International Science Journal of Engineering & Agriculture
2025; 4(5): 50-61
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20250405.05
ISSN: 2720-6319

INTERNATIONAL
SCIENCE GROUP

Information Risk Analysis in Laboratories Complying with ISO/IEC 17025 Standard

Nona Otkhozoria
Faculty of Informatics and control systems, Georgian Technical University, Tbilisi, Georgia
ORCID 0000-0002-5837-5345

Lily Petriashvili
Faculty of Informatics and control systems, Georgian Technical University, Tbilisi, Georgia
ORCID 0000-0003-3593-4877

Taliko Zhvania
Faculty of Informatics and control systems, Georgian Technical University, Tbilisi, Georgia
ORCID 0000-0003-1238-5211

Nino Lortkipanidze
Faculty of Informatics and control systems, Georgian Technical University, Tbilisi, Georgia
ORCID 0009-0004-4998-0334

Abstract: The rapid integration of digital technologies into testing and calibration laboratories has significantly increased both operational opportunities and information security risks. Compliance with ISO/IEC 17025:2017 requires laboratories not only to ensure the technical accuracy of testing and calibration activities but also to implement systematic information risk management practices. This paper presents a comprehensive study on the identification, analysis, and prioritization of information risks in a laboratory environment that employs a Laboratory Information Management System (LIMS), IoT devices, and cloud-based data infrastructures.

The research adopts a hybrid methodology that combines qualitative tools (risk matrix and impact–probability assessment) with quantitative models (Common Vulnerability Scoring System, CVSS). Five predominant risks were identified: outdated and unpatched versions of LIMS, insecure IoT sensor communications, low staff cybersecurity awareness, weaknesses in cloud access control, and lack of logical network segmentation. Among these, unpatched LIMS platforms and insufficient staff awareness emerged as the most critical risks, each scoring high on both likelihood and impact, thus directly threatening laboratory accreditation and data integrity.

The findings reveal that information risks in ISO/IEC 17025-compliant laboratories arise not only from technological vulnerabilities but also from human factors and insufficiently standardized processes. The absence of systematic patch management was identified as the most pressing risk, while inadequate network segmentation further exacerbates incident containment. To address these issues, the study proposes a set of mitigation strategies aligned with ISO/IEC 27001/27005, NIST SP 800-30, and ENISA best practices. Key recommendations include the adoption of automated patch management policies, implementation of network segmentation to isolate IoT devices from core systems, multi-factor authentication, encryption of sensitive data, and continuous staff training.

The proposed framework enhances both compliance and resilience, ensuring that laboratories maintain the integrity, confidentiality, and availability of their information assets while meeting the requirements of ISO/IEC 17025 accreditation. Beyond compliance, this approach positions laboratories to effectively respond to evolving cybersecurity challenges in dynamic environments.

Keywords: Information risk analysis; ISO/IEC 17025; Laboratory Information Management System (LIMS); cybersecurity; IoT security; risk matrix; patch management; network segmentation; ISO/IEC 27005; NIST SP 800-30.

1. Introduction

In the digital transformation era, testing and calibration laboratories represent a unique class of organizations where technical reliability and information security must coexist in equal measure. Unlike typical enterprises, laboratories are directly bound by accreditation standards such as ISO/IEC 17025, where any disruption in the integrity of information can undermine both business continuity and the credibility of national and international measurement systems. In this sense, laboratories operate not only as service providers but also as critical nodes in global scientific and industrial ecosystems, where trust in measurement results directly translates into safety, quality, and regulatory compliance across entire sectors. Consequently, the stakes of information risk management in this environment are unusually high. While commercial organizations may suffer financial or reputational damage from security incidents, laboratories risk invalidation of their calibration results, which can cascade into industrial accidents, regulatory sanctions, or loss of accreditation, with broad consequences for public trust and economic stability.

