INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 2 Tahun 2024 Page 6899-6920
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Design Of Information Security Management System Based On Iso / Iec 27001: 2013 In The Manufacturing Industry

Arief Nugraha[1✉] , Jarot Suroso Sembodo[2]
Information Systems Management Department, BINUS Graduate Program
Master of Information Systems Management, Bina Nusantara University
Jakarta, Indonesia, 11480
Email: arief.nugraha001@binus.ac.id[1✉]

Abstrak

Tujuan dari penelitian ini adalah untuk memahami Sistem Manajemen Keamanan Informasi berdasarkan ISO/IEC 27001:2013, untuk mengetahui karakteristik keamanan informasi dan pada industri manufaktur yang sedang bertransformasi menuju teknologi Industri 4.0, untuk mengetahui persyaratan ISO/IEC klausul 27001:2013 yang telah dipenuhi, baik dari segi framework (kebijakan dan prosedur) maupun aspek penerapannya serta memahami penerapan Sistem Manajemen Keamanan Informasi berdasarkan SNI ISO/IEC 27001:2013 pada industri manufaktur yang sedang menuju Industri 4.0 (Smart Factory), khususnya dalam operasional Data Center. Untuk mengukur tingkat kematangan keamanan informasi digunakan metode Indeks KAMI. Metodologi penelitian menggunakan gap analysis dan pendekatan PDCA (Plan – Do – Check – Act) dengan mengikuti tahapan sesuai dengan ketentuan ISO/IEC 27001:2013. Setelah penerapan manajemen risiko dimulai dengan identifikasi risiko, pengukuran dampak risiko, evaluasi pengendalian, penetapan rencana manajemen risiko hingga pemantauan dan peninjauan risiko terhadap temuan gap analysis, maka dilakukan rencana aksi sebagai tindak lanjut dari temuan tersebut. analisis kesenjangan. Hasil penelitian ini diharapkan mampu menciptakan model Sistem Manajemen Keamanan Informasi berdasarkan SNI ISO/IEC 27001:2013 yang cocok diterapkan pada industri manufaktur yang menggunakan teknologi Industry 4.0 sehingga dapat mencegah kebocoran informasi dan produksi. gangguan dari serangan di dunia maya..

Kata Kunci: *manufaktur, Industri 4.0, keamanan informasi, manajemen risiko, ISO/IEC 27001:2013*

Abstract

The purpose of this research is to understand the Information Security Management System based on ISO/IEC 27001:2013, to know the characteristics of information security and in the manufacturing industry which is transforming towards Industry 4.0 technology, to know the requirements of ISO/IEC 27001:2013 clauses that have been met, both in terms of framework (policies and procedures) as well as aspects of its implementation and understand the implementation of an Information Security Management System based on SNI ISO/IEC 27001:2013 in the manufacturing industry that are heading towards Industry 4.0 (Smart Factory), especially in Data Center operations. To measure the maturity level of information security, the KAMI Index method is used. The research methodology uses a gap analysis and PDCA (Plan – Do – Check – Act) approach by following the stages in accordance with the provisions of ISO/IEC 27001:2013. After the implementation of risk management begins with risk identification, measuring the impact of risk, evaluating controls, establishing a risk management plan to monitoring and reviewing risks against gap analysis findings, an action plan is carried out as a follow-up to the findings of the gap analysis. The results of this study are expected to be able to create an Information Security Management System model based on SNI ISO/IEC 27001:2013 that is suitable for application in a manufacturing industry that uses Industry 4.0 technology so that it can prevent information leaks and production disruptions from attacks in cyberspace..

Keywords: *manufacture, Industry 4.0, information security, risk management, ISO / IEC 27001:2013*

INTRODUCTION

The Information Security Management System (ISMS) currently plays an important role in any information security implementation in the company. Information Security Management System refers to the entire process of information system security management including personnel, technology and procedures. Information security systems combine analysis methods and systems design, manual information systems, managerial problems and social and ethical issues. This information security system includes a broader perspective than computer security systems which connotes threat concepts and physical and logical techniques applied in protecting electronic computers and communication systems. In today's business world, it is very important to look at planning and management of information systems security because issues such as personnel and procedures are handled as important as any other technical measure in securing company assets[1].

Information security systems are also a major concern in the manufacturing industry. Industrial technology 4.0, which combines the concepts of Cyber - Physical System (CPS) and Internet of Things (IoT) in a production system, makes companies more closely connected to machines, the internet and other companies [2].

This results in manufacturing companies vulnerable to information leakage, either due

to inadequate information security technology, personal negligence or attacks from cyberspace[3].

According to Robinson, the manufacturing industry was ranked as the target of espionage through cyber attacks from various industrial sectors with a percentage of 27%[4].

