EVALUATING ERP INFORMATION SECURITY USING ISO/IEC 27001:2013 STANDARD IN AGRICULTURAL TECHNOLOGY ENTERPRISES

Puji Hastuti[1*], Nourma Islam Dewi Cantika[2], Aditya Pratama[3], Dhanar Intan Surya Saputra[4]
Sistem Informasi, Universitas Amikom Purwokerto, Banyumas, Indonesia[1-4]
E-mail address: pujih1211@.com[1], cantikasj20@gmail.com[2],
adityaprtma383951@gmail.com[3], dhanarsaputra@amikompurwokerto.ac.id[4]

Received: 04, April, 2025 ***Revised: 10, May, 2025*** ***Accepted: 20, June, 2025***

ABSTRACT

Data security is an essential component of ERP system management, particularly given the increasing cyber dangers in the digital age. This study assesses the maturity of ERP-based information security at PT BroilerX Yogyakarta using the ISO/IEC 27001:2013 standard. The growing dependence on digital platforms in agriculture has expedited the implementation of ERP solutions, like Odoo, to optimize business processes. This research employs a qualitative descriptive case study methodology to examine the implementation of ten ISO domains, utilizing data gathered from interviews with the IT team and analyzed through the Capability Maturity Model Integration. The findings indicate that the majority of domains attained a maturity level of 4 (Managed), signifying consistent and thoroughly documented processes, although Human Resource Security and Incident Management remained at level 3 (Defined), highlighting the necessity for enhanced automation and proactive incident management. These findings underscore both the strengths and flaws in ERP security implementation and offer actionable advice to enhance the Information Security Management System (ISMS). This research contextualizes ISO/IEC 27001:2013 within a poultry agritech enterprise, thereby enhancing understanding of the integration of international security standards in technology-driven agribusiness and providing practical insights for similar organizations aiming to bolster their resilience against cyber threats.

Keywords: Enterprise Resource Planning (ERP), ISO/IEC 27001:2013, Information Security, Agritech Enterprise, Maturity Level Assessment

1. INTRODUCTION

Digital transformation in the agricultural sector has become a key catalyst in driving the modernization of agribusiness practices through the utilization of information technology. (Amirova & Klychova, 2022). One of the most concrete manifestations of this transformation is the adoption of Enterprise Resource Planning (ERP) systems, which are designed to improve operational efficiency and strengthen integration across business processes. (Auliani, 2023a) (Pryshliak & Semenenko, 2024) (Shirokov, 2019a). In the face of global challenges concerning food security and supply chain efficiency, ERP systems offer a viable solution by accelerating the flow of information, minimizing data redundancy, and enhancing coordination among various units within an agricultural organization (Singh et al., 2024).

ERP systems are digital platforms that integrate various core organizational functions such as financial management, inventory, production, distribution, and human resources into a single, real-time, interconnected system (Mazorenko, 2025). With this capability, ERP supports more accurate and timely data-driven decision-making while providing comprehensive visibility into operational performance (Alwan & Fahmi, 2023a) (Shirokov, 2019b;Litvinova et al., 2020). In the agricultural sector, the implementation of ERP can assist business actors in responding to market dynamics, increasing productivity, and developing adaptive management strategies based on analytical data insights (Val et al., 2025).

However, despite its numerous advantages, ERP systems present specific challenges, particularly regarding the complexity of their architecture and their heavy reliance on centralized information. (Melnyk, 2024). This dependency makes ERP systems vulnerable to information security threats, including cyberattacks, data breaches, and unauthorized system access. (Nehrey, 2023). The intricate configuration of ERP also creates challenges in terms of system maintenance and comprehensive data protection (Chervanova, 2024). Therefore, in adopting ERP, the agricultural sector must not only focus on functionality but also establish robust information security strategies, including human resource training and the implementation of strict security policies (Nobari et al., 2022) (Chutcheva, 2025) (Voitsekhovska & Lomachynska, 2025) (Demchuk & Rusyn-Hrynyk, 2024).

PT. BroilerX Yogyakarta is a technology startup in the poultry farming sector that employs Odoo-based ERP to facilitate its business operations, encompassing production management, logistics, and digital payments. This system also features a connection to a mobile application for direct interaction with farmer partners in real time. This information was obtained through interviews with the IT team at PT. BroilerX Yogyakarta.

