | 118,00 |
| 20 | ISO/IEC TS 27022:2021 - Guidance on information security management system processes | 158,00 |
| 21 | ISO/IEC 27031:2011 - Guidelines for information and communications technology readiness for business cont... | 158,00 |
| 22 | ISO/IEC 27032:2012 - Guidelines for cybersecurity | 158,00 |
| 23 | ISO/IEC 27033-1:2015 - Network security overview and concepts | 158,00 |

Figure 2: Representation of a part of the data set used in the statistical analysis.

Table 2: Descriptive statistics of the variables in the analysis.

| One-sample statistics | | | | |
|---|---|---|---|---|
| | N | Mean | Std. Deviation | Std. Error Mean |
| Standard_Price | 65 | 139.0462 | 35.33608 | 4.38290 |

Table 3: One sample t-test results.

| One-sample test | | | | | | |
|---|---|---|---|---|---|---|
| | Test Value = 118 | | | | | |
| | t | df | Sig. (2-tailed) | Mean Difference | 95% Confidence Interval of the Difference | |
| | | | | | Lower | Upper |
| Standard_Price | 4.802 | 64 | .000 | 21.04615 | 12.2903 | 29.8020 |

# 6 RESULTS AND DISCUSSION

Today, the cost and efficiency of implementing the ISO/IEC 27001 standard are addressed through cost-benefit analyses, risk assessments, and return-on-investment models. Organisations increasingly adopt a risk-based approach, implementing only those security controls that are economically justified and tailored to their business needs. In addition, integration with other standards and the use of cloud and automated solutions help reduce the costs of implementing and maintaining the information security system.

In order to empirically examine the cost differences identified through these approaches, a one-sample T-test was applied, and the following hypotheses were formulated:

- H0: The price of the ISO/IEC 27001 standard is statistically not significantly different from the price of other published standards from the ISO/IEC 27000 family.
- H1: The price of the ISO/IEC 27001 standard is statistically significantly different from the price of other published standards from the ISO/IEC 27000 family.

After performing the T-test for one sample in the SPSS tool, the results shown in Tables 2 and 3 were obtained.

Table 2 shows descriptive statistics, i.e., the number of samples, mean, standard deviation, and standard error of the mean. The average value of the test result is 139.04. Table 3 shows the one-sample T-test statistics. In the first row, the mean value of the population is entered (test value = 118). It is necessary to refer to the fourth column (Sig. (2-tailed)) for the significance of the T-test statistic. If $p > .05$, the null hypothesis is not rejected. In this case, the p-value is less than 0.05 ($p = .000 < .05$), so the null hypothesis is rejected, and it is concluded that the price of the ISO/IEC 27001 standard is statistically significantly different from the price of other published standards from the ISO/IEC 27000 family.

The results indicate a significant difference between the true mean (M=118.00) and the mean test score (M=139.04; SD=35.33), [$t(64) = 4.802$, $p = .000$]. Therefore, the null hypothesis that there is no difference between the true mean and the comparison value is rejected, and it is concluded that the mean test score is significantly different from the true population mean.

This statistically significant difference in the price of the ISO/IEC 27001 standard compared with the other ISO/IEC 27000 standards suggests that cost is a potential barrier to decision-making for organizations considering certification. This result may also affect decision-making processes, especially for small and medium-sized enterprises, by highlighting the role of cost-related factors in the adoption of information security standards. This study provides empirical evidence on economic factors in information security, alongside technical and organizational factors. By quantitatively demonstrating price differences across these standards, the analysis has contributed to a more complete picture of the information security standards adoption process.

The strength of the ISO/IEC 27001 standard is its ability to help an organization establish an information security risk management framework that protects vital information. This is based on various studies indicating that organizations that adopt the ISO/IEC 27001 standard will see improved employee awareness, greater security uniformity, and better defenses against online attacks. However, achieving this standard will depend on the organization's commitment to incorporating security controls into its culture, thereby enabling the development of a customized standard to suit the organization’s needs. From this perspective, ISO/IEC 27001 certification alone is not enough; the organization’s culture plays a critical role in the standard’s success.

# 7 CONCLUSIONS

Implementing IT standardization is one of the fastest ways to achieve business goals. In other words, IT standardization can help organizations achieve their goals faster and continuously upgrade their growth and profits.

Awareness of the importance of information security is increasing, a positive trend that should continue. The International Organization for Standardization (ISO) remains committed to helping global organizations by developing standards based on input from subject matter experts around the world.

The ISO/IEC 27000 family of standards was created to help organizations manage the risks of cyberattacks and internal threats to data security. The ISO/IEC 27001 standard from the specified family of standards provides a framework for ISMS organizations and is certifiable and widely used, with a tendency of constant growth. It consists of processes, policies, and resources that can be used to systematize an organization's security requirements.

By statistical analysis, specifically by applying the Student's T-test for one sample over the created data set, which contains published standards from the ISO/IEC 27000 family, it was necessary to determine and give an answer to the question whether the price of the most popular and in practice the most applied standard from the ISO family /IEC 27000, the ISO/IEC 27001 standard, statistically significantly differs from the price of other published standards from the mentioned family. Based on the obtained results, it is concluded that the price of the ISO/IEC 27001 standard is statistically significantly different from the price of other published standards from the ISO/IEC 27000 family.

The importance of the ISO/IEC 27001 standard for organizations is reflected in the fact that it enables systematic information security management through risk identification and control, protection of confidentiality, integrity, and availability of data, as well as compliance with legal and contractual requirements, thereby reducing security incidents and strengthening the trust of customers and partners. On the other hand, the cost of implementing and certifying this standard plays a key role because it affects the scope, quality, and sustainability of the information security management system, so adequate investment represents a long-term investment in the stability of the business, its reputation, and the competitive advantage of the organization.