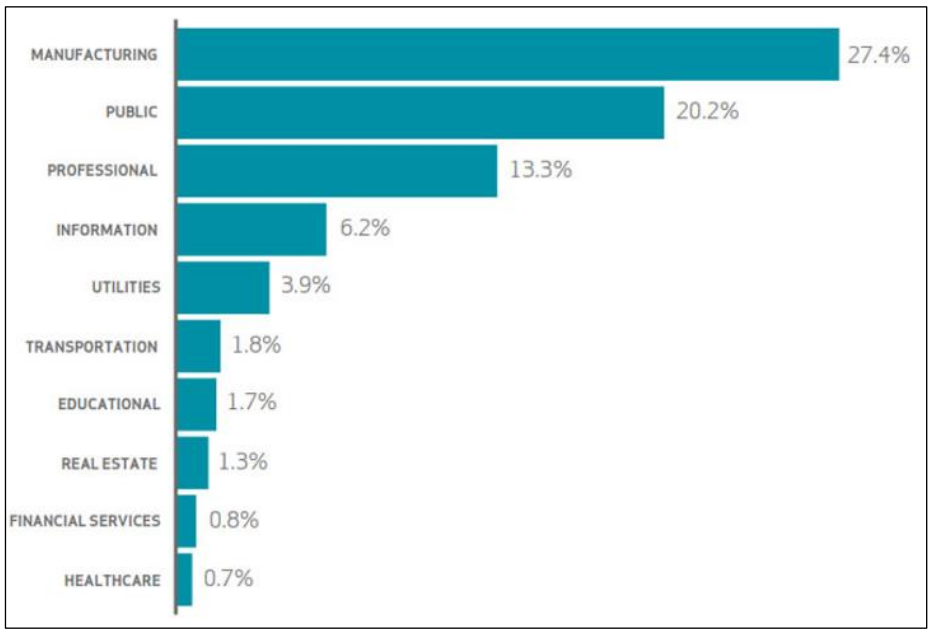

FIGURE 1.Top 10 Industries targeted for espionage[4]

In the EEF cybersecurity survey, around 48% of manufacturers reported having been targeted by cyberattacks, about half of them saying they suffered losses as a result. This doesn't count businesses that don't even realize they've been attacked. [5]

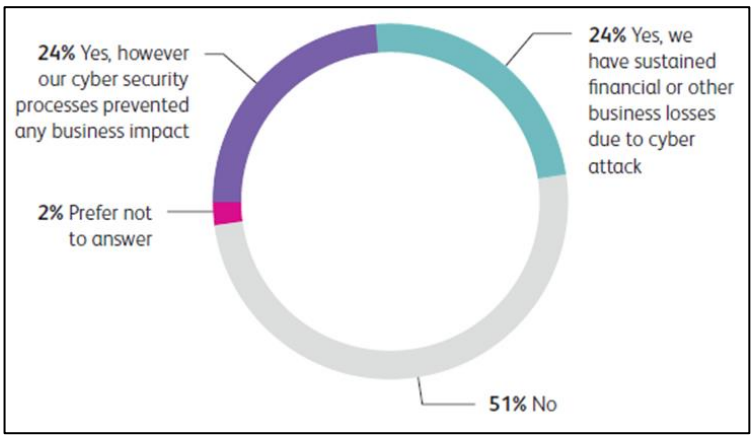

FIGURE 2Report on losses due to cyber attacks [5]

This research was conducted to study and analyze the Information Security Management System standards, in this case ISO / IEC 27001: 2013 [6]and its application to

the manufacturing industry especially in scope of Data Center operation in order to transform technology into Industry 4.0 to protect technology from information leakage that can result in the fall of the technology to outsiders, especially competitors, as well as preventing cyber attacks that can result in the cessation of the manufacturing process in the company.

In the analysis of the application of ISO / IEC 27001: 2013 based ISMS in the manufacturing industry, there are several questions that need to be answered: What are the criteria for Information Security Management System based on ISO / IEC 27001:2013? What are the characteristics of information security in the manufacturing industry especially for data center operation that is getting ready to use Industry 4.0 technology? To what extent have the requirements of ISO / IEC 27001:2013 clauses been fulfilled, both in the aspects of the framework (policies and procedures) and aspects of its implementation? And what is the model for implementing the Information Security Management System based on ISO / IEC 27001:2013 in the manufacturing industry 4.0 (Smart Factory)?

The results of this study are expected to be able to create a model of Information Security Management System based on ISO / IEC 27001 which is suitable for application at data center operation in a manufacturing industry that uses Industry 4.0 technology in order to prevent information leakage and production disruption from attacks in cyberspace.

2. Literature Review.As a reference for this research, a review of several technology-related research and journals in Industry 4.0 and the following information security management systems was conducted:

Industry 4.0 Cybersecurity: Challenges & Recommendations [7]

This study provides the results of a gap analysis carried out to identify the main challenges in implementing security and security measures for Industry 4.0 and Industrial IoT. ENISA follows a holistic and comprehensive approach to issues related to cybersecurity in Industry 4.0, where challenges and recommendations are linked to one of the following categories: People, Processes and Technologies.