The international standard ISO/IEC 27001:2013 provides a framework for systematically managing information security based on risk assessment (Jevelin & Faza, 2023) (ISO, 2013). ISO 27001:2013 has 14 security control clauses, encompassing a total of 35 control objectives and 114 security controls to achieve the objectives (Diamantopoulou et al., 2020) (Vorobyev & Kuleshova, 2023). The 14 security control clauses such Information security policies, Organization of information security, Human resource security, Asset management, Access control, Cryptography, Physical and Environmental security, Operations security, Communications security, System acquisition, development, and maintenance, Supplier relationships, Information security incident management, Information security aspects of business continuity management, and Compliance (Fajar et al., 2018). Previous research indicates that the implementation of ISO 27001 can improve operational efficiency, regulatory compliance, and stakeholder trust (Clarissa & Wang, 2023; Rodríguez et al., 2023; Suorsa & Helo, 2023) (Khanna, 2020).

However, there has been little research specifically analyzing the implementation of ISO/IEC 27001:2013 controls in the context of ERP in the poultry farming industry, particularly in startups using platforms like Odoo. Therefore, this study contributes to filling this gap and provides a new perspective on evaluating information security systems based on international standards in the agricultural technology business environment. To resolve these issues, this

research aims to analyze the level of implementation and maturity of information security controls in the ERP system at PT. BroilerX Yogyakarta uses the ISO/IEC 27001:2013 standard. The study employs a descriptive qualitative approach using a case study method, focusing on the 10 main domains in Annex A of the ISO standard (A.5, A.6, A.7, A.9, A.10, A.12, A.13, A.14, A.16, and A.18). Data was collected through interviews with the company's IT team and analyzed using a maturity model framework to measure the gap between the current state and ideal practices. This research is expected to contribute to improving information security practices in the Indonesian agritech sector. This structure enables a systematic assessment of the extent to which the company has met the security standards established by ISO 27001:2013.

2. THEORY

According to (Amirinnisa et al., 2023)Information security refers to a set of measures taken to protect information from various threats to ensure business continuity, reduce risk, and optimize investment value. The main principle follows the CIA (Confidentiality, Integrity, and Availability) model as a guideline in maintaining confidentiality, integrity, and availability of information. ISO/IEC 27001:2013 is an international standard that specifies the requirements for an information security management system (ISMS) (Podrecca et al., 2022). According to Alit Yuniargan Eskaluspita, ISO 27001 itself is an international standard published by the International Organization for Standardization (ISO), which describes the information security management methodology in organizations, with the latest revision in 2013, so that ISO 27001: 2013 was produced. Accuracy of the system to protect information (Eskaluspita, 2020).

ERP (Enterprise Resource Planning) is a software system used to organize and integrate all the main business processes in an organization into one integrated system (Alwan & Fahmi, 2023b). According to (Auliani, 2023b)ERP (Enterprise Resource Planning) is an integrated application that organizations can use to collect, save, organize, and interpret data from the daily business activities of the company. ERP provides an integrated and continuously updated view of core business processes using a common database.

According to (Kaban & Legowo, 2018) Maturity level is a tool to measure how maturity achieved by a company in the application of information system audit. The CMMI (Capability Maturity Model Integration) framework provides structured levels to measure this maturity. The goal of implementing CMMI within an organization is to improve manufacturing and the product of the company's software. (Junior et al., 2023).

3. METHOD

In this research, data collected by interviews with the company's IT team improved information system security from May 6, 2025, to June 16, 2025. The research is intended to obtain insights into how ISO/IEC 27001:2013 the implementation of information security controls in the ERP system at PT. BroilerX Yogyakarta. The interview guidelines were developed based on the controls outlined in ISO/IEC 27001:2013, with a focus on 10 key domains. An overview of the clauses used in this research can be seen in Table 1.

