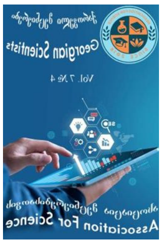
Georgian Scientists

ქართველი მეცნიერები

Vol. 7 Issue 4, 2025

https://doi.org/10.52340/gs.2025.07.04.46



Risk Analysis and Control of Information Systems in ISO/IEC 17025 Accredited Testing Laboratories

Nino Lortkipanidze

[1]Georgian Technical University, faculty of Informatics and Control systems, Tbilisi, Georgia

Abstract

In the era of digital transformation, information security has become a critical determinant of reliability in ISO/IEC 17025 accredited testing laboratories, especially those conducting transformer parameter measurements that directly influence national energy infrastructure. This study develops a comprehensive risk analysis and control framework grounded in ISO/IEC 27005 and NIST SP 800-30 methodologies and enhanced with modern cybersecurity mechanisms, including Zero Trust architecture, DevSecOps practices, automated monitoring, and disaster recovery solutions. To provide an integrated evaluation of laboratory information system resilience, the research introduces a Trustworthiness Index (TI), combining confidentiality, integrity, and availability as core security attributes. Simulation results involving three hypothetical laboratories demonstrate that the implementation of advanced control mechanisms significantly increases TI values—from medium trustworthiness levels (55–68) to high levels (78–85). Additionally, an optimization model using the Steepest Ascent Method identifies the most effective configuration of controls for each laboratory profile, ensuring resource-efficient security enhancement. The findings reveal that compliance with ISO/IEC 17025 alone is insufficient to guarantee comprehensive information security, highlighting the need for systematic integration of international cybersecurity standards. Future work will involve validating the proposed model using real laboratory data and extending the TI methodology to multi-criteria or weighted assessment approaches.

Key words: accredited testing laboratories, information security, ISO/IEC 17025, ISO/IEC 27005, risk management

Introduction

In the modern digital era, information systems security represents one of the most critical challenges for both private companies and the public sector. The process of digital transformation has significantly increased the volume, sensitivity, and value of data flows within organizations, thereby intensifying the risks of cyberattacks, technical failures, and mismanagement of information.

This issue is particularly important for accredited testing laboratories operating under the ISO/IEC 17025 standard [1]. Such laboratories ensure the reliability of measurement and control processes, which serve as the basis for numerous technical and economic decisions. The data generated within laboratories directly affect the safety and efficiency of energy systems, including the evaluation of electrical characteristics of transformers.

In transformer testing, the measured parameters—no-load losses, insulation resistance of windings, winding resistance under direct current, dielectric loss angle, and transformation ratio—represent critical information for the resilience of energy infrastructure. The loss, alteration, or misinterpretation of such data may lead to significant economic damage and even large-scale failures of power systems.

Therefore, the analysis of information system risks and the application of modern control methods in laboratories is not only essential for fulfilling accreditation requirements but also represents a strategic component of energy sector reliability and national energy security. This research addresses this necessity by aiming to highlight methods and tools that strengthen the resilience, security, and efficiency of information systems in laboratories accredited under ISO/IEC 17025.

With these challenges in mind, the present study sets the following research objectives:

The main objective of the research is to study and model modern methods for analyzing and controlling information system risks in accredited testing laboratories (in compliance with ISO/IEC 17025), with a focus on laboratories conducting electrical parameter measurements of transformers.

This objective is broken down into the following tasks:

- To compare information security and risk management practices across three hypothetical laboratories;
- To identify, classify, and evaluate risks based on international standards (ISO 27005, NIST SP 800-30);
- To explore the applicability of modern control mechanisms such as Zero Trust, DevSecOps, and automated monitoring tools;
- To develop recommendations aimed at increasing the resilience of laboratories.

This paper contributes by developing an integrated framework that not only complies with ISO/IEC 17025 but also strengthens resilience against cyber and operational risks.