The technological profile of modern laboratories further amplifies these challenges. Laboratory Information Management Systems (LIMS) centralize sensitive experimental and calibration data, IoT devices provide real-time monitoring of processes, and cloud infrastructures enable remote collaboration and scalable storage. However, each of these technologies introduces specific vulnerabilities: IoT devices often lack strong encryption, cloud solutions can create compliance risks related to GDPR and data residency, and LIMS software is prone to unpatched exploits. Moreover, laboratory personnel are usually trained as scientists and engineers rather than cybersecurity specialists, which increases the probability of human-factor-driven incidents. These conditions highlight the need for a structured methodology capable of addressing both technical and organizational risks, ensuring that laboratories can maintain the integrity of data flows while simultaneously meeting accreditation demands and responding to rapidly evolving cyber threats.

The importance of information risk analysis is well established in international practice, yet its application to ISO/IEC 17025 laboratories has distinctive features. Unlike other accredited organizations, such laboratories must not only secure sensitive data but also ensure metrological traceability, reproducibility of results, and compliance with strict audit procedures. This dual requirement places them at the intersection of quality management and information security, demanding hybrid methods that combine qualitative assessments with quantitative precision. Furthermore, the international character of calibration and testing services means that laboratories often exchange information across borders, which introduces additional complexities related to harmonization of cybersecurity requirements, legal frameworks, and data protection regimes.

The aim of this study is therefore to propose and validate a hybrid methodological framework that integrates probability–impact matrices with the Common Vulnerability Scoring System (CVSS) in order to generate balanced, reproducible, and audit-friendly risk assessments for laboratories. The novelty of the research lies in adapting well-known information risk analysis tools to the specific environment of ISO/IEC 17025 compliance, where both technical vulnerabilities and human factors play equally critical roles.

The article is structured as follows: Section 2 describes the object and subject of research, while Section 3 formulates the main target of the study. Section 4 provides a review of the scientific literature and relevant standards, with particular attention to hybrid approaches in risk assessment. Section 5 presents the methodological framework, including integration of ISO/IEC 27005 principles with practical

scoring models. Section 6 reports the results of the case study and interprets them under different scenarios. Finally, the conclusion summarizes the key findings, compares ISO/IEC 17025 with other accreditation standards, and outlines future directions for adaptive risk management.

2. Object and subject of research

The object of this research is the information infrastructure of testing and calibration laboratories operating in compliance with the ISO/IEC 17025:2017 standard. These laboratories represent complex socio-technical systems where human, organizational, and technological elements are tightly interconnected. The technological dimension includes Laboratory Information Management Systems (LIMS), IoT-based measurement sensors, remote data storage services, and cloud platforms. Together, these components create an integrated environment that enables efficient laboratory workflows, while at the same time exposing the laboratory to multiple categories of information risks.

The subject of the research is the set of processes, methods, and control mechanisms related to the identification, assessment, and management of information risks within ISO/IEC 17025-accredited laboratories. Specifically, the study focuses on the interaction between laboratory digital infrastructures and cybersecurity requirements, investigating how vulnerabilities emerge from outdated systems, insecure network configurations, and insufficient personnel awareness. The subject also includes methodological aspects — risk analysis techniques that combine qualitative (risk matrices, expert evaluations, interviews) and quantitative (statistical models, CVSS) approaches.

Thus, the object of the research is the information environment of the ISO/IEC 17025-compliant laboratory as a socio-technical system, while the subject is the methodological and practical framework of information risk analysis within this environment.

3. Target of research

The target of the research is the development of a structured, hybrid approach for information risk analysis that ensures both compliance with ISO/IEC 17025 requirements and the operational resilience of laboratories in a dynamic digital environment. The study aims to design a methodological framework that systematically identifies critical risks, evaluates their probability and impact, and proposes effective mitigation strategies aligned with international standards such as ISO/IEC 27001/27005, NIST SP 800-30, and ENISA guidelines [7] [8].