Table 1. Clauses used in this Research

No	Domain (Clauses)	Control
1	A5	Information Security Policy
2	A6	Information Security Organizational
3	A7	Human Resource Security
4	A9	Access Controls
5	A10	Cryptography
6	A12	Operational Security
7	A13	Communication Security
8	A14	System Development Security
9	A16	Information Security Incident Management
10	A18	Compliance

The data collected will be analyzed based on each control domain, aiming to identify the conformity of implementation with the ISO/IEC 27001:2013 standard and to identify any possible gap analysis by comparing the actual conditions obtained from the interview results with the ideal standards in ISO/IEC 27001:2013, and using the CMMI model, which covers five maturity levels. The research is based on the alignment between the actual conditions in the company and the characteristics of each maturity level. An overview of the maturity level used in this research can be seen in Table 2.

Table 2. Clauses used in this Research

Level	Name	Description
Level 1	Initial	No procedures; ad-hoc practices
Level 2	Repeatable but Intuitive	Procedures exist but are not documented or consistently applied.
Level 3	Defined	Policies are documented, but not fully implemented consistently or evaluated.
Level 4	Managed	The controls are implemented, documented, trained, and monitored regularly.
Level 5	Optimized	The controls have been automated and are sustainable best practices.

Based on the analysis results and maturity level, conclusions and strategic recommendations are provided to improve the information security management system (ISMS) implementation at PT. BroilerX Yogyakarta.

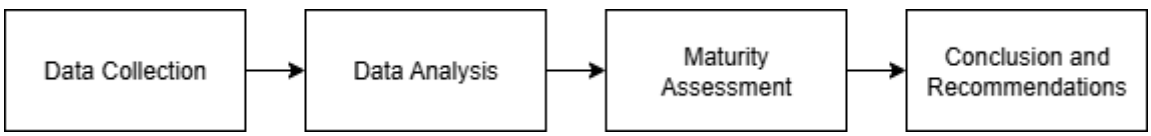

Figure 1. Research Concept.

4. RESULTS AND DISCUSSION

These research results were obtained through interviews with the IT team at PT. BroilerX Yogyakarta. The interview was structured based on the ISO/IEC 27001:2013 framework, which encompasses the ten core domains of an Information Security Management System (ISMS). This research aims to gain a comprehensive understanding of the effective implementation of information security controls at PT. BroilerX Yogyakarta. The analysis

P-ISSN : 2088-6705
E-ISSN : 2621-5608

process has three main steps: data collection from interviews, gap analysis, and a maturity level assessment based on domains A.5, A.6, A.7, A.9, A.10, A.12, A.13, A.14, A.16, and A.18.

The interview results were then analyzed according to the ten domains of ISO/IEC 27001:2013. The domain covers relevant questions on information security control aspects with responses from the IT team at PT. BroilerX Yogyakarta. This structure enables a systematic assessment of the extent to which the company has met the security standards established by ISO 27001:2013.

4.1 Results of interviews with IT based on the ISO 27001:2013 standard

4.1.1 Domain A.5 (Information Security Policy)

This document guides all divisions in maintaining data and system security and is evaluated and updated regularly to anticipate threats and meet the company's evolving needs.

4.1.2 Domain A.6 (Information Security Organization)

In Domain A.6 at PT BroilerX Yogyakarta, the structure of the information security organization has been defined clearly. In addition to the IT team, there are representatives from management and the Quality Assurance (QA) division who are also responsible for the implementation of the security policy. IT security is a part of the routine evaluation in management meetings. Security issue escalation protocols are in place, although documentation needs to be improved to ensure more effective communication channels.

4.1.3 Domain A.7 (Human Resource Security)

PT BroilerX has implemented information security training for new employees and periodic re-training. Access revocation procedures are carried out automatically and manually through coordination between the IT and Human Resources divisions. However, monitoring of security violations by employees is still done manually, so it does not yet fully support systematic monitoring.

4.1.4 Domain A.9 (Access Control)

In Access control implementation has been effective. Access rights are granted based on job responsibilities and must be approved by a supervisor. The system has also implemented multi-factor authentication, with most internal systems using two-factor authentication. Access to sensitive data is strictly limited to authorized personnel, supported by audit logs and regular system updates.

4.1.5 Domain A.10 (Cryptography)

The system uses strong encryption such as AES-256 and TLS 1.2/1.3 for data protection, both during storage and transfer. Encryption key management is carried out through a Key Management System (KMS) and is equipped with encrypted access logs.