Information System Security Management Standards Based on ISO / IEC 27001: 2005 [8]

This journal discusses the lack of attention of stakeholders and information managers on information system security along with the development of information technology. To protect and prevent threats to information systems, information security management standards are needed, one of which is by using ISO / IEC 27001. The purpose of the journal is to explain ISO / IEC 27001 as a standard for information system security management and

the benefits of its application.

Risk Management & Mitigation Plan for Data Center Environment[9]

The background of this research is to carry out a risk assessment and risk mitigation plan to ensure that the Data Center will function normally under any possible conditions so that the organization's business can run without problems. The research method uses the Facilitated Risk Analysis and Assessment Process (FRAAP) technique to list and mitigate risks to a company's Data Center. The purpose of the research is to ensure that Data Center IT data centers are resistant to threats.

On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center [10]

The research background is the importance of protecting the data center both physically and logically to secure information systems from security attacks such as information theft, service failure and unauthorized access. Implementing the ISMS will help to identify, manage and reduce security threats in the data center. The purpose of this research is to design an ISMS framework that is specifically designed to protect information security in data centers based on the ISO / IEC 27001 Annex A standard. Implementing this ISMS framework can reduce threats to information security in the data center to support business continuity.

Based on the journal and research references above, and paying attention to the need to protect the manufacturing industry from increasing information security threats, it is necessary to design an ISMS, especially with regard to technological transformation for manufacturing industries that will use industrial technology 4.0 (Smart Factory).

RESEARCH METHOD

The research methodology uses a gap analysis and PDCA (Plan – Do – Check – Act) approach by following the stages in accordance with the provisions of ISO/IEC 27001:2013. The methodology diagram is illustrated below:

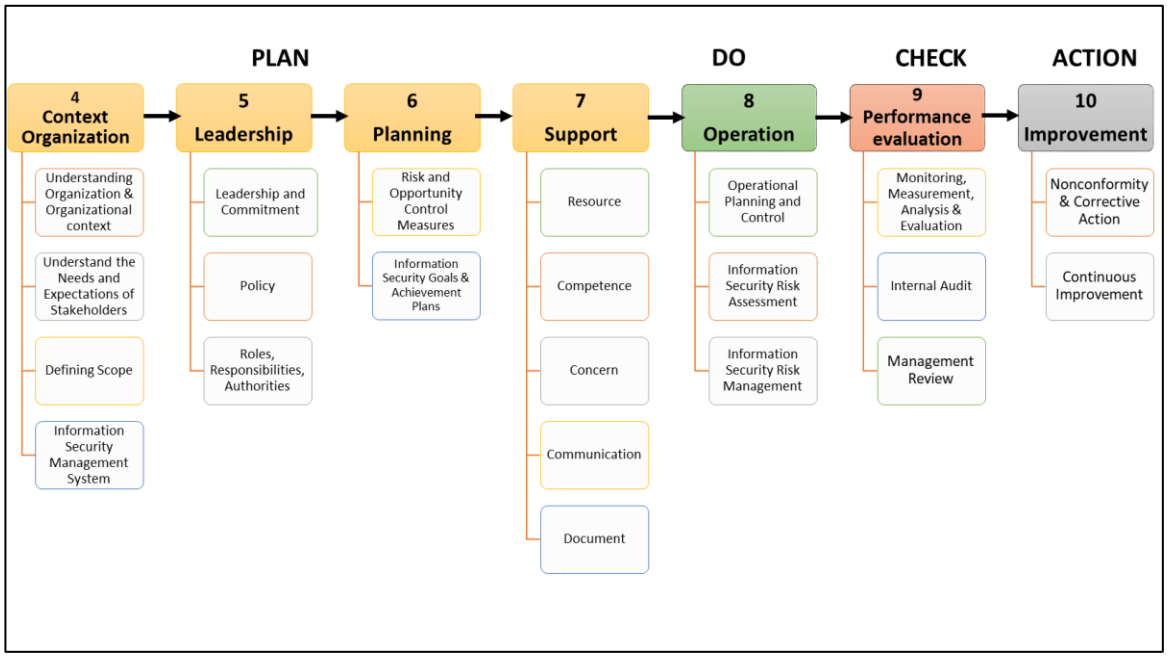

FIGURE 3ISO/IEC 27001:2013 Research Methodology[11]

3.1. Plan.In the preparatory stage, preparatory activities for the implementation of ISO/IEC 27001 are carried out in the form of:

• understanding of the organizational structure, business processes, procedures, existing IT environment and system, understanding the needs and expectations of interested parties,

• collection of documents/data in the form of policies, procedures, documents and records according to ISO/IEC 27001:2013 standards.

