International Journal of Innovative Technologies in Social Science

e-ISSN: 2544-9435

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw,
Poland 00-773
+48 226 0 227 03
editorial_office@rsglobal.pl

ARTICLE TITLE	CYBERSECURITY LAW OF MONGOLIA: DEFINITION, IMPLEMENTATION, AND ITS IMPACT ON NATIONAL SECURITY
DOI	https://doi.org/10.31435/ijitss.4(48).2025.4298
RECEIVED	22 October 2025
ACCEPTED	16 December 2025
PUBLISHED	23 December 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

CYBERSECURITY LAW OF MONGOLIA: DEFINITION, IMPLEMENTATION, AND ITS IMPACT ON NATIONAL SECURITY

Munkhjargal Bayanjargal
Founder, Nomad Cyber Defense LLC; PhD Candidate, National Defense University, Ulaanbaatar, Mongolia

Munkhtsetseg Erdenebulgan
Senior Lecturer; PhD Candidate, National Defense University, Ulaanbaatar, Mongolia

Byambadorj Dondogmegd
Doctor (PhD), Senior Lecturer, University of Science and Technology, Ulaanbaatar, Mongolia

Odmaa Luvsan
Doctor (PhD), Associate Professor, Senior Lecturer, National Defense University, Mongolia

ABSTRACT

The Cyber Security Law enacted in Mongolia in 2022 is the initial comprehensive legal framework aimed at safeguarding the cyber environment, yet there are uncertainties and deficiencies in its enforcement.
This study seeks to examine the terminology, risk assessment, and regulatory methodology for information security audits under the Mongolian Cyber Security Law, assess their impact on national security, and compare and evaluate them against international practices.
The analysis involved a review of relevant Mongolian laws, regulations from the Ministry of Electronic Development, and information from authorized entities, along with a quantitative and qualitative comparison of the implementation levels of information security audits and cybersecurity risk assessments.
Additionally, comparisons were made with international standards such as ISO/IEC 27001, ISO/IEC 27005, NIST SP 800-30, ENISA, and the cybersecurity practices of countries like Estonia, Singapore, and South Korea. While Mongolia has a foundational legal framework for cybersecurity, significant shortcomings persist in its execution. To address these issues, it is imperative to refine terminology, establish a national audit body, standardize risk assessment and audit methodologies in alignment with global standards, establish a centralized monitoring and inspection system, develop a national centralized platform, and enhance human resource capabilities. These measures are crucial for safeguarding national security and ensuring the resilience of Mongolia's cyber environment.

KEYWORDS

Cybersecurity Law, Terminology, Audit, Risk Assessment

CITATION

Munkhjargal Bayanjargal, Munkhtsetseg Erdenebulgan, Byambadorj Dondogmegd, Odmaa Luvsan (2025) Cybersecurity Law of Mongolia: Definition, Implementation, and Its Impact on National Security. *International Journal of Innovative Technologies in Social Science*. 4(48). doi: 10.31435/ijitss.4(48).2025.4298

Introduction

In recent years, the rapid advancement of information and communication technologies has opened up new opportunities for the country's social, economic, and public administration systems, while also presenting numerous threats and challenges. A prime example of this is the issue of cybersecurity, which is not only a technical concern but also involves legal and policy-level regulations.

The Cyber Security Law enacted in Mongolia in 2022 marked the country's first comprehensive national legal framework in this domain. The utilization of the term "cyber" directly from English aligns with global standards, though there is ongoing scholarly discourse on whether the term "electronic" might be more suitable. This semantic ambiguity poses not only linguistic challenges but also risks undermining the efficacy of law enforcement and policy implementation.

Furthermore, the law mandates annual cybersecurity risk assessments and biennial information security audits, yet lacks detailed specifications regarding their purpose, content, and execution methods. Consequently, practical observations indicate that these activities are often carried out as routine services rather than delivering tangible organizational benefits, thereby compromising national security.

Hence, the objective of this research article is to:

1. Explore the theoretical underpinnings of terminology usage in Mongolian cybersecurity legislation,
2. Identify methodological deficiencies in the regulation of cybersecurity risk assessments and information security audits,
3. Examine the actual implications of these shortcomings on national security and conduct a comparative analysis with international practices,
4. Propose recommendations for enhancing the legal framework further.

Terminology Issues (Theoretical Foundation)

The term "cyber" has its origins in cybernetics, a concept first developed by Norbert Wiener in the 1940s. It has been widely used since the 1980s with the advancement of information technology. Today, "cyber security" is a common term found in international legal documents and research literature, encompassing various information systems, networks, and digital environments.

When translating into Mongolian, using the direct English term "cyber" is an example of incorporating foreign words into the language. However, considering Mongolian language traditions and semantics, it may be more appropriate to use the term "electronic" for better understanding and compatibility. "Electronic security" pertains to safeguarding communication and information systems, while "cyber security" has a broader scope, covering national digital environments, artificial intelligence, automation, and virtual networks.