4.1.6 Domain A.12 (Operational Security)

Patch management for the company's IT systems is carried out every week and on an ad-hoc basis if critical vulnerabilities are identified. Before launching new features, a set of Quality Assurance tests and internal audits is carried out to make sure the system is stable and secure. Monitor logs and detect anomalies using security information and event management software, which allows for early identification of potential disruptions. Network Infrastructure is protected through the implementation of active firewalls and IDS. Data backup processes are performed daily and stored in separate locations to ensure data availability in the event of a

system failure. Additionally, antivirus software on all servers and endpoints is always active and regularly updated to address the latest malware threats.

4.1.7 Domain A.13 (Communication Security)

Communication networks within the company environment are protected through firewall configuration and the implementation of an active intrusion detection system (IDS), with real-time monitoring carried out by the information security team to quickly detect and respond to potential threats.

4.1.8 Domain A.14 (System Development Security)

PT BroilerX Yogyakarta has implemented secure software development procedures with regular secure coding training, as well as code review and testing to detect potential vulnerabilities early on. Version control is managed using Git to ensure structured and transparent change logging. All application development is done internally using the Odoo system, customized to the company's needs.

4.1.9 Domain A.16 (Information Security Incident Management)

The PT. BroilerX Yogyakarta has established Standard Operating Procedures (SOPs) for incident handling, including isolation, investigation, reporting, and system recovery. However, incident response simulations are not conducted regularly, which poses a risk of reducing preparedness for real-world attacks. It is recommended to conduct regular simulations to enhance incident response capabilities and effectiveness.

4.1.10 Domain A.18 (Compliance)

PT BroilerX Yogyakarta routinely conducts security audits, both internal and external, and documents the results thoroughly. This practice helps ensure compliance with information security standards and supports continuous improvement. Monitoring and updating audits must be ongoing to keep pace with regulatory developments and security threats.

4.2 Manurity level

Maturity level assessments are done for the ISO 27001:2013 control domains based on interview results that are categorized according to clauses A.5, A.6, A.7, A.9, A.10, A.12, A.13, A.14, A.16, and A.18. The control domain is evaluated using indicators that reference five maturity levels.

Table 3. Maturity Level of ISO 27001:2013 Based on Interviews.

Domain Control	Testing Results	Maturity Level	Description
A5 - Information Security Policy	The company has documented SOPs that are routinely reviewed and revised.	4 - Managed	Procedures are in place, and documents need to be strengthened.
A6 - Information Security Organizational Structure	The responsibilities are clear, and SOPs are available.	4 - Managed	Organized but not yet comprehensive.
A7 - Human Resource Security	Training and suspension of access are implemented, but penalties are not monitored automatically.	3 - Defined	Effective and consistent implementation of controls.

Domain Control	Testing Results	Maturity Level	Description
A9 - Access Controls	Using 2FA, access rights are restricted according to need and position.	4 - Managed	Active cryptographic system.
A10 - Cryptography	Data and encryption keys are well managed and conform to industry standards.	4 - Managed	The operational process is running well.
A12 - Operational Security	System backup and monitoring procedures are performed regularly and consistently.	4 - Managed	Protected network infrastructure.
A13 - Communication Security	The use of IDS, firewalls, and network security is active and under monitoring.	4 - Managed	Documented and implemented.
A14 - System Development Security	Adoption of secure coding and documentation of the development process has been implemented.	4 - Managed	Simulations need to be held regularly.
A16 - Information Security Incident Management	There is an SOP for incident handling, but an incident simulation has not been carried out periodically.	3 - Defined	An audit has been conducted and recorded.
A18 - Compliance	Security audits are conducted regularly, and there are records of audit results.	4 - Managed	Procedures are in place, and documents need to be strengthened.

4.2 Gap Analysis

A gap analysis was conducted to compare the actual state of information security implementation at PT BroilerX Yogyakarta with ideal practices as stipulated in ISO/IEC 27001:2013. The differences between the IT team's interviews and these international standards serve as the basis for identifying areas requiring improvement. Domains with no gaps indicate that security controls have been adequately implemented and align with best practices. Table 3 below presents the current state of implementation based on the interview results and findings from the testing conducted.

Table 3. Maturity Level of ISO 27001:2013 Based on Interviews.