• carry out a readiness assessment by conducting interviews based on an assessment checklist which contains questions regarding the implementation of information system security management referring to ISO/IEC 27001:2013 domains and controls and the KAMI Index, discussions (interviews) with all relevant parties in the IT unit and business unit,

• Conducting gap analysis of clauses and control of current conditions in the aspects of people, process and technology with the requirements of ISO/IEC 27001:2013 and identifying findings (weaknesses) in all aspects of people, process, technology and documentation according to the provisions of ISO/IEC 27001:2013.

• Prepare scope documentation and Statement of Applicability (SoA) ISO/IEC 27001:2013.

• prepare an action plan (roadmap) in detail for remediation or filling gaps (gap analysis) with clauses & provisions of ISO/IEC 27001:2013 for the Information Technology Department and other related parties according to the scope.

3.2. Do.At this stage, the implementation of a follow-up plan (action plan) is carried out according to the roadmap to meet the requirements of ISO/IEC 27001:2013. The main activities carried out at this stage are:

- Compile a checklist of documents and content needed to meet the requirements for ISO/IEC 27001:2013 certification.
- Make complete ISO/IEC 27001:2013 documentation required for the implementation of the Information Security Management System.
- Fulfillment of clauses 4 to 10 of ISO/IEC 27001:2013 according to the scope of company.
- Implementation of information security controls consisting of 14 categories and 114 applicable security controls according to the requirements of ISO/IEC 27001:2013.
- Prepare scope documentation and Statement of Applicability (SoA) ISO 27001.
- Develop policy documents, procedures and records (records) in IT units and related parties for compliance with requirements (clauses) and ISO 27001 security controls.
- Carrying out risk management starting from risk identification, measuring the impact of risk, evaluating controls, establishing risk management plans to monitoring and reviewing risks

3.3. Check.At this stage an overall review and evaluation of the results of the implementation of ISO 27001 will be carried out in collaboration with the Quality Assurance Department. Review and evaluation can be a simulation (internal audit) before the certification auditby external auditors. The results of the review and evaluation (audit) provide an overview of the company's readiness to face a certification audit. The results of the review (internal audit) which contain findings and recommendations for improvement in order to comply with ISO 27001 standards will be reported to the company's management as management review material.

The main activities carried out at this stage are as follows:

- Identify findings (weaknesses) throughout ISO 27001 processes and documentation.
- Prepare recommendations for compliance with ISO 27001 clauses.
- Carrying out corrective actions based on audit results.
- Carry out management review.

3.4. Action.Remediation is carried out to meet the deficiencies in fulfilling the requirements of ISO/IEC 27001:2013, the results of the review and evaluation of the Internal Audit up to the plan to submit ISO/IEC 27001 Certification which will be carried out by the External Audit.

RESULT AND DISCUSSION

As a strategic manufacture company in Indonesia, it is obliged to provide IT services supported by reliable and secure data center that are safe and able to maintain the confidentiality, integrity and availability of all information belonging to users and IT services. To fulfill this and integrate all business processes with information security, management took the initiative to develop an Information Security Management System Work Plan (ISMS) or Information Security Management System Plan.

Scope of Implementation

The scope of implementation of the Information Security Management System (ISMS) based on ISO/IEC 27001:2013, namely "Information Security Management System in Data Center Operations".

Activities in the implementation of ISO/IEC 27001:2013 are:

1. Readiness assessment & gap analysis of existing information security conditions against ISO 27001 requirements which cover aspects of:
   • People, namely organizational structure, roles, duties and responsibilities, KPIs, work programs, etc.
   • Process, namely: policies, procedures and activities for managing user access, incidents security, application development, security monitoring, etc.
   • Technology, namely information security infrastructure, firewalls, IDS/IPS, antimalware, vulnerability assessment tools, security monitoring tools, etc.
2. Compile ISO 27001 scope documentation and Statement of Applicability (SoA).
3. Prepare an Assessment Gap Analysis report that includes aspects of people, process & technology as well as ISO 27001 documentation.
4. Develop a follow-up strategy or action plan and roadmap for meeting gaps in ISO 27001 provisions.
5. Implementation of follow-up or action plans to fulfill gaps in ISO 27001 requirements covering aspects of People, Process & Technology, such as policies, procedures, reports, job descriptions, KPIs, risk analysis, security hardening, and other documentation (records) in accordance with ISO 27001 provisions.

Current State of Information Security.

Referring to the domain and control of ISO 27001: 2013 and the KAMI (Information Security) Index, the results of filling out the KAMI assessment obtained the following scores:

the maturity level is included in the Level I+ category, up to Level II+ Category, with the final evaluation value: Fulfillment of the Basic Framework.

The level of dependence on the role of information and communication technology (SE score) is 23. This shows that the level of dependence regarding the role of information and communication technology is included in the "High" category, namely the use of information and communication technology is an integral part of the work process.