Related Work

Existing studies on information security and risk management provide a strong methodological basis for the analysis of accredited testing laboratories. ISO/IEC 27005 [2] and NIST SP 800-30 [3] offer internationally recognized frameworks for systematic identification and evaluation of risks in information systems. Research on Zero Trust architectures [4] emphasizes the elimination of implicit trust and continuous verification of users and devices, while DevSecOps practices [7] integrate security into the entire software lifecycle. Studies on cloud computing security highlight challenges of ensuring confidentiality and reliability in cloud-based infrastructures, where risks such as data leakage and service availability remain critical [6], [10]. Additionally, recent works on cyber-physical systems security [5] and digital infrastructure [8] trustworthiness contribute to the development of integrated evaluation models. However, despite these advances, limited attention has been paid to the specific context of ISO/IEC 17025 accredited laboratories, where the accuracy of transformer measurements directly affects energy system resilience. This gap motivates the need for tailored approaches that combine international best practices with laboratory-specific requirements [9].

Therefore, this research addresses a gap by contextualizing information security risk management specifically for transformer parameter testing laboratories.

Proposed Method

To validate the applicability of international standards in practice, three hypothetical laboratories were modeled to represent different infrastructural and organizational contexts.

Laboratory A – Accredited by the National Accreditation Center, employing 15 staff members.

- Main focus: Measurement of power transformer energy efficiency.
- Data processing: Conducted within an in-house ERP system.
- Risks: Unauthorized alteration of measurement results due to insufficient access controls; inadequate data archiving policies.

Laboratory B – Accredited according to an international scheme (via ILAC).

- Main focus: Quality control of small- and medium-capacity transformers.
- Data processing: Performed on a cloud-based platform (SaaS).
- Risks: Availability issues of cloud infrastructure; cybersecurity threats such as phishing and data leakage.

Laboratory C – A mixed-profile laboratory conducting tests on both high-voltage and low-voltage equipment.

- Main focus: Analysis of dielectric losses.
- Data processing: Based on internal servers within an isolated network.
- Risks: Physical security violations; lack of backup systems.

The analysis of these laboratory profiles provides a basis for identifying and assessing risks within a systematic framework, as defined by the research methodology.

- Data Collection: Modeling of hypothetical scenarios derived from the requirements of ISO/IEC 17025 [1].
- Risk Identification: Combination of ISO 27005 [2] and NIST SP 800-30 [3] methodologies.
- Evaluation Criteria:
  - Impact on the accuracy and reliability of measurements;
  - Availability and integrity of information;
  - Compliance of the laboratory with the standard.

Algorithm Description

A risk matrix was developed for each laboratory, illustrating the sources of risk, their consequences, probability, impact, overall risk level, and potential control mechanisms. The identified risks are summarized in risk matrices for each laboratory (see Table 1, Table 2, and Table 3).

Table 1. Risk Matrix for Laboratory A

Risk source	Consequence	Probability	Impact	Risk level	Control mechanism
Unauthorized alteration of measurement results in ERP	Loss of data reliability	Medium	High	High	Data integrity checks (hash/checksum), access logging
Inadequate archiving policy	Loss of historical data	High	Medium	High	Backup archives, automated backup system
Weak authentication mechanisms	Unauthorized access	Medium	High	High	Multi-factor authentication (MFA)
Power outage	Interruption of measurement process	Low	High	Medium	Use of UPS and generators

Table 2. Risk Matrix for Laboratory B

Risk source	Consequence	Probability	Impact	Risk level	Control mechanism
cloud service outages	Loss of access to data	Medium	High	High	Multi-tenant hosting, SLA management
phishing attacks, data leakage	Breach of confidentiality	High	High	Very High	Zero Trust model, anti-phishing, SOC monitoring
Network interruption	Delay in measurements	Medium	Medium	Medium	Network backup channels
incorrect user privileges	Alteration of critical data	Medium	High	High	RBAC model (Role-Based Access Control)

Table 3. Risk Matrix for Laboratory C

Risk source	Consequence	Probability	Impact	Risk level	Control mechanism
physical intrusions	Device damage	Low	High	Medium	physical security control (card system, cameras)
absence of backup systems	Total data loss in case of failure	Medium	High	High	Automated backup servers
internal network failures	Measurement delays	Medium	Medium	Medium	Network monitoring and recovery plans
Uncontrolled personnel access,	Data alteration or deletion	Medium	High	High	RBAC, MFA, regular access audit

These matrices enable a detailed view of laboratory vulnerabilities, the probability of threat realization, and the degree of their impact. However, risk identification and classification alone are insufficient. While the matrices reveal individual risk levels, an integrated indicator is needed to evaluate the overall system security.