ISO Clauses	Current Implementation	Testing Results
A5	There is an SOP policy.	-
A6	Tasks are clearly defined, and SOPs are available.	Advanced documentation for escalation procedures is required.
A7	Training and revocation are active.	Sanction monitoring is not yet automated.
A9	Factor Authentication and appropriate access rights.	-

ISO Clauses	Current Implementation	Testing Results
A10	The encryption and Key Management System works well.	-
A12	Routine monitoring and backup are carried out.	-
A13	Intrusion Detection System and firewall are active.	-
A14	Safe coding practices in action.	-
A16	Handling SOP document available.	Incident simulation is still not done regularly.
A18	There is an SOP policy.	-

To quantitatively determine the level of the gap, maturity levels were measured in each domain. The results of these measurements are shown in Table 4.

Table 4. Result of Maturity Levels Gap by Domain

Domain	Maturity Level Real	Maturity Level Ideal	GAP ANALYSIS
A5	4	5	1
A6	4	5	1
A7	3	5	2
A9	4	5	1
A10	4	5	1
A12	4	5	1
A13	4	5	1
A14	4	5	1
A16	3	5	2
A18	4	5	1

The measurement results show that most domains, such as A5 (Information Security Policies), A6 (Organization of Information Security), A9 (Access Control), A10 (Cryptography), A12 (Operations Security), A13 (Communications Security), A14 (System Acquisition, Development and Maintenance), and A18 (Compliance), have reached maturity level 4 (Managed). This indicates that security controls in these areas have been implemented consistently and are well-documented.

However, there are still two domains that are only at maturity level 3 (Defined), namely A7 (Human Resource Security) and A16 (Incident Management). This gap is mainly caused by the suboptimal automation in the sanctions monitoring system in A7, as well as the lack of periodic incident simulations in A16. To clarify the comparison between the actual conditions and the ideal standard ISO/IEC 27001:2013, a visual representation in the form of a spider chart is used in Figure 1.

P-ISSN : 2088-6705
E-ISSN : 2621-5608

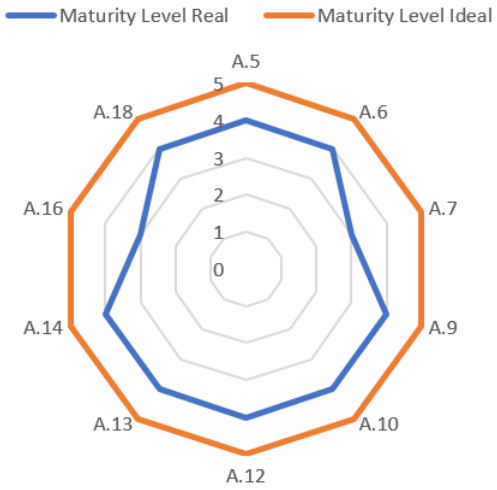

Figure 1. Representation Manurity Level Result.

The orange line in the figure represents the ideal maturity level (level 5 – Optimal) expected to be achieved across all domains, while the blue line shows the actual maturity level based on interviews with the IT team at PT BroilerX Yogyakarta. This visualization shows that although most domains are at level 4, there are still significant gaps in the human factor and incident readiness aspects. Overall, this gap analysis indicates that the ERP security system at PT BroilerX has a strong foundation. However, to achieve the optimal maturity level according to the ISO/IEC 27001:2013 standard, strengthening the Human Resource Security aspect is necessary through automated monitoring, as well as increasing the effectiveness of Incident Management through conducting scheduled incident simulations.

5. CONCLUSIONS AND SUGGESTIONS

Based on the results of investigations and studies on ISO 27001:2013, PT BroilerX has adopted various information security measures that are quite adequate, with a maturity level between 3 (Defined) and 4 (Managed). The company has official policies and solid technical implementations in most areas, particularly in access control, encryption, and operational aspects. However, there are still some areas that can be improved, such as training for incident handling and documentation for system development testing.