The governance and information security framework section is at level I+, i.e. Initial Conditions. The risk management and asset management section is at level II, while for the Technology and Information Security section is at level II+, namely Fulfillment of the Basic Framework.

The final result of measuring information system security uses the KAMI Index to draw conclusions by looking at the level of completeness of the implementation of the ISO 27001:20013 standard in the yellow area and the total value of the level of completeness of the application of the SNI ISO 2701: 2013 standard is 355, so that it is included in the readiness status Requires Improvement to increase the level of completeness of the Information Security Management System (ISMS) implementation.

As an equivalent to the ISO/IEC 2700:2013 standard, the expected maturity level for the minimum threshold for certification readiness is Level III+.

Gap Analysis

From the results of the Evaluation & Analysis carried out by observing directly to the field, asking questions with related parties and checking applicable documents, such as: Policies, Procedures & WI, Service Catalog, Risk List, Security Penetration Test Documents, network and infrastructure topology , then compared with the clauses in ISO 27001, 35 findings were found with the following recommendations:

TABLE 1. Gap Analysis and recommendations

No.	Finding	Clause	Recomendation
1.	There is no SMKI Work Plan document which contains: • Scope of ISMS. • The processes and parties involved in the ISMS.	Clause 4.3 Clause 6.1.1 Clause 6.1.3	Prepare ISMS Plan documents according to ISO requirements and management system implementation (PDCA).

	• Planned ISMS evaluation schedule. • SMKI KPI targets. • ISMS resources. • Planned ISMS reporting schedule to related parties. • Schedule risk assessment & management review plan.	Clause 6.2 Clause 8.1 Clause 9.4	
2.	There is no information security risk assessment (ISMS) document that contains a list of risks, risk level, treatment options, risk owner, residual risk.	Clause 6.1.2 Clause 6.1.3	Prepare assessment and handling of information security risks (ISMS) according to ISO requirements.
3.	There is no regular ISMS objective evaluation report (KPI).	Clause 9.1	Prepare routine ISMS objective evaluation (KPI) reports according to ISO requirements.
4.	There is no periodic Management Review (MR) report for ISMS which contains: a) action status from previous management review; b) changes in external and internal issues (if any) c) non-conformities and corrective actions;	Clause 7.5.3	Make periodic Management Review (MR) reports for ISMS according to ISO requirements.
5.	There is no master ISMS document that contains a list of documents and records of evidence of ISO 27001 implementation.	Clause 7.5	Compile the ISMS master document as a document controller & record for evidence of ISO 27001 implementation.

	The master document functions as a document & record controller.		
6.	There are no HCM SOP documents which include provisions for Recruitment, Transfer & Termination of Work, background checks, work agreements/NDA, sanctions, removal of access, etc.	A.11.2.9	Develop HR SOPs which include Recruitment, Transfer & Termination of Work, provisions for background checks, work agreements/NDA, sanctions, removal of access, etc.
7.	There is no SOP document that regulates the use & security of Test Data, namely the data used by the development team when carrying out UAT/SIT.	A.9	Develop SOP regarding terms of use of Test Data to prevent misuse by unauthorized parties.
8.	Some notes/records (reports, logs, forms) do not yet have a standard format: title, date, version, doc number, party that made, reviewed and approved.	Clause 7.5.3	Create and apply standard formats for all records (reports, forms) according to ISO requirements.
9.	There are no ISMS improvement (corrective) reports for non-compliance with ISO 27001 standards, for example improvements to external & internal audit findings, security incidents, VA & pentest results, etc.	Clause 10.1 Clause 10.2	Make an ISMS improvement (corrective) report for non-compliance with ISO standards.

10.	There is no evidence (record) that the IT Security team has contact with authorities, such as cybercrime, BSSN, etc.	A.6.1.3	Making contact with authorities, such as cybercrime, BSSN, etc
11.	There is no evidence (record) that the IT Security team is affiliated with communities, forums and professional associations of security specialists, such as ISACA, ISPN, Hackernews, etc.	A.6.1.4	Join as a member of security specialist communities, forums and professional associations, such as ISACA, ISPN, Hackernews, etc.
12.	There is no formal report (record) on the list of information security training and the results of its evaluation.	A.7.2.2	Compile a formal report (record) list of information security training & evaluation results.
13.	There is no formal report (record) listing information assets, classification, retention & owner for the scope of the Data Center.	A.8.1.1 A.8.1.2	Make a formal report (record) list of information assets, classification, owner (owner).
14.	There is no formal report (record) for closing access company applications and returning company assets by employees/vendors who stop working (resign or end of contract period).	A.8.1.4	Make a formal report (record) of closing access and returning PT KS assets by employees/vendors who stop working (resign or end of contract period).
15.	There is no evidence (record) of the implementation of CONFIDENTIAL information classification procedures on	A.8.2.1 A.8.2.2	Create documents (BA/report) proof of implementation of CONFIDENTIAL