The ISO/IEC 27001 standard cannot be downloaded for free from official sources but must be purchased from ISO or national standards bodies. Cost can be a significant barrier for small businesses and other organizations, especially in lower-income countries. This limitation reduces the wider availability of knowledge, since the standard contains recommended practices and controls for information security management, which, in the interest of general security improvement, should be more accessible to the public. Difficult access to the standard further reduces the likelihood that organizations will understand its importance and consider its implementation.

# REFERENCES


[1] The MBA Institute, “Definitions of IT,” 2025, [Online]. Available: https://themba.institute/information-systems-for-managers/definitions-of-it/, [Accessed: Aug. 20, 2025].

[2] PC Press, “Standardi u informacionim sistemima i tehnologijama,” 2025, [Online]. Available: https://pcpress.rs/standardi-u-informacionim-sistemima-i-tehnologijama/, [Accessed: Aug. 20, 2025].

[3] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, “The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda,” The TQM Journal, vol. 33, no. 7, pp. 76-105, 2021, [Online]. Available: https://doi.org/10.1108/TQM-09-2020-0202.

[4] A. Y. El-Bably, “Overview of the impact of human error on cybersecurity based on ISO/IEC 27001 Information Security Management,” Journal of Information Security and Cyber Research (JISCR), vol. 4, no. 1, pp. 95-102, 2021, [Online]. Available: https://doi.org/10.26735/WLPW6121.

[5] O. Fonseca-Herrera, A. Rojas, and H. Florez, “A model of an information security management system based on NTC-ISO/IEC 27001 standard,” IAENG International Journal of Computer Science, vol. 48, no. 2, pp. 213-222, 2021, [Online]. Available: https://www.iaeng.org/IJCS/issues_v48/issue_2/IJCS_48_2_01.pdf, [Accessed: Aug. 27, 2025].

[6] N. K. Gunawan, R. B. Hadiprakoso, and H. Kabetta, “Comparative study between the integration of ITIL and ISO/IEC 27001 with the integration of COBIT and ISO/IEC 27001,” in IOP Conf. Series: Materials Science and Engineering, Jakarta, Indonesia, Nov. 21-22, 2020, pp. 1-5, [Online]. Available: https://doi.org/10.1088/1757-899X/852/1/012128.

[7] S. Choubey and A. Bhargava, “Significance of ISO/IEC 27001 in the implementation of governance, risk and compliance,” IJSRNSC Int. J. of Scientific Research in Network Security and Communication, vol. 6, no. 2, pp. 30-33, 2018, [Online]. Available: https://ijsrnsc.org/index.php/j/article/view/130/130, [Accessed: Sept. 2, 2025].

[8] Institut za standardizaciju Srbije, "Šta je standard?" 2025, [Online]. Available: https://iss.rs/sr_Latn/shta-je-standard_p13.html, [Accessed: Sept. 3, 2025].

[9] CIO Wiki, "IT Standard (Information Technology Standard)," 2025, [Online]. Available: https://cio-wiki.org/wiki/IT_Standard_(Information_Technology_Standard), [Accessed: Sept. 4, 2025].

[10] 1+1 Technology, "Achieve your business goals faster with IT standardization," 2025, [Online]. Available: https://www.1plus1tech.com/achieve-your-business-goals-faster-with-it-standardization/, [Accessed: Sept. 5, 2025].

[11] DKE Standards, "The importance of standardization – benefits and advantages," 2025, [Online]. Available: https://www.dke.de/en/standards-and-specifications/importance-of-standardization, [Accessed: Sept. 6, 2025].

[12] Standards+Innovation, "Standardization organizations," 2025, [Online]. Available: https://www.standardspluselearning.eu/b-1-1-standardization-organizations, [Accessed: Sept. 7, 2025].

[13] D. Ganji, H. Mouratidis, and S. M. Gheytassi, "Towards a modelling language for managing the requirements of ISO/IEC 27001 standard," in Proc. SOFTENG 2019 – Fifth Int. Conf. on Advances and Trends in Software Engineering, Valencia, Spain, Mar. 24-28, 2019, pp. 17-23, [Online]. Available: https://www.researchgate.net/publication/332801832.

[14] A. Renvall, Improving Cybersecurity Through ISO/IEC 27001 Information Security Standard in the Context of SMEs, M.S. thesis, Metropolia Univ. of Applied Sciences, Helsinki, Finland, 2018, [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/157277/Renvall_Aleksi_final.pdf.

[15] IT Governance, "ISO 27000 series of standards," 2025, [Online]. Available: https://www.itgovernance.co.uk/iso27000-family, [Accessed: Sept. 13, 2025].

[16] Auro Standard, "ISO 27001," 2025, [Online]. Available: https://www.aurostandard.org/standardi/iso-27001/, [Accessed: Sept. 13, 2025].

[17] Jonik, "ISO 27001:2013," 2025, [Online]. Available: https://www.jonik.rs/rs/iso-27001-2013, [Accessed: Sept. 15, 2025].

[18] IEEE, "About IEEE," 2025, [Online]. Available: https://www.ieee.org/, [Accessed: Sept. 16, 2025].

[19] ISO, "ISO/IEC/IEEE 18882:2017," 2025, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:18882:ed-1:v1:en, [Accessed: Sept. 16, 2025].

[20] IEEE Computer Society, "Cybersecurity and Privacy Standards Committee," 2025, [Online]. Available: https://www.computer.org/volunteering/boards-and-committees/standards-activities/committees/cybersecurity-privacy, [Accessed: Sept. 20, 2025].