In modern information security risk management approaches, particular importance is given to the objective assessment of system trustworthiness. For this study, a hypothetical model of the Trustworthiness Index (TI) was developed, based on a three-dimensional framework aligned with international standards.

The TI is defined as an integrated metric combining the evaluation of:

- Confidentiality (C)
- Integrity (I)
- Availability (A)

These parameters were selected as the core determinants of information system trustworthiness in line with ISO/IEC 27001 and ISO/IEC 17025 requirements.

At the first stage, each parameter was scored on a scale of 0 to 100, where 0 represents a critically vulnerable state and 100 indicates maximum protection. The scoring was derived from the results of the risk matrices describing identified threats, their probability of occurrence, and their potential impact.

The Trustworthiness Index was calculated using the arithmetic mean formula:

$$TI = \frac{C + I + A}{3}$$

Where:

- TI – Trustworthiness Index
- C – Confidentiality score
- I – Integrity score
- A – Availability score

Evaluation

The next stage of the research involved simulation analysis aimed at evaluating how the Trustworthiness Index of laboratories changes following the integration of different control mechanisms.

The simulation considered modern mechanisms such as:

Zero Trust Architecture – eliminating implicit trust in system access and enforcing strict identification policies [4];

DevSecOps Practices – embedding security into the development and operational lifecycle [7];

Automated Monitoring and SOC Systems – enabling real-time detection and prevention of risks [9];

Backup and Disaster Recovery Mechanisms – ensuring data protection under critical circumstances.

The analysis of laboratory processes showed the following results:

The comparative results of Trustworthiness Index values before and after the implementation of control mechanisms are illustrated in Figure 1.

Laboratory A – At the initial stage, the Trustworthiness Index was 62. The risk matrix indicated weaknesses in data integrity controls within the ERP system and inadequate backup policies. After the adoption of Zero Trust architecture and automated backup solutions, the probability of data integrity compromise was significantly reduced. Consequently, the index rose from 62 to 81, indicating that addressing core security weaknesses ensures higher reliability of measurement results and stronger compliance with ISO/IEC 17025 requirements.

Laboratory B – The initial Trustworthiness Index was 55. The primary risks were related to cloud infrastructure threats, especially phishing and data leakage. The simulation showed that implementing a Zero Trust model (with continuous verification of access) and SOC monitoring (ensuring constant oversight of network activities) substantially reduced the probability of data leakage. As a result, the index increased from 55 to 78. Nevertheless, dependency on third-party providers for guaranteed cloud service availability remained a residual risk, preventing the index from reaching its maximum.

Laboratory C – The initial Trustworthiness Index was relatively high, at 68, due to the system’s physical isolation and lack of exposure to open networks. However, the absence of backup systems created a major threat of complete data loss under critical conditions. By implementing backup servers, enforcing access control via the RBAC model, and adding monitoring tools, system resilience improved significantly. As a result, the index rose from 68 to 85, the highest score among the three laboratories [5], [8], [12].