More specifically, the research seeks to achieve the following objectives:

- Identification of risks – to determine key categories of information risks in ISO/IEC 17025 laboratories, including technological vulnerabilities (e.g., unpatched LIMS, insecure IoT communication, weak access control), organizational shortcomings (e.g., lack of network segmentation, insufficient process standardization), and human factors (e.g., low staff awareness).
- Methodological integration – to adapt a hybrid risk assessment methodology, ensuring that the limitations of purely descriptive or purely numerical models are overcome through a balanced combination of qualitative and quantitative tools.
- Mitigation measures – to propose a structured set of technical and organizational controls that reduce vulnerabilities and create long-term resilience by embedding information risk management into the quality management system of the laboratory.
- Accreditation alignment – to demonstrate how effective information risk management directly supports laboratory credibility, reliability, and international recognition in accordance with ISO/IEC 17025 accreditation criteria.

The ultimate target is to strengthen the capability of laboratories to proactively detect, evaluate, and mitigate information risks. By achieving this, the research contributes to the broader scientific and

practical agenda of securing laboratory infrastructures, protecting sensitive data, and maintaining compliance with international standards.

4. Literature analysis

The scientific literature demonstrates that information risk management has become one of the key determinants of organizational resilience in the digital era [12]. A wide range of methodologies has been developed, each reflecting different perspectives on how to identify, assess, and mitigate risks. Classical approaches such as the Risk Matrix provide a simple and intuitive tool for visualizing the relationship between probability and impact, although they lack quantitative precision [13]. The FMEA (Failure Mode and Effects Analysis) methodology emphasizes identifying failure points and prioritizing them based on severity, likelihood, and detectability [14]. Bayesian networks offer a probabilistic perspective, enabling the modeling of dynamic risk scenarios where multiple factors interact [16].

Organizationally oriented models such as OCTAVE place emphasis on asset criticality and business context, thereby aligning risk analysis with strategic objectives. Furthermore, the ISO/IEC 27005 methodology provides a structured framework fully compatible with information security management systems (ISMS), while NIST SP 800-30 offers a practical guide widely applied in international practice [2]. Recent guidelines by ENISA and ILAC emphasize the integration of cybersecurity risk management into laboratory accreditation frameworks, highlighting the role of LIMS and IoT security as emerging priorities.

In addition to these widely recognized models, scholars underline the importance of combining strategic, organizational, and technological viewpoints. For example, risk communication theory emphasizes not only technical identification of threats but also the ability of institutions to disseminate information effectively across all organizational levels, ensuring that decision-makers and practitioners share a common understanding of vulnerabilities. This is particularly relevant for laboratories, where scientists, IT specialists, and quality managers must coordinate their roles within a single framework.

Emerging approaches are also expanding the methodological landscape. Artificial intelligence and machine learning are increasingly applied to detect anomalies in laboratory data flows and to forecast the probability of cyber incidents with higher accuracy. Big data analytics enables the processing of large volumes of logs in real time, identifying hidden risk patterns that traditional methods might overlook. Cloud-native security concepts and the “Zero Trust” model are gaining momentum, requiring continuous verification of users and devices, which is particularly relevant in laboratories where IoT devices and remote access channels are widely employed [10]. The literature also suggests that combining these emerging tools with classical frameworks such as ISO/IEC 27005 can produce methodologies that are not only more accurate but also better aligned with the practical requirements of accreditation audits.

Recent studies broaden this perspective. Shameli-Sendi et al. [17] developed a taxonomy of information security risk assessment methods, highlighting the diversity of qualitative and quantitative tools and the importance of methodological completeness. Wangen, Snekkenes, and Hallstensen [18] proposed a framework for measuring the comprehensiveness of risk assessment models, stressing that hybrid methods achieve greater accuracy in dynamic infrastructures such as laboratories. Spring, Hatleback, and Householder [19] analyzed vulnerability disclosure timelines, demonstrating that delayed updates substantially increase the attack surface — a finding consistent with the present research on unpatched LIMS systems. Similarly, ENISA’s Cybersecurity Threat Landscape 2023 report [20] identifies IoT and cloud ecosystems as primary sources of emerging laboratory risks, echoing the significance of weak segmentation and access control. Zhou, Sun, and Yang [21] proposed Bayesian-network-based models for industrial IoT environments, while Kure, Islam, and Razzaque [22] advocated for an integrated cyber-physical risk management model, underscoring the socio-technical nature of laboratories where human, organizational, and technological factors converge.