The distinction between the terms "cyber" and "electronic" is crucial at the legislative level for practical implementation. Using "cyber" can encompass a broad range of theories but may lead to ambiguity and inconsistency in everyday use by citizens and organizations. Conversely, "electronic" is more aligned with common usage but may not adhere to international standards. This lack of clarity in terminology has negative implications for law enforcement. It can result in varying interpretations and implementations of legislation, as well as reliance on service providers' discretion and knowledge, hindering monitoring and analysis efforts.

Therefore, it is believed that accurately defining and optimizing the use of terms is crucial not only from a linguistic perspective but also as a foundational requirement for the effective implementation of cyber environment policies and legal frameworks. This is highlighted in Article 4 of the Law on Cyber Security, which provides definitions for key legal terms:

4.1.9. "cyber security risk assessment" refers to a specialized process aimed at determining the likelihood of cyber security incidents, threats, vulnerabilities, potential consequences, and measures for risk mitigation and prevention;

4.1.10. "information security audit" involves an independent, external evaluation conducted by professionals to assess compliance with cybersecurity laws, regulations, and standards.

The discrepancy in the usage of the term "cyber security" in Mongolian legislation compared to "information security" and "electronic security" in international contexts can lead to confusion and challenges in practical application.

Current Status of Legal Regulation

The Cyber Security Law of Mongolia is the first comprehensive legal regulation aimed at ensuring information security in the cyber environment at the national level. One of the key provisions of the law requires organizations to conduct an annual cybersecurity risk assessment and an information security audit every two years.

However, the implementation of this regulation has several weaknesses, including:

1. Lack of methodological clarity:

- The law does not specify detailed methodologies, standards, or specific criteria for conducting risk assessments and audits.
- Organizations are unsure about which standards and methodologies to follow for these activities, often relying on consulting service providers for guidance.
- This reliance on external providers can lead to ineffective assessments and audits that prioritize business interests over actual security.
- Without a clear methodology, organizations may not be able to ensure real security through assessments and audits, as some providers may focus solely on form filling and "reporting" rather than addressing genuine risks.

2. Inadequate monitoring and analysis:

- The process for monitoring and evaluating the execution of activities outlined in the law lacks clear definition.
- State agencies face challenges in conducting monitoring using the reports and audits from organizations.
- Ambiguous standards for risk assessment and audits place strain on technical and human resources and add complexity to operations. Without a proper risk assessment, organizations are unaware of their vulnerabilities and potential points of attack. Consequently, organizations holding critical information may be left vulnerable and at higher risk of attacks.

3. Policy and standard non-compliance:

- While periodic regulations like annual risk assessments and biannual audits are common business practices, they do not offer national security assurance.
- The current legal regulations do not completely align with international standards and best practices (ISO 27001, ISO 27005, NIST, ENISA guidance).
- Detailed methodological and criteria instructions found in international standards (ISO 27005, NIST SP 800-30, ENISA) are not fully reflected in Mongolian legal regulations.

4. Impact on National security:

- The absence of consistent standards and approaches for assessing risks and conducting audits greatly heightens the vulnerability of organizations to cyberattacks and data breaches, resulting in systemic vulnerabilities within the national information infrastructure.

These regulatory deficiencies compromise the integrity of essential government systems, raise the probability of cyber assaults, and jeopardize the digital aspect of national security with significant strategic implications. Consequently, organizations often rely on individual expertise and experience to deliver services, failing to ensure adequate cybersecurity safeguards at the national scale. A comparison table is used to illustrate the implementation and enforcement of cybersecurity laws in Mongolia, in relation to international standards such as ISO, NIST, ENISA, Estonia, Singapore, and South Korea. The table evaluates the extent of legal regulation, terminology usage, risk assessment and audit standards, monitoring and control measures, and human resource policies.