To resolve these issues and improve the effectiveness of the Information Security Management System (ISMS), they suggested a few strategic recommendations, including: 1) Improving documentation and evaluating procedures regularly. 2) Implementing regular information security incident simulations. 3) Automating monitoring and reporting of policy violations. 4) Integrating encryption key lifecycle management policies. 5) Standardizing access controls in all ERP modules. The implementation of these recommendations is expected to enhance PT. BroilerX Yogyakarta is ready against digital security threats and supports the sustainable operation of a secure and reliable ERP system.

6. ACKNOWLEDGEMENTS

The authors would like to gratefully express their sincere thanks to PT. BroilerX Yogyakarta for the opportunities and support provided during the research process. Special thanks to the IT team for their cooperation and insights during the interviews and data collection. The authors would also like to thank the academic mentors and lecturers from the Department of Sistem

Informasi at Universitas Amikom Purwokerto for the continuous guidance and support. This research would not have been possible without the support and contributions of all parties involved.

REFERENCES

Alwan, S., & Fahmi, M. A. (2023a). Implementasi sistem ERP pada divisi rantai pasok PT. Pindad (Persero). *Jurnal Kewirausahaan, Akuntansi Dan Manajemen Tri Bisnis*, *5*(2), 139–148. https://doi.org/10.59806/tribisnis.v5i2.279

Alwan, S., & Fahmi, M. A. (2023b). Implementasi sistem ERP pada divisi rantai pasok PT. Pindad (Persero). *Jurnal Kewirausahaan, Akuntansi Dan Manajemen Tri Bisnis*, *5*(2), 139–148. https://doi.org/10.59806/tribisnis.v5i2.279

Amirinnisa, M., Bisma, R., Kom, S., & Kom, M. (2023). Analysis of Information Security Risk Assessment Based on Iso 27005 for Preparation for Iso 27001 Certification in The Government of Madiun City. *Journal of Emerging Information System and Business Intelligence (JEISBI)*, *4*(4), 47–58.

Amirova, E., & Klychova, G. (2022). Digital transformation of the agricultural economy. *Regional Economics: Theory and Practice*. https://doi.org/10.24891/re.20.1.156

Auliani, L. N. (2023a). Implementasi enterprise resource planning odoo dalam optimalisasi proses bisnis PT XYZ. *Qualitative Research of Business and Social Sciences*, *1*(1), 50–61. https://doi.org/10.31316/qrobss.v1i1.5574

Auliani, L. N. (2023b). Implementasi enterprise resource planning odoo dalam optimalisasi proses bisnis PT XYZ. *Qualitative Research of Business and Social Sciences*, *1*(1), 50–61. https://doi.org/10.31316/qrobss.v1i1.5574

Chervanova, D. A. (2024). Problems of legal regulation of digitization in the field of agribusiness. *Analytical and Comparative Jurisprudence*. https://doi.org/10.24144/2788-6018.2024.06.79

Chutcheva, T. (2025). Digital Transformation of Agriculture: From Theory to Practice. *Economics and Business: Theory and Practice*, *12*(4), 113–123. https://doi.org/10.29039/2500-1469-2024-12-4-113-123

Clarissa, S., & Wang, G. (2023). Assessing Information Security Management Using ISO 27001:2013. *Jurnal Indonesia Sosial Teknologi*, *4*(9), 1361–1371. https://doi.org/10.59141/jist.v4i9.739

Demchuk, O., & Rusyn-Hrynyk, R. (2024). Current level of digitalization of business processes agricultural enterprises. *Economic Scope*. https://doi.org/10.32782/2224-6282/191-7

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC 27002:2013 information security controls to personal data protection controls: Guidelines for GDPR compliance. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 11980, pp. 238–257). https://doi.org/10.1007/978-3-030-42048-2_16

Eskaluspita, A. Y. (2020). ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University. *IOP Conference Series: Materials Science and Engineering*, *879*(1). https://doi.org/10.1088/1757-899X/879/1/012074

Fajar, A. N., Christian, H., & Girsang, A. S. (2018). Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet. *Journal of Physics: Conference Series*, *1090*(1). https://doi.org/10.1088/1742-6596/1090/1/012060

ISO. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*.

Jevelin, J., & Faza, A. (2023). Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification. *Journal of Information Systems and Informatics*, *5*(4), 1240–1256. https://doi.org/10.51519/journalisi.v5i4.572

Junior, R., Utomo, R. G., & Oktaria, D. (2023). *Information Security Analysis in PT. XYZ Using ISO/IEC 27001:2013*.