What emerges from this body of literature is a strong consensus: no single method can fully capture the complex interplay of threats in laboratory environments. Instead, effective risk management depends on hybrid models that integrate qualitative intuition, quantitative rigor, and adaptive mechanisms driven by technological innovation. This recognition forms the basis for the present study, which aims to tailor such hybrid methodologies specifically to ISO/IEC 17025 laboratories, where both technical and accreditation-related requirements converge in unique ways.

5. Methodological framework

The methodological framework of this study is based on a hybrid model that integrates both qualitative and quantitative approaches.

- Risk Matrix in ISO/IEC 27005 Context – intuitive mapping of probability and impact.
- Common Vulnerability Scoring System (CVSS) – numerical scoring for comparability.
- Integration of methods – combination of visualization and precision.
- Supporting processes – asset inventory, threat modeling, risk prioritization, control measure selection.

This integrated approach balances accessibility and technical precision, suitable for ISO/IEC 17025 laboratories.

While the preceding section outlined the conceptual basis of the hybrid model, the following paragraphs provide a more detailed, step-by-step description of its practical application in ISO/IEC 17025 laboratories, accompanied by illustrative examples.

Asset Inventory

Asset inventory represents the initial stage, where all digital and physical resources of the laboratory are systematically classified. According to ISO/IEC 27005, the purpose of asset inventory is to identify weak points and define their criticality. Assets include hardware (servers, workstations, IoT sensors), software (LIMS platforms, data analytics tools), data (sensor outputs, calibration results), and services (cloud storage and collaboration platforms).

Practical example:

In one ISO/IEC 17025-accredited laboratory, the asset inventory revealed:

- X-type servers – storing calibration data and requiring 24/7 availability;
- Y-type IoT sensors – continuously transmitting temperature and pressure data;
- Z cloud platform – used for archiving experimental results, but requiring additional controls for GDPR compliance.

Such detailed inventory allows laboratories to determine which assets require strict protection and which are less critical.

Risk Identification

Risk identification involves discovering potential threats and vulnerabilities that may affect the confidentiality, integrity, and availability of assets. This process typically combines interviews, technical audits, network traffic analysis, and document reviews.

Practical example:

During a security audit, the following issues were identified:

- The LIMS system operated on an outdated version known to contain publicly disclosed vulnerabilities;
- IoT sensors were transmitting data without encryption, making them susceptible to interception;
- Employees used the same passwords across multiple systems.

This illustrates how risks can emerge from both technological weaknesses and human factors.

Risk Assessment

In this stage, each identified risk is evaluated in terms of probability and impact. Both a probability–impact matrix and the Common Vulnerability Scoring System (CVSS) are applied. Together, these tools provide both a visual overview and a precise numerical evaluation.

Practical example:

- Unencrypted IoT communication was rated: probability = 3 (monthly occurrence), impact = 4 (data compromise), total score = 12 → medium risk.
- Outdated LIMS version was rated: probability = 4, impact = 5, total score = 20 → high risk.

Such assessments enable management to prioritize those threats that pose the greatest danger.

Risk Prioritization

Risk prioritization involves comparing the results of the assessment and establishing a final ranked list of risks. The most critical risks are addressed first, ensuring resources are allocated effectively. Composite indicators (Probability × Impact) or CVSS scores are commonly used.