Table1. Comparative Analysis of Cybersecurity Law and International Practice

Country/ Standard	Terminology Cyber/Digital	Risk Assessment Standards	Audit Frequency	Monitoring & Oversight	Professional Workforce Policy	Characteristics	Assessment
Mongolia	"Cyber" (directly borrowed from English)	Detailed methodology lacking	Annually	Mechanism unclear	Weak training system	Lacks alignment with international standards	Weaknesses: Methodology and monitoring system inadequate; terminological ambiguity creates practical obstacles.
ISO	Cybersecurity	ISO/IEC 27005 (risk assessment)	ISO/IEC 27001 (management system)	ISMS internal/ external audit	Certification and accreditation system	Global standard, established practice	Features: Clear implementation standards (ISMS); Directly applicable to Mongolia.
NIST (USA)	Cybersecurity	NIST SP 800-30, SP 800-39	Organizational level, depending on sector	NIST Framework compliance audit	Training & Certification Programs (Cyber Corps, NICE)	In-depth methodology, government support	Features: Comprehensive risk assessment; Effective for policy-regulatory alignment in Mongolia.
ENISA (EU)	Cybersecurity	ENISA Risk Mgmt. Guidelines	Organizational level, sector-based	EU Cybersecurity Agency Framework oversight	Skills Framework + Training Guidance	Policy-strategic alignment focused	Features: Policy-standard-capacity coordination; Implementable as policy model in Mongolia.
Estonia	Cybersecurity (localized)	ISO + NIST integrated national methodology	Nationwide (for critical agencies)	CERT-EE oversight, Cyber Range training	Government-led training centers	E-Governance, digital citizenship model	Features: Centralized oversight and training; Model for strengthening Mongolia's digital government foundation.
Singapore	Cybersecurity (aligned with CSF)	National Cyber Risk Assessment Framework	Critical sectors — annually	Cybersecurity Agency+ (CSA) oversight	SkillsFuture, GovTech Academy	Advanced, centralized monitoring system	Features: Risk-based oversight; Suitable for Mongolia's critical infrastructure implementation.
South Korea	Cybersecurity / Information Security	KISA standards (ISO+NIST based)	Public agencies — annually	Korea Internet & Security Agency oversight	Government-organized extensive training programs	Unified ICT policy	Features: Strong government leadership; Model for improving inter-sectoral coordination in Mongolia.

- **ISMS** = Information Security Management System
- **CERT-EE** = Computer Emergency Response Team of Estonia
- **CSA** = Cybersecurity Agency (Singapore)
- **KISA** = Korea Internet & Security Agency
- **CSF** = Cybersecurity Framework

This table compares Mongolia's cybersecurity legal framework with international standards (ISO, NIST, ENISA) and best practices from Estonia, Singapore, and South Korea across key dimensions: terminology, risk assessment standards, audit frequency, oversight mechanisms, workforce development, and overall assessment.

The table indicates that in Mongolia, the concept is broad in theory, but in reality, it leads to uncertainty. Additionally, there are no specific standards and criteria for risk assessment and audit. The monitoring and evaluation system is ineffective and limited to reporting. There is a shortage of qualified personnel policies and a lack of government-backed specialized training programs.

Research Section

In this study, the Ministry of Electronic Development, Innovation, and Communications gathered data from 42 companies, including authorized legal entities for information security audits and cybersecurity risk assessments, and examined their services for risk assessment and audits.

- Methodology or concept.
- A comparative analysis was carried out by comparing prices.