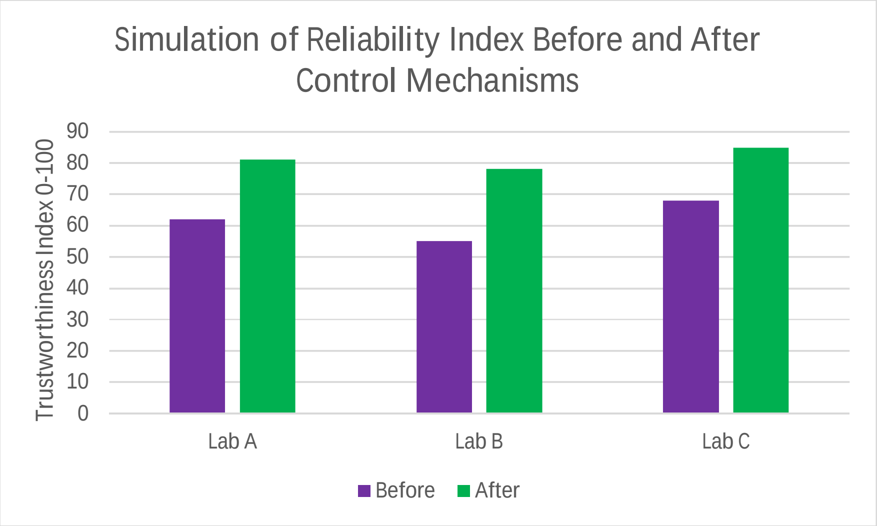


Figure 1 Simulation of Reliability before and after Control Mechanisms

Optimization of Control Mechanisms Using the Steepest Ascent Method

Although the simulation process demonstrated the effect of individual control mechanisms on the Trustworthiness Index (TI), modern cybersecurity management increasingly requires defining optimal combinations of security controls. To address this requirement, the present study integrates a mathematical optimization model based on the Steepest Ascent Method, which determines the configuration of control mechanisms that maximizes TI for each laboratory type [11], [15].

Parameterization of Security Controls

To apply optimization techniques, the security control mechanisms were parameterized as continuous variables $x_i \in [0,1]$, representing the strength of their implementation. The following decision variables were defined:

- x_1– Zero Trust strictness level
- x_2– Backup and disaster recovery frequency
- x_3– SOC/monitoring automation depth
- x_4– Access control strength (RBAC + MFA)
- x_5– Network segmentation level

Each variable affects the three main TI components—Confidentiality (C), Integrity (I), and Availability (A)—by reducing the probability or impact of specific risks.

Objective Function

The optimization problem aims to maximize the Trustworthiness Index:

$$TI = \frac{C(x) + I(x) + A(x)}{3}.$$

Therefore, the mathematical formulation is:

$$\text{Maximize } TI(x_1, x_2, \dots, x_5)$$

subject to:

$$0 \le x_i \le 1, i = 1, \dots, 5.$$

Because TI is not analytically known and depends on simulation outcomes, partial derivatives were approximated numerically using finite differences.

Steepest Ascent Optimization Algorithm

The Steepest Ascent Method identifies the direction of the fastest improvement in TI. The gradient vector is computed as:

$$\nabla TI(x) = [\frac{\partial TI}{\partial x_1}, \frac{\partial TI}{\partial x_2}, \frac{\partial TI}{\partial x_3}, \frac{\partial TI}{\partial x_4}, \frac{\partial TI}{\partial x_5}].$$

At each iteration k, the variables were updated using:

$$x^{(k+1)} = x^{(k)} + \lambda \nabla TI(x^{(k)}),$$

where $\lambda$is the learning rate selected to ensure stable convergence without oscillation. The algorithm terminated when:

$$| TI(x^{(k+1)}) - TI(x^{(k)}) | < \epsilon,$$

indicating convergence to a local optimum.

Optimization Results

Table 4 Gradient analysis revealed the most influential control variables for each laboratory

Laboratory	Dominant Gradient Component	Interpretation
A	$\frac{\partial TI}{\partial x_2}$	Increasing backup frequency yields the largest marginal increase in TI.
B	$\frac{\partial TI}{\partial x_1}$	Zero Trust strictness maximizes growth due to high confidentiality risk.
C	$\frac{\partial TI}{\partial x_3}$	Automated monitoring provides the steepest improvement.