Practical example:

The prioritization process in the laboratory produced the following order:

1. Unpatched LIMS system – high risk (score 20).
2. Low staff cybersecurity awareness – high risk (score 20).
3. Weak cloud access control – high risk (score 15).
4. Lack of network segmentation – high risk (score 16).
5. Unencrypted IoT communication – medium risk (score 12).

This structured prioritization helps the laboratory focus first on issues that are most likely to jeopardize accreditation and data integrity.

Control Measures

Control measures are the final stage, where both technical and organizational safeguards are selected to mitigate risks. This step often relies on the ISO/IEC 27001 Annex A control set, as well as recommendations from NIST and ENISA.

Practical example:

- For the unpatched LIMS platform – an automated patch management system was introduced, checking for updates weekly.
- For IoT sensors – TLS encryption was implemented and the devices were placed in a dedicated VLAN.
- For employees – quarterly awareness trainings were conducted on phishing, password management, and safe use of collaboration tools.
- For cloud access – multi-factor authentication (MFA) and role-based access control (RBAC) were enforced.

By implementing such measures, laboratories significantly reduce risks stemming from both technological vulnerabilities and human behavior.

6. **Research section**

The methodological framework described above was applied in practice to an ISO/IEC 17025–compliant testing laboratory. Using the previously defined hybrid approach (probability–impact matrix combined with CVSS scoring), risks were identified through staff interviews, technical audits, and analysis of network traffic and access logs.

The application of this methodology enabled the prioritization of risks and the development of mitigation strategies, ensuring both technical accuracy and organizational alignment. The following section summarizes the key findings.

This methodological combination ensures accuracy in reflecting both technical vulnerabilities and organizational weaknesses, providing a comprehensive picture of the laboratory's risk landscape.

The rationale for selecting the hybrid approach that combines the Risk Matrix and CVSS lies in the complementary nature of these methods. While the Risk Matrix offers a clear and intuitive visualization of risks based on probability and impact, CVSS provides a standardized, numerical evaluation that enables comparability across different types of vulnerabilities. This combination ensures that both decision-makers without deep technical expertise and cybersecurity professionals can work within a unified framework. Furthermore, the proposed methodology could be supported by specialized software tools for risk analysis, which would automate asset inventory, generate risk scores, and simulate mitigation effects. Such automation not only increases accuracy but also reduces the burden on laboratory staff, ensuring consistency in applying ISO/IEC 17025 requirements.

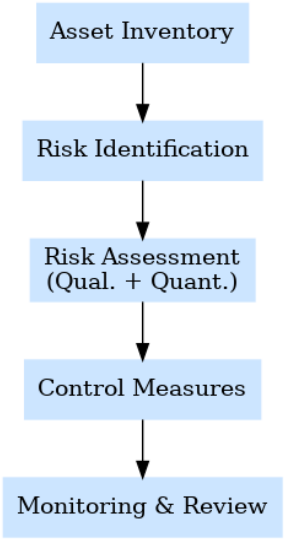

Figure 1. Risk Analysis Process Model for ISO/IEC 17025 Laboratories.

Identification of Major Threats

A study was conducted in a laboratory compliant with the ISO/IEC 17025 standard. Following the identification of risks, we assessed the likelihood of occurrence (on a scale from 1 to 5) and the impact effect (also on a scale from 1 to 5), based on the following assumptions:

- **Likelihood (P):**
  - *P = 1* — very low; the threat occurs approximately once per year or is nearly negligible.
  - *P = 5* — very high; the threat may occur frequently, on a monthly basis.
- **Impact (I):**
  - *I = 1* — negligible damage; minimal influence on operations.
  - *I = 5* — critical damage; complete data loss and potential loss of accreditation.