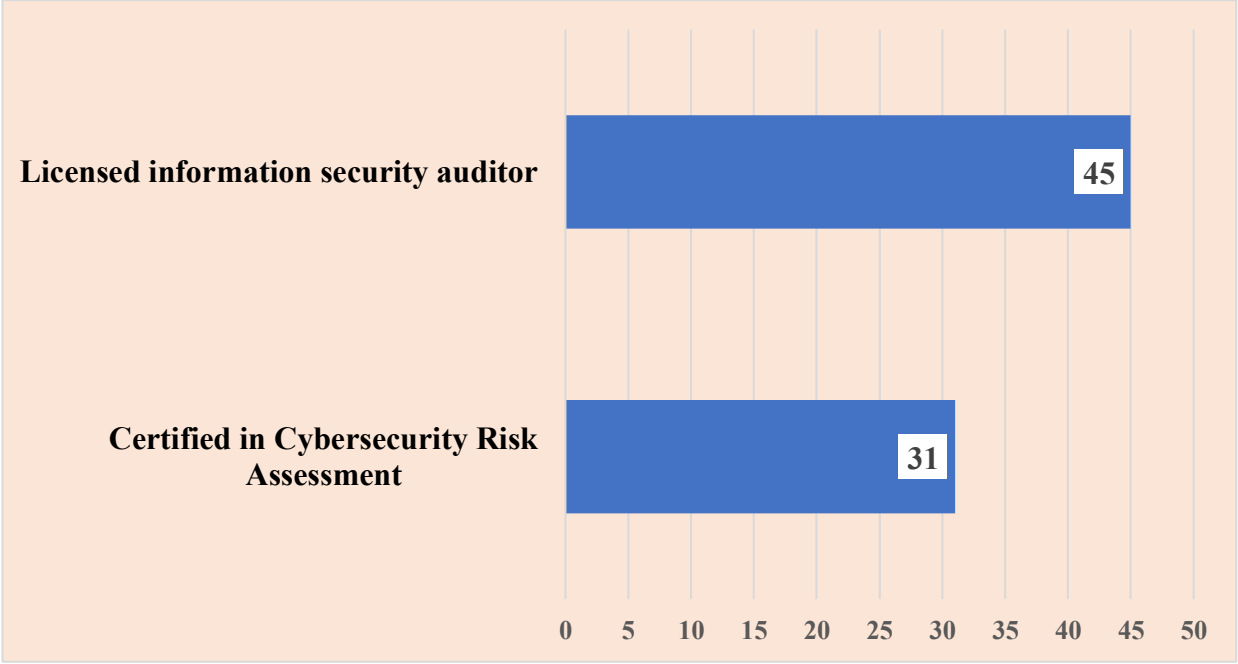

Fig. 1. *The range of approvals from the institutions surveyed.*

Out of the organizations surveyed, 31 have licenses to perform cybersecurity risk assessments, while 45 have licenses to perform information security audits. This suggests that while licenses for information security audits are more common, there are fewer organizations licensed to conduct cybersecurity risk assessments.

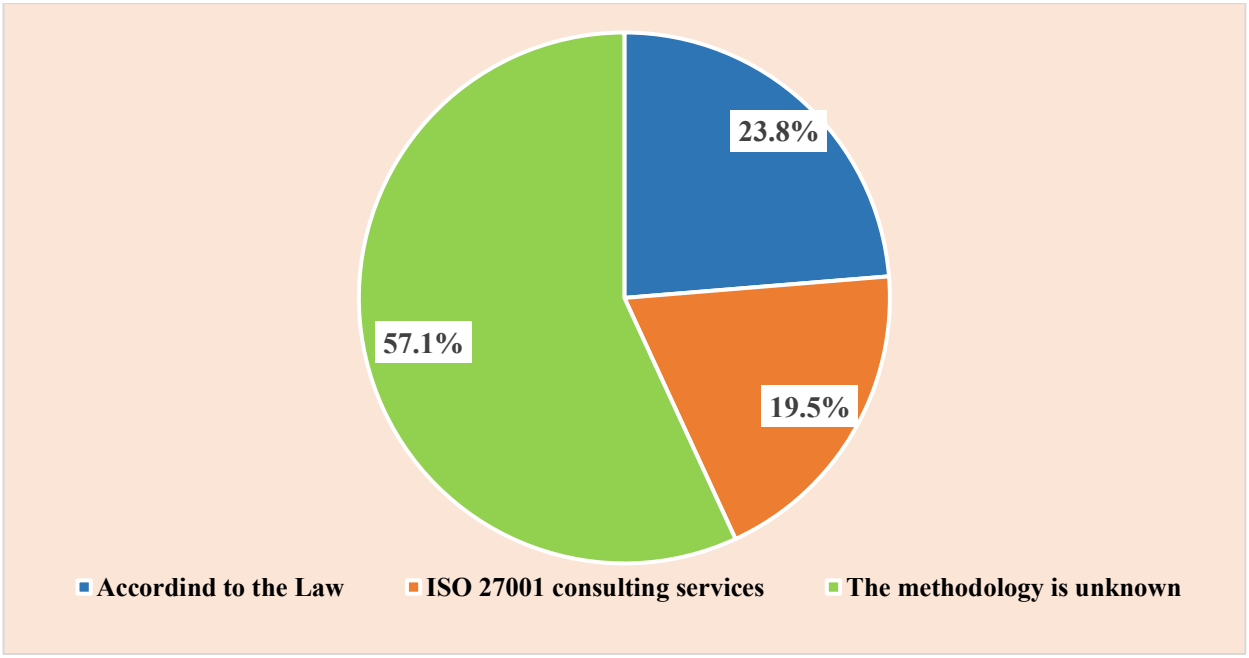

Fig. 2. *Structure of implementing an information security audit (categorized by method)*

The survey revealed that 23.8% of organizations carried out information security audits in compliance with regulations, 19.5% followed ISO/IEC 27001 consulting services, and the remaining 57.1% did not specify their approach. This suggests a lack of clarity in how organizations are implementing information security audits, highlighting the importance of aligning them with legal and international standards (Figure 2).