	paper and electronic documents (e-mails, files, etc.), such as the use of labels, passwords & encryption.		information classification procedures on paper and electronic documents (e-mails, files), such as the use of labels, passwords & encryption.
16.	There is no evidence (record) of the implementation of the procedure for destroying CONFIDENTIAL information in the data center (if any).	A.8.3.1	Make documents (BA/report) proof of implementation of the procedure for destroying CONFIDENTIAL information in the data center (if any).
17.	There is no evidence (record) of the implementation of procedures for sending media containing CONFIDENTIAL information, in data centers such as couriers, encrypted files, etc.	A.8.3.1	Create documents (BA/report) proof of implementation of media transfer procedures that contain CONFIDENTIAL information in the data center, such as couriers, etc.
18.	There are no User Access Matrix (UAM) documents for applications, IT infrastructure and data centers.	A.9.2.2	Create application UAM documents, IT infrastructure and data centers.
19.	There is no document listing User IDs and access rights for applications, IT infrastructure and data centers as of November 2022.	A.9.2.2	Create a document listing User IDs and access rights for applications, IT infrastructure and data centers as of November 2022.

20. There are no documents for closing/deleting User Access applications, IT infrastructure and data centers during 2022.	A.9.2.2	Create documents for closing/deleting User Access applications, IT infrastructure and data centers during 2022.
21. There is no document listing applications & utility programs (tools) used by the IT Dept., especially data centers during 2022.	A.9.4.4 A.9.2.2	Make a document listing the utility programs (tools) used by the IT Dept., especially the data center during 2022.
22. There is no document listing users/personnel who have access to the application source code in the data center in 2022.	A.9.2.2	Create a list of user ID documents that have access to application source code in the data center in 2022,
23. There is no document listing the use of encryption, validity period & access rights to application encryption & IT infrastructure in data centers in 2022.	A.10.1.2	Create a document listing the use of encryption, validity period & access rights to application encryption & IT infrastructure in the data center in 2022.
24. There is no review report on the list of employees who have access to the IT Dept room & the data center (fingerprint/card/PIN) in 2022.	A.11.1.2	Make a review report on the list of employees who have access to the IT Dept room &data center (fingerprint/card/PIN) in 2022.
25. There are no documents for checking user access to data centers, applications & IT infrastructure in 2022.	A.9.2.5	Create documents for checking user access to data centers,

			applications, IT infrastructure in 2022.
26.	There are no inspection documents for data center security facilities, such as CCTV, Genset, FM200, APAR, Smoke Detector, grounding & room cleanliness during 2022.	A.11.2.2	Make inspection documents for data center security facilities, such as CCTV, Genset, FM200, APAR, Smoke Detector, grounding & room cleanliness during 2022
27.	There is no standard document for the configuration of security parameters (hardening): • Application & IT infrastructure in data center . • Desktop & laptop in PT KS data center.	A.11.2.9	Create a standard document for hardening desktop & laptop security parameters, applications & IT infrastructure in the data center.
28.	There are no data testing documents for backup (restore) IT applications & infrastructure in the data center during 2022.	A.12.3.1	Creating data backup (restore) test documents for applications & IT infrastructure in data centers during 2022.
29.	There is no capacity plan document for IT applications & infrastructure in data centers in 2022.	A.12.1.3	Create capacity plan documents for applications & IT infrastructure in data centers in 2022.
30.	There are no documents for examining security parameters for IT infrastructure & applications in data centers in 2022, such as checking	A.11.2.6	Create documents for checking application security parameters & IT infrastructure in data centers in 2022, such as

	password configurations, clock sync, logs, etc.		password configuration, clock sync, logs, etc.
31.	There are no application architecture & topology documents & IT infrastructure in data centers in 2022. There is no data center layout document in 2022.	A.12.1.3	Create architectural & topology documents for IT applications & infrastructure in data centers in 2022. Create data center layout documents for PT KS in 2022.
32.	There are no documents for examining logs for Administrator/root application users, IT infrastructure and data centers in 2022.	A.11.2.9	Create document checking log user administrator/application root, IT infrastructure and data center in 2022.
33.	Periodic Security Vulnerability Assessments or Penetration Tests of applications, IT infrastructure and data centers have not been carried out to ensure that existing security holes are identified and repaired.	A.9	Conduct periodic Security Penetration Tests of applications, IT infrastructure and data centers.
34.	The data center space has not yet used a strong metal door. The door lock to the server room is broken. There is no separation of power & data cable lines. Not all network cables have labels.	A.11.2.9	Implementing physical & environmental controls in the data center according to ISO 27001.

35.	There are no routine (daily) inspection documents for the cleanliness, temperature, humidity of the data center space.	A.11.2.9	Perform routine data center room inspections according to ISO 27001 requirements.

Risk Assessment

Risk Management is a series of processes used to manage risk which includes: risk identification, risk measurement, risk response determination, risk control activities, risk information and communication, as well as risk monitoring of every activity carried out by company.