The risk level was calculated as R = Risk Level (R) = Probability (P) × Impact (I), with possible values ranging from 1 to 25. The results were categorized as follows:

- **1–7 → Low risk**
- **8–14 → Medium risk**
- **15–25 → High risk**

Table 1. Top 5 identified risks and their assessment

№	Risk Description	Likelihood (1–5)	Impact (1–5)	Risk Level (P×I)	Priority
1	Unpatched version of LIMS platform	4	5	20	High
2	Insecure communication of IoT sensors	3	4	12	Medium
3	Low cybersecurity awareness among personnel	5	4	20	High
4	Weaknesses in cloud service access control	3	5	15	High
5	Absence of network segmentation	4	4	16	High

The risk matrix analysis revealed five predominant risks (see Table 1 and Fig. 2). Among them, the most critical are the unpatched version of the LIMS platform and the low level of cybersecurity awareness among personnel, both of which were assigned a high-risk score of 20. Other significant challenges include deficiencies in cloud service access control mechanisms, the lack of logical network segmentation, and the insecure communication of IoT sensors.

A more detailed interpretation of the results reveals that each identified risk has distinct implications for ISO/IEC 17025 accreditation. For example, an unpatched LIMS platform threatens the integrity of measurement data, potentially leading to invalid test results and non-conformities during audits. Low cybersecurity awareness among personnel increases the likelihood of social engineering attacks, which may compromise confidentiality and damage client trust. Weak cloud access control poses a direct risk to compliance with data protection regulations, while the absence of network segmentation makes laboratories particularly vulnerable to cascading failures once an intrusion occurs. Compared to these factors, insecure IoT communication, although classified as medium risk, may escalate rapidly if combined with other vulnerabilities. These insights underline the necessity of treating risk management not as an isolated technical task but as a strategic process integrated into the quality assurance system.

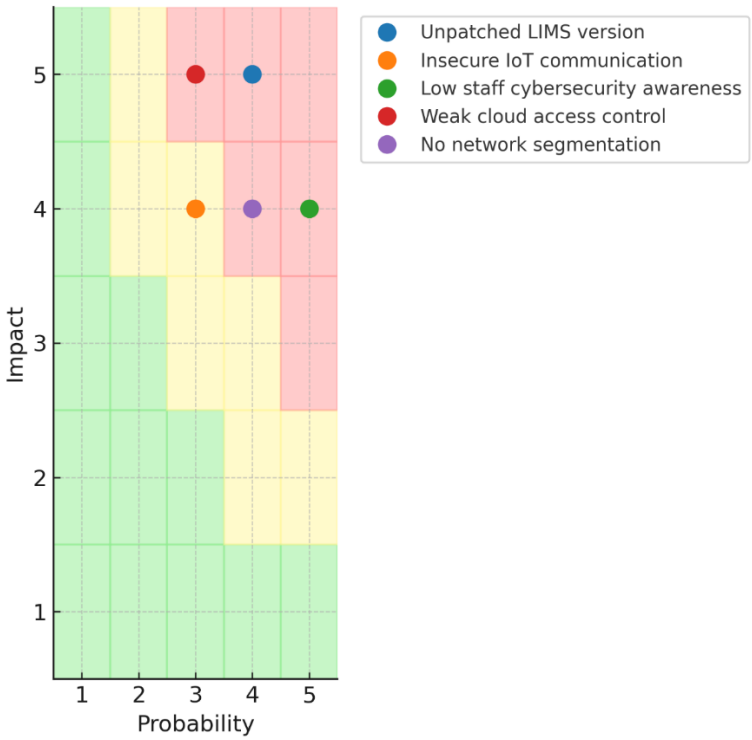

Figure 2. Probability–Impact risk matrix of key cybersecurity threats in laboratory information systems.

1. Research Results

The application of the methodology led to the identification of five primary risks:

1. Unpatched versions of the LIMS platform.
2. Insecure communication channels in IoT sensors.
3. Low cybersecurity awareness among laboratory personnel.
4. Weaknesses in cloud access control.
5. Lack of logical network segmentation.

The probability–impact analysis revealed that the most critical risks are the unpatched LIMS system and insufficient staff awareness, both assigned a high-risk score of 20. Weak cloud access control and lack of segmentation also represent high-priority risks, while insecure IoT communications were classified as medium risk.