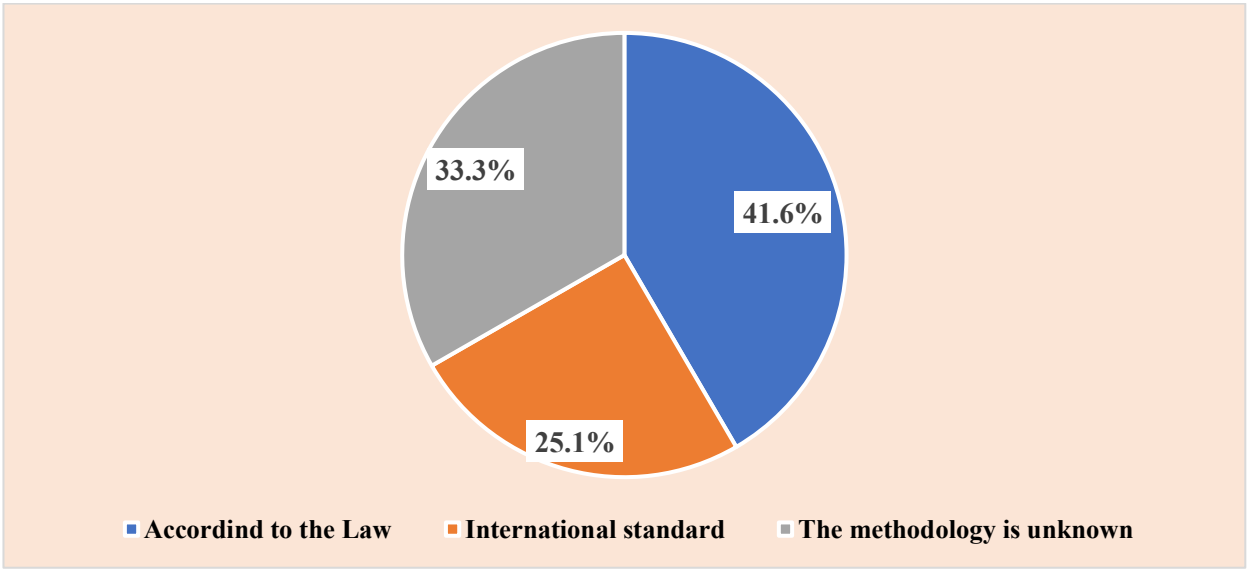

Fig. 3. *Cybersecurity risk assessment implementation framework (categorized by method)*

In terms of cybersecurity risk assessments implementation, 41.6% were carried out in compliance with the law, 25.1% followed international standards, and 33.3% did not specify their approach. This suggests that there is unevenness in the execution of risk assessments among organizations, highlighting that adherence to legal requirements and global standards is not yet at a satisfactory level (Figure 3).

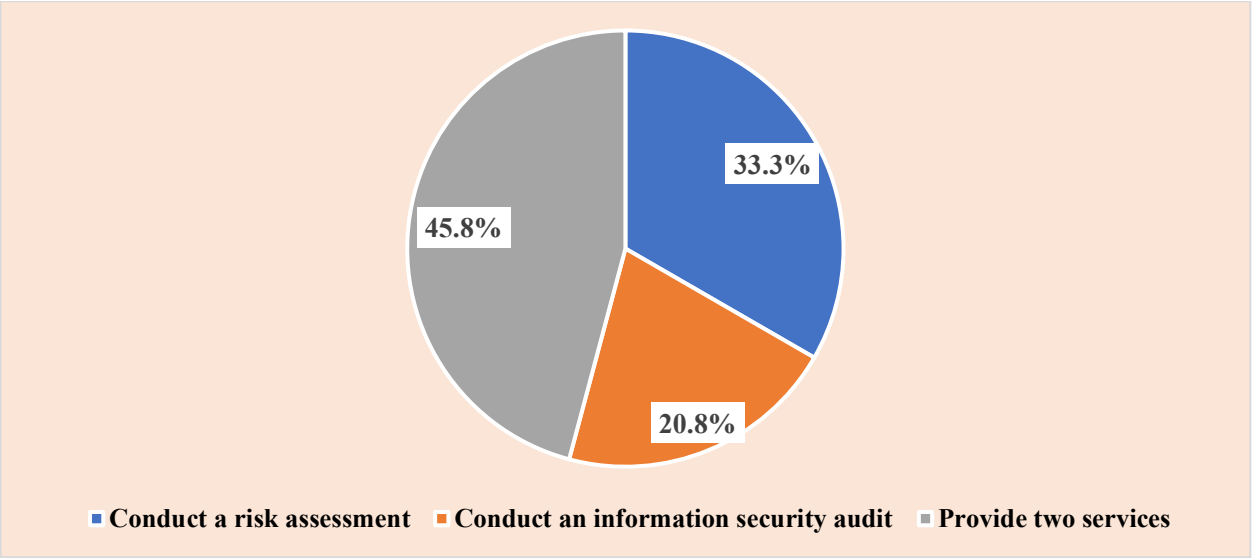

Fig. 4. *Competency structure of service providers*

When looking at the service capabilities of the organizations surveyed, 33.3% could only conduct risk assessments, 20.8% could only perform information security audits, and 45.8% were able to offer both services. This suggests that while many organizations can provide integrated services, there are still a considerable number with specialized capabilities (Figure 4).