After optimization (table 4), the model produced the following optimal configurations:

Laboratory A: High backup frequency + moderate Zero Trust + strong authentication

Laboratory B: Maximum Zero Trust + strong anti-phishing and SOC monitoring

Laboratory C: High monitoring automation + strong RBAC and MFA

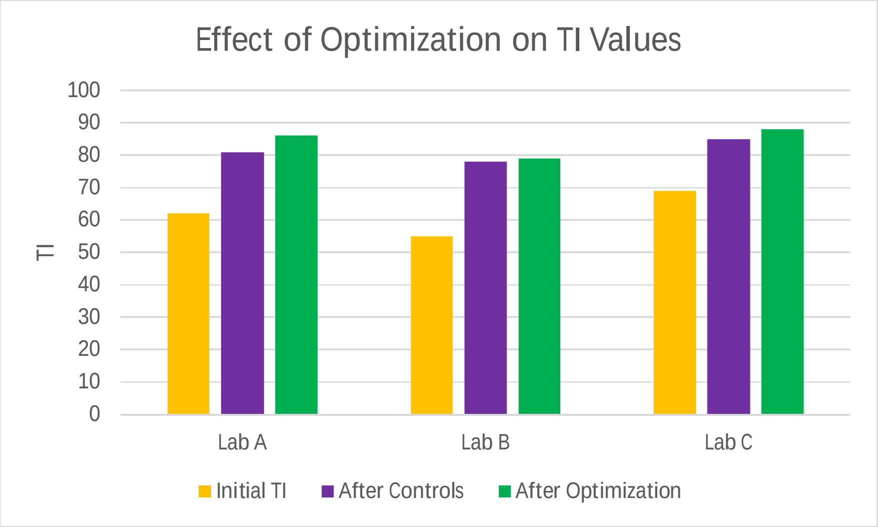


Figure 2. Effect of Optimization on Trustworthiness Index (TI).

Figure 2 illustrates the comparative changes in the Trustworthiness Index (TI) for Laboratories A, B, and C across three stages: the initial state, the implementation of baseline security controls, and the optimized configuration derived using the Steepest Ascent Method. The diagram demonstrates that while all laboratories experience a substantial increase in TI after the introduction of standard security measures, an additional improvement is achieved once the optimal combination of controls is applied. This confirms that security mechanisms not only elevate overall trustworthiness but can be further enhanced through mathematical optimization to maximize resilience with efficient resource allocation. Laboratory C exhibits the highest post-optimization TI due to its strong gains from monitoring automation and strengthened access control. Overall, the figure highlights the importance of both structured cybersecurity enhancements and their optimization for ISO/IEC 17025 accredited laboratories [13].

The optimization model provides a mathematically justified method for selecting the optimal security investments for ISO/IEC 17025 laboratories. The method demonstrates that TI can be improved not only through individual controls but also via their synergistic configuration, ensuring efficient resource allocation and maximum resilience of laboratory information systems.

Conclusion

The study demonstrated that information systems security in ISO/IEC 17025[1] accredited testing laboratories requires a multidimensional approach that extends beyond the baseline requirements of the standard. By integrating international cybersecurity frameworks—ISO/IEC 27005 [2], NIST SP 800-30 [3], Zero Trust architecture [4], DevSecOps principles [7], automated monitoring, and disaster recovery—the research showed that laboratory resilience can be significantly increased without compromising operational efficiency.

The proposed Trustworthiness Index (TI) provided a unified and quantifiable method for assessing laboratory information system security across confidentiality, integrity, and availability dimensions. Simulation results from three hypothetical laboratories revealed that their TI values increased from medium (55–68) to high levels (78–85) once modern control mechanisms were implemented. These findings confirm that structured cybersecurity interventions have a measurable and substantial impact on the reliability of laboratory measurements, the stability of supporting information systems, and, ultimately, national energy security.

Furthermore, the optimization model based on the Steepest Ascent Method introduced a novel analytical layer for resource-efficient security enhancement. The results showed that the optimal set of controls varies depending on laboratory characteristics: backup frequency in Laboratory A, Zero Trust strictness in Laboratory B, and monitoring automation in Laboratory C. This indicates that cybersecurity investment strategies should be tailored to specific infrastructural and operational contexts rather than uniformly applied.