Each identified risk has distinct implications for accreditation. For instance, an unpatched LIMS platform threatens data integrity and may cause audit non-conformities; low staff awareness increases susceptibility to social engineering; weak cloud access control jeopardizes compliance; lack of segmentation enables cascading failures; insecure IoT communication, although medium risk, may escalate rapidly if combined with other vulnerabilities.

These insights underline that risk management should not be treated as an isolated technical task but as a strategic process integrated into the quality assurance system.

Additional Scenario-Based Analysis

Beyond the core findings, several scenarios illustrate how risks may escalate if not addressed in a timely manner. For instance, outdated IoT firmware can accumulate vulnerabilities that allow attackers to inject false measurement data. Non-compliance of cloud providers with GDPR may create legal and reputational damage. Shadow IT introduces unmonitored data flows that erode traceability.

These examples highlight that risks extend beyond the laboratory's technical perimeter, intertwining technological and human factors. They reinforce the need for continuous monitoring, staff awareness, and integrated governance as part of the laboratory's quality management system.

7. Conclusion

This study has examined information risk analysis in ISO/IEC 17025–accredited laboratories and demonstrated that managing risks in such environments requires a hybrid methodology integrating both qualitative and quantitative approaches. Unlike typical enterprises, laboratories operate under strict accreditation rules where even minor failures in data integrity can compromise measurement traceability, reproducibility, and international credibility. This unique context amplifies the significance of cybersecurity vulnerabilities and makes systematic risk management inseparable from quality management processes.

The research confirmed that the most critical threats include outdated and unpatched LIMS platforms, insufficient staff awareness of cybersecurity practices, weaknesses in cloud access control, insecure IoT communication, and lack of network segmentation. Among these, ineffective patch management and inadequate personnel training were identified as the highest-priority risks because they not only increase exposure to attacks but also jeopardize compliance during accreditation audits. Importantly, these risks were shown to arise not only from technological shortcomings but also from organizational and human factors, underlining the socio-technical nature of the problem.

By applying a hybrid framework that combines probability–impact analysis with the Common Vulnerability Scoring System (CVSS), the study provided a balanced and reproducible method of risk assessment. The qualitative component (risk matrix) ensured that managers and auditors without technical expertise could interpret the results, while the quantitative component (CVSS) enabled precise prioritization and comparability across vulnerabilities. This dual approach reduces subjectivity, improves transparency, and supports decision-making at both technical and managerial levels.

Beyond the direct findings, scenario-based analysis demonstrated how unaddressed risks can escalate. For example, unpatched LIMS may lead to compromised calibration data, shadow IT introduces uncontrolled data flows that erode traceability, and non-compliance of cloud providers with GDPR or similar regulations exposes laboratories to legal and reputational harm. These scenarios illustrate that risk management is not a one-time exercise but a dynamic process requiring continuous monitoring, adaptation, and integration into laboratory governance.

From a comparative perspective, ISO/IEC 17025 laboratories face challenges that differ from other accreditation frameworks. Medical laboratories accredited under ISO/IEC 15189 prioritize confidentiality of patient data, while inspection bodies under ISO/IEC 17020 focus on impartiality of assessment processes. By contrast, ISO/IEC 17025 laboratories must simultaneously ensure metrological traceability, data reproducibility, and information security. This creates a uniquely complex risk landscape that demands multidimensional approaches, blending technical controls, organizational safeguards, and cultural awareness.

The practical implications of the research are significant. Laboratories that implement hybrid risk management frameworks do not merely comply with accreditation requirements but also build long-term resilience against evolving threats. Essential control measures include automated patch management, strict network segmentation, multi-factor authentication, encryption of sensitive information, and continuous staff training. However, resilience cannot rely solely on technical fixes; it requires embedding a risk-aware culture into the laboratory's daily operations and aligning information security with overall quality management objectives.