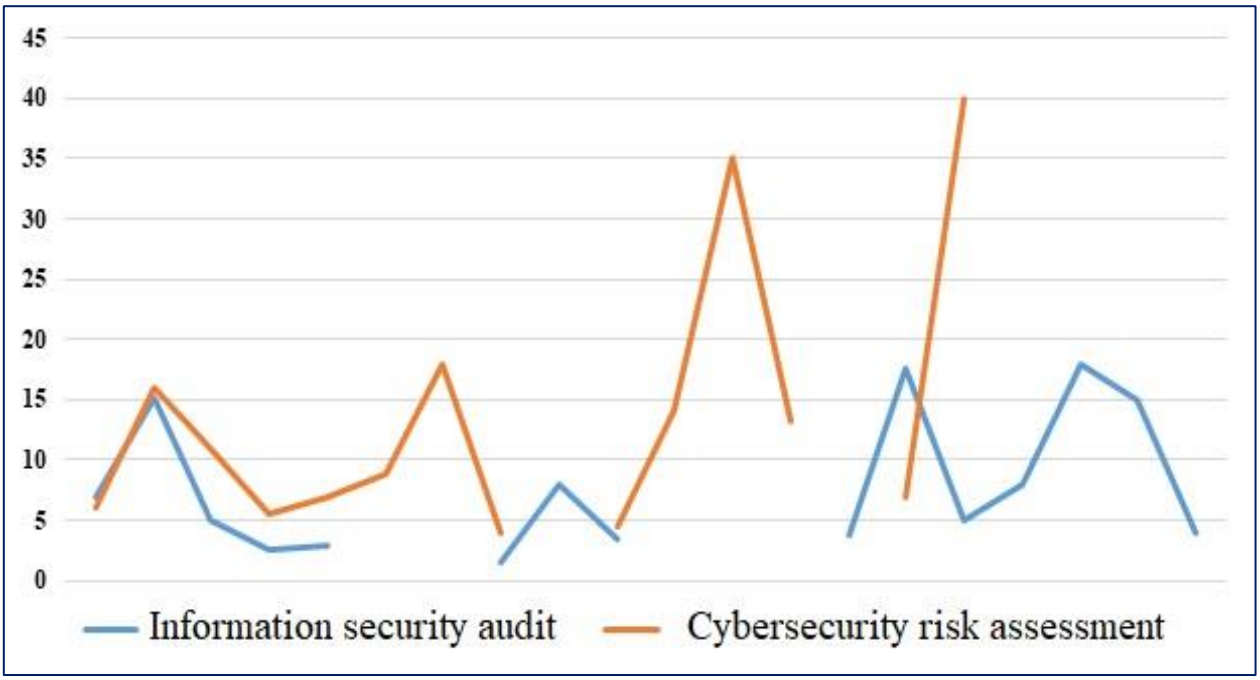

Fig. 5. *A comparison of prices for audit and risk assessment services for companies.*

When comparing the prices of information security audits and cybersecurity risk assessments offered by companies, it is evident that audit services generally have stable prices with minimal fluctuations, whereas risk assessment prices vary more widely and fluctuate at higher levels.

The analysis reveals that cybersecurity risk assessment prices typically fall within the range of 8-10 million tugriks for most companies, with some outliers charging significantly higher prices of 30-40 million tugriks, suggesting that certain market offerings are overpriced. This variation in pricing could be influenced by factors such as company characteristics, service scope, or organizational reputation. On the other hand,

information security audit services are priced at an average of 3-5 million tugriks, but there are instances where prices spike to 15-17.5 million tugriks, indicating anomalies that surpass the standard market rates. This disparity in pricing suggests inconsistencies in the information security audit services market.

These findings highlight the price fluctuations and pricing strategies within the industry, underscoring a potential lack of price standardization in the sector.

The Information Security Audit Oversight System:
Necessity, International Practices, and Mongolia's Current Situation

In Mongolia, the "Cyber Security Law" mandates annual risk assessments and biennial information security audits, but lacks a centralized monitoring system for overseeing these activities. Organizations follow their own approaches and rely on consulting service providers, leading to varying audit quality and outcomes, sometimes limited to superficial compliance checks. Consequently, there is insufficient aggregation of audit findings at a national level, hindering the development of cohesive government policies.

The failure to centralize the audit control system in a unified unit has negative impacts on national security, including insufficient risk assessment and effectiveness of audit results, inability to compare organization's information security levels, increased risk of cyber-attacks and data loss, and lack of basic data and statistics for national policy development. Therefore, centralizing information security audit control under a unified unit is justified.