Kaban, E., & Legowo, N. (2018). Audit Information System Risk Management Using ISO 27001 Framework at Private Bank. *Journal of Theoretical and Applied Information Technology*, *15*(1).

Khanna, N. (2020). Digital Transformation of the Agricultural Sector: Opportunities and Challenges. *Applied Economic Perspectives and Policy*. https://doi.org/10.1002/aepp.13103

Litvinova, O., Abrosimova, M. S., Vasilyeva, O., Filippova, S., Gordeeva, L., & Nesterova, N. (2020). Digital platform as a liaison mechanism and a business model in agribusiness. *IOP Conference Series: Earth and Environmental Science*, *604*. https://doi.org/10.1088/1755-1315/604/1/012033

Mazorenko, M. (2025). Digitalisation of accounting in the agricultural sector: Government initiatives and strategic approaches. *Business Navigator*. https://doi.org/10.32782/business-navigator.78-60

Melnyk, R. (2024). Analysis of digital transformation and cybersecurity in agribusiness in the context of economic financialization. *Scientific Opinion: Economics and Management*. https://doi.org/10.32782/2521-666x/2024-88-19

Nehrey, M. (2023). Digital transformation of the agricultural sector: prospects, challenges and solutions. *Scientific Papers NaUKMA. Economics*. https://doi.org/10.18523/2519-4739.2023.8.1.94-100

Nobari, B. Z., Azar, A., Kazerooni, M., & Yang, P. (2022). Revisiting enterprise resource planning (ERP) risk factors over the past two decades: defining parameters and providing comprehensive classification. *International Journal of Information Technology*, *14*(2), 899–914. https://doi.org/10.1007/s41870-020-00502-z

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, *142*, 103744. https://doi.org/10.1016/j.compind.2022.103744

Pryshliak, V., & Semenenko, L. (2024). Digital Transformation of Agricultural Enterprises With Elements of Precision Agriculture: Strategic Planning. *Agroecological Journal*, *32*(60), 4–10. https://doi.org/10.25264/2311-5149-2024-32(60)-4-10

Rodríguez, G. R. D. L. C., Fernández, R. A. M., & Santos, A. C. M. D. L. (2023). Information security in e-commerce based on ISO 27001: A systematic review. *Innovación y Software*, *4*(1), 219–236. https://doi.org/10.48168/innosoft.s11.a79

Shirokov. (2019a). The Digitalization Of Management Processes In Agriculture Industry. *Proceedings of the Future Academy*. https://doi.org/10.15405/epsbs.2019.12.05.114

Shirokov, V. (2019b). The Digitalization of Management Processes in Agricultural Enterprises. *The European Proceedings of Social and Behavioural Sciences*, 1071–1079. https://doi.org/10.15405/epsbs.2019.12.05.114

Singh, S., Suman, Kour, P., & Kumar, S. (2024). Digitalization and technology in agribusiness: Trends, impacts, and future directions. *International Journal of Advanced Biochemistry Research*. https://doi.org/10.33545/26174693.2024.v8.i11a.2805

Suorsa, M., & Helo, P. (2023). Information Security Failures Measured and ISO/IEC 27001:2022 Controls Ranked by General Data Protection Regulation Penalty Analysis. *2023 11th International Conference on Cyber and IT Service Management (CITSM)*, 1–5. https://doi.org/10.1109/CITSM60085.2023.10455413

Val, O. M., Stadnik, A. T., Samokhvalova, A. A., & Kuznetsova, I. G. (2025). Digital Transformation of Agriculture in the Far North Regions. *AIC: Economics, Management*. https://doi.org/10.33305/252-19

Voitsekhovska, & Lomachynska. (2025). Risks for Agricultural Enterprises in the Context of Digital Transformation: Impact on Innovative Development and Competitiveness. *Journal of Management, Economics and Technology*. https://doi.org/10.69803/3083-6034-2025-1-44

Vorobyev, A., & Kuleshova, M. (2023). The Impact of Digital Transformation Processes on the Security of Industrial Information Systems. *Digital Economy*, *2*, 64–71. https://doi.org/10.24888/2949-2793-2023-2-64-71