Risks related to the Data Center within the scope of ISO 27001 XYZ compay which have been identified along with the Risk Mitigation plan are 56 issues refer to 4 categories.

TABLE 3. RISK ANALYSIS AND TREATMENT PLAN

No	Risk Category	Issues	ISO 27001 Controls (Annex)	Risk Level	Risk Treatment Plan	Residual Risk
1	Information Security	19 issues	A5 Information security policy A9 Access Control A11 Physical & environmental security A12 Operations security	Moderate to Very High	Mitigate	Moderate
2	Operational	19 issues	A5 Information security policy A9 Access Control A11 Physical & environmental security A12 Operations security	Low to High	Mitigate	Moderate

3	Project / Development	16 issues	A5 Information security policy A9 Access Control A11 Physical & environmental security A12 Operations security	Moderate to High	Mitigate	Moderate
4	Human Resources	2 issues	A5 Information security policy A9 Access Control A11 Physical & environmental security A12 Operations security	Moderate to High	Mitigate	Moderate

Control Determination and Control Targets

Statement Of Applicability (SOA) is a requirement of ISO 27001:2013. This SOA reflects the results of Company's risk assessment process and describes the scope of the ISMS implemented within the company.

The controls are designated in the same order and use the same numbering as in Appendix A of this ISO 27001 standard explaining which controls have been adopted and setting out the reasons for this decision.

Summary Statement of Applicability (SOA) Data Center Operation is as follows:

• Applicable : 105.

• Not Applicable : 9

Not applicable control in Data Center Operation are A.14.1.1 to A.14.3.1 (System acquisition, development & maintenance) caused by no development activity on Data Center Operation.

Preparation of ISMS

After determining the ISO 27001 controls and control objectives for "Information Security

Management Systems in Data Center Operations" as the scope of ISO 27001, the following are recommendations for developing an ISMS, policies, procedures and instructions that can be applied to managing information system security at the Company especially in Data Center operations.

1. Addition of Information Security Improvement KPI.

   As a form of management's commitment to improving information security, it is proposed to add 1 (one) item to the Information Technology Department's Key Performance Index (KPI) in 2023, namely: Improvement of Information Security. Included in this KPI are all activities related to improving information security, including the implementation of ISO 27001.

2. Formation of ISO 27001 Implementation Team

   Implementation of ISO 27001 is a cross-departmental activity with the Information Technology Department as the main driver. To facilitate coordination with related departments such as Quality Assurance, Electrical, Civil, Human Capital, Procurement, Corporate Communication and Security, it is proposed to form an ISO 27001 Implementation Team signed by the Main Director with the following team duties and responsibilities:

- Conduct a gap analysis, and identify an ISO 27001 implementation plan.
- Identifying the scope and objectives of implementing ISO 27001.
- Compile references for governance of business process support organizations and information technology in the form of guidelines, procedures, standards and other documents needed.
- Evaluate the implementation and plan to improve the implementation of ISO 27001.
- Carry out the certification process by an accredited certification body.
- Do other things that are necessary in connection with the duties and responsibilities of the Team.

3. Preparation of an ISMS Work Plan

   ISO 27001 Information Security Management System Work Plan is the maindocument in the implementation of ISO 27001. This document includes:

   - Vision, Mission, Scope of ISO 27001 and Management Commitment,
   - Information Security Policies, Procedures and Organizational Structure
   - Information Security Management Plan, as well
   - Support in the form of Human Resources, competence and supporting technology.

4. Preparation of IT Risk Register and Risk Management Plan

   Risks related to the Data Center as part of Company's ISO 27001 scope which have been identified along with the Risk Mitigation plan are documents that also complement the implementation of ISO 27001.

5. Completeness of ISO 27001 Documents

   For the purposes of implementing ISO 27001, it is necessary to prepare and complete all supporting documents in the form of policies, procedures, WI, Minutes and Records related to Data Center Operations.

6. Creation of ISO 27001 Master Document

   To facilitate monitoring and control of documents related to ISO 27001, a master document is created which lists all ISO 27001 documents. Any changes made to the document will be updated in this master document.

Proposed ISO 27001 Supporting Activities

Several activities related to improving information security are proposed as work programs of the Information Technology Department, including:

- Establishment of a Security Operation Center (SOC) as a device for monitoring cyber security using third party services.
- Formation of a Cyber Security Incident Response Team (CSIRT) as an emergency response team for cyber incidents, communicating with BSSN.
- Addition of Personal Information Security in IT operational services
- Carry out routine Vulnabirity Assessments and Penetration Tests (once a year)
- Drilltest related to the Disaster Recovery Plan due to cyber attacks.

Information Security Officer who is responsible for each work unit appointed by his / her supervisor (Team Leader, Factory Manager or Head of Department), performs and supports Information Security work in defined security areas and mediates issues within the organization.