Recommendation

This study highlights that the existing state and practical application of cybersecurity laws in Mongolia could potentially jeopardize national security. While legal frameworks have laid the groundwork for safeguarding information security at a national level, issues such as ambiguity in methodologies, deficiencies in monitoring and oversight, and lack of alignment with global standards diminish the efficacy of enforcement. To enhance national security and promote policy consistency, the following recommendations are proposed:

1. Standardize terminology: Clarify the definition of "cybersecurity" in line with international norms and consistently use it across legal texts to avoid confusion.
2. Establish a dedicated national entity: Revise the Cybersecurity Law to include provisions for establishing a "National Cybersecurity Audit Unit" responsible for approving audit methodologies, monitoring compliance, and ensuring the accuracy of audit reports.
3. Establish standardized risk assessment and audit methodologies: Legislation should include detailed methodologies and criteria for conducting risk assessments and information security audits, making them mandatory procedures. Localize international standards such as ISO/IEC 27001, ISO/IEC 27005, NIST SP 800-30, and ENISA guidance to align with national conditions.
4. Enhance monitoring and evaluation mechanisms: Create a centralized mechanism overseen by the state monitoring body to ensure the quality and effectiveness of risk assessments and audits conducted by organizations. Implement an automatic algorithm to verify the accuracy and compliance of audit reports, utilizing artificial intelligence to classify risk levels and predict national trends.
5. Align policies and practices: Update the frequency and content of policies and regulations to better align with national security requirements, going beyond the current business cycle considerations.
6. Establish a national centralized platform: Digitize and register audit and risk assessment reports conducted by organizations, providing access to state supervisory authorities. Integrate reports with an automated analysis (RegTech) solution.
7. Enhance training and knowledge development: Regularly provide training to organization management, information technology, and information security staff on risk assessment and audit methodologies. Offer certification programs to build a pool of internationally certified specialists, strengthening human resource capacity.

The establishment of legal regulations on cybersecurity in Mongolia is a positive development, but there are still significant deficiencies in practical implementation. To safeguard national security, it is essential to carry out information security audits and risk assessments in a coordinated manner at the international standard level. By implementing these measures, policy coherence and effectiveness can be enhanced, leading to a more stable cyber environment in Mongolia.

As there is no officially defined methodology for conducting cybersecurity risk assessments and information security audits in Mongolia, organizations are utilizing various international methodologies such as ISO/IEC 27005, NIST SP 800-30, ENISA, and ISO/IEC 27001, resulting in inconsistent implementation.

This lack of standardization hinders the ability to compare assessment quality and draw unified conclusions at the national level. Therefore, it is crucial to address these discrepancies by incorporating provisions in the Cyber Security Law and outlining the methodology in the accompanying regulations. Table 2 below outlines the disparities in purpose, implementation process, status, methodology, scope, and outcomes between information security audits and ISO/IEC 27001 certification.

Table 2. Information security audit vs. ISO/IEC 27001 Certification differences and distinctions

Comparison	Information Security Audit	ISO/IEC 27001 Certification
Purpose	To examine the implementation of an organization's information security policies, procedures, and controls; identify weaknesses; and provide improvement recommendations	To verify that an organization has fully implemented the ISO/IEC 27001 standard and issue an internationally recognized certificate
Who conducts it	Can be conducted as an internal audit or external audit	Conducted only by accredited certification bodies
Status	Produces a report with findings and recommendations. Does not grant formal legal certification	Issues official ISO/IEC 27001 certificate. Valid for 3 years with annual surveillance audits
Methodology	Based on ISO/IEC 19011, ISO/IEC 27007. May use checklists, risk assessments, and technical tests	Comprehensively examines ISO/IEC 27001 requirements + Annex A controls implementation, rendering a “compliant/non-compliant” conclusion
Scope	Can be modified based on organizational needs and objectives (e.g., network security only, data center only, etc.)	Specifies a defined scope for certification and evaluates the entire ISMS
Output	Audit report	ISO/IEC 27001 certificate + audit report

- **ISMS** - Information security Management system
- **Annex A** - The control objectives and controls section of ISO/IEC 27001

This table clearly distinguishes between operational audits (checking current state) and formal certification (validating standard compliance)

Cybersecurity risk assessment methodologies are essential for recognizing, evaluating, prioritizing, and addressing risks to an organization's information and systems. These assessments, carried out with these methodologies, offer crucial background details for successful audits and are mandatory documentation for ISO/IEC27001 certification.

Table 3. Commonly used Cybersecurity risk assessment methodologies

Methodology	Characteristics
ISO/IEC 27005	Standard methodology aligned with ISMS; internationally compliant
NIST SP 800-30	NIST's (USA) risk assessment guide; widely used in government and finance sectors
OCTAVE (Carnegie Mellon)	Emphasizes business processes
FAIR (Factor Analysis of Information Risk)	Methodology based on financial calculations
ENISA Risk Management	Framework designed for EU organizations

- **ISMS** - Information security Management system
- **NIST** - National Institute of Standards and Technology
- **OCTAVE** - Operationally critical threat, asset, and vulnerability evaluation
- **FAIR** - Factor analysis of Information risk
- **ENISA** - European Union Agency for Cybersecurity

An information security audit involves reviewing previous implementations, while a cybersecurity risk assessment is a strategic tool used to predict potential risks. Standards certification, on the other hand, is a formal third-party evaluation process that is based on the results of audits and a risk management plan. Table 4 provides a comparison between information security audits and cybersecurity risk assessments.