Looking forward, the study highlights several directions for further development. Artificial intelligence and predictive analytics could enhance early detection of vulnerabilities, while machine learning techniques may support anomaly detection in laboratory data flows. Integration of "Zero Trust" architectures and cloud-native security tools would further reduce dependency on perimeter defenses, which are increasingly insufficient in distributed environments. Finally, international cooperation

between accreditation bodies, laboratories, and cybersecurity agencies can promote the exchange of best practices, improve regulatory alignment, and accelerate the adoption of proactive security models.

In conclusion, effective information risk management in ISO/IEC 17025 laboratories must be proactive, hybrid, and continuously adaptive. Only by combining technical precision with organizational awareness can laboratories safeguard confidentiality, integrity, and availability of their data, uphold accreditation, and reliably contribute to global measurement and calibration systems. Strengthening these practices has both micro-level benefits for individual laboratories and macro-level importance for industrial safety, scientific credibility, and societal trust.

References:

1) ISO/IEC 17025:2017 – *General requirements for the competence of testing and calibration laboratories*.

2) ISO/IEC 27005:2018 – *Information security risk management*.

3) NIST SP 800-30 Rev.1 – *Guide for Conducting Risk Assessments*.

4) Smith, J., et al. (2021). *Security challenges in LIMS platforms*. *Journal of Laboratory IT Security*, 15(3), 45–56.

5) ILAC (2020). *ISO/IEC 17025 Implementation Guide*. International Laboratory Accreditation Cooperation.

6) FIRST.org (2019). *Common Vulnerability Scoring System v3.1: Specification Document*.

7) Menabde, T., Otkhozoria, N., & Otkhozoria, V. (2024). Use of the theory of measurement uncertainty in procedures for data processing and results obtained by checking-calibration gas flow meters. *International Science Journal of Engineering & Agriculture*, *3*(2), 40–46. https://doi.org/10.46299/j.isjea.20240302.03

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

9) Azmaiparashvili, Z., & Otkhozoria, N. M. (2016). Identification of Two Sorts of Processes and Determining of Their Differences Criteria. Journal of Technical Science and Technologies,. https://doi.org/10.31578/jtst.v5i2.106

10) 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

11) 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

12) **I**SO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, Geneva, 2022.

13) Benaim, E., & Humphreys, P. (2020). *Risk management standards and guidelines in laboratories: Integration with ISO/IEC 17025.* Journal of Risk Research, 23(6), 763–779. https://doi.org/10.1080/13669877.2019.1673805

14) Disterer, G. (2013). *ISO/IEC 27000, 27001 and 27002 for information security management.* Journal of Information Security, 4(2), 92–100. https://doi.org/10.4236/jis.2013.42011

15) ENISA (2022). *Cybersecurity for SMEs and laboratories: Practical guidelines for risk assessment and mitigation.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu

16) Zhang, J., Wang, L., & Zhang, H. (2021). *IoT security risk assessment based on CVSS and Bayesian networks.* Computers & Security, 106, 102270. https://doi.org/10.1016/j.cose.2021.102270

17) Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

18) Wangen, G., Snekkenes, E., & Hallstensen, C. (2018). A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 17(6), 681–699. https://doi.org/10.1007/s10207-018-0415-0

19) Spring, J. M., Hatleback, E., & Householder, A. D. (2021). Time to patch: The relative effectiveness of vulnerability disclosure timelines. IEEE Security & Privacy, 19(5), 27–37. https://doi.org/10.1109/MSEC.2020.3048416

20) ENISA (2023). Cybersecurity Threat Landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

21) Zhou, Y., Sun, Y., & Yang, S. (2021). Risk assessment model of industrial IoT systems based on attack graph and Bayesian networks. Future Generation Computer Systems, 119, 105–118. https://doi.org/10.1016/j.future.2021.01.025

22) Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), 898. https://doi.org/10.3390/app8060898