Nevertheless, the study has limitations. The analysis relied on hypothetical laboratory profiles and simulated data, which may not fully capture the complexity of real-world scenarios. The Trustworthiness Index, although effective as a composite indicator, treats confidentiality, integrity, and availability equally, which may not always reflect operational priorities. Future research should therefore validate the model using real laboratory datasets, develop weighted or risk-sensitivity-based versions of TI, and incorporate additional dimensions such as traceability, auditability, and human-factor risks.

Overall, the developed framework offers a practical and scalable methodology for laboratory managers, accreditation bodies, and cybersecurity specialists seeking to strengthen the protection of measurement data and ensure alignment with global best practices. By combining risk management standards with modern security architectures and optimization methods, this research contributes to advancing the resilience, reliability, and trustworthiness of laboratory information systems in the digital era.

References

[1] ISO/IEC 17025:2017. General requirements for the competence of testing and calibration laboratories. Geneva: ISO.

[2] ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on information security risk management. Geneva: ISO.

[3] NIST SP 800-30 Rev. 1. (2022). Guide for Conducting Risk Assessments. National Institute of Standards and Technology, U.S. Department of Commerce.

[4] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). Gaithersburg: NIST.

[5] Humayed, A., Lin, J., Li, F., & Luo, B. (2021). “Cyber-Physical Systems Security—A Survey.” IEEE Internet of Things Journal, 8(7), 5606–5625.

[6] Abomhara, M., & Koien, G. M. (2021). “Security and Privacy in Cloud Computing: Current Challenges and Future Research Directions.” Journal of Cloud Computing, 10(1), 50.

[7] Shackleford, D. (2022). DevSecOps Practices and Tools: A Guide for Secure Development and Operations. SANS Institute.

Ahmad, R. W., Gani, A., & Hamid, S. H. A. (2023). “Resilience and Reliability in Cloud-based Critical Infrastructures.” Future Generation Computer Systems, 143, 230–243.

[8] Georgescu, A. (2024). “Trustworthiness in Digital Infrastructures: Towards a Unified Index for Risk Assessment.” International Journal of Information Security Science, 13(1), 11–25.

[9] ENISA (2025). Cybersecurity Guidelines for Testing and Calibration Laboratories. European Union Agency for Cybersecurity.

[10] Nona Otkhozoria, Vano Otkhozoria, & Shorena Khorava. (2022). SEARCH FOR AN EXTREMUM USING THE STEEPEST DESCENT METHOD UNDER THE CONDITIONS OF EXPERIMENTAL ERRORS. World Science, (2(74). https://doi.org/10.31435/rsglobal_ws/28022022/7785

[11] Otkhozoria, N., Petriashvili, L., Zhvania, T., & Lortkipanidze, N. (2025). Information Risk Analysis in Laboratories Complying with ISO/IEC 17025 Standard. International Science Journal of Engineering & Agriculture, 4(5), 50–61. https://doi.org/10.46299/j.isjea.20250405.05

[12] Lortkipanidze, N., & Otkhozoria, N. (2024). Navigating business excellence: The crucial role of information technology service management through best practice ITIL. Georgian Scientists, 6(1), 120–124. https://doi.org/10.52340/gs.2024.06.01.15

[13] Otkhozoria, N., Petriashvili, L., Zhvania, T., & Imerlishvili, A. (2025). Advancing information system testing: challenges, methods, and practical recommendations. International Science Journal of Engineering & Agriculture, 4(2), 203–214. https://doi.org/10.46299/j.isjea.20250402.13

[14] Chkheidze, I., Otkhozoria, N., & Narchemashvili, M. (2021). EVALUATION OF MEASUREMENT QUALITY USING THE MONTE-CARLO METHOD. Universum, 65-70. DOI: 10.32743/UniTech.2021.84.3-4.65-70

[15] Otkhozoria, N., Tsiklauri, N., & Otkhozoria, V. (2024). Selection of Mathematical Optimization Methods for Solving Engineering Practice Problems. Georgian Scientists, 6(2), 286–293. https://doi.org/10.52340/gs.2024.06.02.30