Table 4. Differences between Information security audit and Cybersecurity risk assessment

Indicator	Information Security Audit	Cybersecurity Risk Assessment
Purpose	To verify compliance and provide assurance	To identify, evaluate, and mitigate risks
Nature	Retrospective (examining current state)	Prospective (predicting future risks)
Methodology	Checklists, standard compliance	Threat–Vulnerability–Impact model
Output	Audit report, non-conformities, recommendations	Risk register, Heat Map, action plan
Standards	ISO/IEC 27001 audit, ISACA COBIT	ISO/IEC 27005, NIST SP 800-30

- **ISACA COBIT** - Information systems audit and control Association's control objectives for Information and related technologies
- **Heat Map** - Visual representation of risk levels (typically color-coded: red - high risk, yellow - medium, green - low)
- **Retrospective** = Looking at what has been done (backward-looking)
- **Prospective** = Looking at what might happen (forward-looking)

This table clearly differentiates between **auditing** (checking compliance with existing standards) and **risk assessment** (anticipating and evaluating future threats).

Conclusions

The current regulation of cybersecurity legislation in Mongolia is crucial for safeguarding the national cyber environment, but it presents challenges in practical implementation.

Ambiguities in terminology such as "cyber" and "electronic" lead to varying interpretations of the law, policies, and implementation, hindering organizational coordination. Additionally, while the Cyber Security Law mandates annual risk assessments and biennial audits, it lacks detailed methodologies, standards, and criteria, relying solely on consulting services' knowledge and experience. This results in inadequate protection of national information systems, infrastructure, and critical databases, weakens government oversight and regulation, and hampers compliance with international standards.

In accordance with the Mongolian Cybersecurity Law, the Ministry of Electronic Development has been assigned the responsibility of issuing permits, registering, and overseeing information security audits and cybersecurity risk assessments. The Ministry's Order No. A/46, issued on April 17, 2023, has endorsed the "Procedures for the Selection, Licensing, and Registration of Organizations Providing Information Security Audit and Risk Assessment Services," serving as the primary administrative regulation to maintain operational quality and standard consistency.

While this regulation may seem to adhere to legal standards, it has limitations in drawing definitive conclusions about the effectiveness of monitoring and performance evaluation and the actual quality of organizations' activities. For instance, in 2023, it was noted that some licensed organizations shared the same domain address and registration details, and multiple organizations were registered under the same individual's address, potentially compromising the independence of information security audit service providers and leading to conflicts of interest.

Moreover, the oversight mechanisms for monitoring and validating the performance of these licensed entities and auditing outcomes are inadequate, lacking benchmarks and reporting systems to systematically assess compliance with criteria such as training certifications, human resource capabilities, and quality of work. Therefore, merely granting a license is insufficient; additional legal scrutiny, such as implementing a continuous monitoring system and conflict of interest detection methods, is necessary.

Despite the Mongolian Cybersecurity Law being a fundamental regulation, the lack of clear terminology, methodological deficiencies, weaknesses in the control system, and inconsistency with international standards hinder the effective implementation of the law. Consequently, the protection of the cyber environment is inadequate, and the digital aspect of national information is at significant risk. Therefore, aligning legal regulations with standardization, monitoring, and human resources systems is essential to enhance the practical effectiveness of organizations, safeguard national security, and establish a legal framework that aligns with international standards.

REFERENCES

1. Ministry of Digital Development. (2023). *Regulations on selection, authorization, and registration of organizations providing information security audit and risk assessment services* (Order No. A/46).
2. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
3. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 — Information security risk management*. ISO.
4. National Institute of Standards and Technology. (2012). *NIST Special Publication 800-30 Rev. 1: Guide for conducting risk assessments*. NIST. https://doi.org/10.6028/NIST.SP.800-30r1
5. European Union Agency for Cybersecurity. (2020). *Cybersecurity risk management guidelines*. ENISA. https://www.enisa.europa.eu/publications/cybersecurity-risk-management-guidelines
6. Wiener, N. (1948). *Cybernetics: Or control and communication in the animal and the machine*. MIT Press.
7. State Great Khural of Mongolia. (2022). *Law on cybersecurity*. Ministry of Justice and Home Affairs.
8. Stallings, W. (2017). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley Professional.
9. Whitman, M., & Mattord, H. (2020). *Principles of information security* (6th ed.). Cengage Learning.
10. European Union Agency for Cybersecurity. (2019). *Good practices for national cyber security strategies*. ENISA. https://www.enisa.europa.eu/publications/good-practices-for-national-cyber-security-strategies
11. Kshetri, N. (2016). *Cybersecurity management in developing countries*. Springer. https://doi.org/10.1007/978-3-319-25535-6