CONCLUSIONS

From this case study research several conclusions can be drawn as follows following:

1. The results of measuring the maturity level using the KAMI index, the maturity level of the information system security of XYZ Company is included in the Level I+ category, up to Level II+ Category, with the final evaluation value: Fulfillment of the Basic

Framework.

2. There are 105 out of 114 controls in ISO 27001 that can be applied to the Data Center Operation Statement of Applicability (SOA). The 9 controls that cannot be applied are in A 14 (System acquisition, development & maintenance), because there are no development activities in the Data Center operations.
3. After the gap analysis was carried out, there were 35 findings that needed to be followed up for compliance with ISO 27001.
4. There are a total of 56 risks divided into 4 categories: Information Security, Operations, Project/Development and Human Resources related to Data Center operations within the scope of ISO/IEC 27001:2013 which have been identified along with their Risk Mitigation plans.
5. There are several recommendations regarding the implementation of ISO 27001 for the scope of Data Center Operations, namely:
   a. Additional Information Security Improvement KPIs
   b. Formation of ISO 27001 Implementation Team
   c. Preparation of an ISMS Work Plan
   d. Preparation of IT Risk Register and Risk Management Plan
   e. Completeness of ISO 27001 Documents
   f. Production of ISO 27001 Master Documents
   6. Proposed ISO 27001 Supporting Activities, namely:
   a. Formation of Security Operation Center (SOC)
   b. Establishment of Cyber Security Incident Response Team (CSIRT)
   c. Additional Personal Information Security in IT operational services
   d. Carrying out routine Vulnabirity Assessments and Penetration Tests

For subsequent research, an analysis can be carried out on expanding the scope of ISO/IEC 27001 to become IT service operations which cover all IT service operations in the form of application services, internet, computer equipment, printers, networks, VPN, video conferencing and telecommunications, taking into account the available resources, both in the form of human resources, budget availability, and management policies.

REFERENCES

A. Anir Norman and N. Mohd Yasin, "A Critical Review of Information Systems Security Management (ISSM) Implementation: Comparison between Stable Organizations and Emergent Organizations," *Int. J. Digit. Soc.*, vol. 1, no. 3, pp. 1–9, 2010.

A. Rojko, "Industry 4.0 Concept: Background and Overview," *Int. J. Interact. Mob. Technol.*, vol. 11, no. 5, p. 77, Jul. 2017, doi: 10.3991/ijim.v11i5.7072.

Deloitte, "Predicting the future of Cyber Security in Finnish Manufacturing Cyber Secure Manufacturing in 2021," 2018, [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/risk/Cyber Secure Manufacturing in 2021.pdf

A. Robinson, "Manufacturing and Cyber Security: A 5 Step Process to Create Internal and Customers' Peace of Mind," *Manufacturing, Technology*, 2016.

T. M. O. EEF, "Cyber Security for Manufacturing." 2018.

V. V. Fomin, H. J. de Vries, and Y. Barlette, "ISO/IEC 27001 Information System Management Standard: Exploring The Reasons for Low Adoption," *Proc. third Eur. Conf. Manag. Technol.*, no. September, 2008.

ENISA, "Enisa Lists High-Level Recommendations To Different Stakeholder Groups in Order To Promote Industry 4.0 Cybersecurity and Facilitate Wider Take-Up of Relevant Innovations in a Secure Manner. 2 Industry 4.0 Cybersecurity: Challenges & Recommendations," 2019.

C. Chazar, "Standard Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005," *J. Inf.*, vol. VII, no. 52, p. 77, 2015, doi: 10.1093/nq/s6-IX.213.77-d.

et al., "Risk Management & Mitigation Plan for Data Center Environment," *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 1260–1264, 2020, doi: 10.35940/ijrte.f7656.038620.

D. Achmadi, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center," *2018 Int. Work. Big Data Inf. Secur.*, pp. 149–157, 2018, doi: 10.1109/IWBIS.2018.8471700.

ISO, "International Standard ISO/IEC 27001 Second Edition," pp. 1–30, 2013.

C. M. Ringle, S. Wende, and J.-M. Becker, "'SmartPLS 3.' Boenningstedt," *SmartPLS GmbH*, 2015.

C. M. Ringle, M. Sarstedt, R. Mitchell, and S. P. Gudergan, "Partial least squares structural equation modeling in HRM research," *Int. J. Hum. Resour. Manag.*, 2020, doi: 10.1080/09585192.2017.1416655.

M. Sarstedt, C. M. Ringle, and J. F. Hair, "Treating unobserved heterogeneity in PLS-SEM: A multi-method approach," in *Partial Least Squares Path Modeling: Basic Concepts, Methodological Issues and Applications*, 2017. doi: 10.1007/978-3-319-64069-3_9.

Z. Awang, A. Afthanorhan, and M. Mustafa, "The Likert scale analysis using parametric based Structural Equation Modeling (SEM)," *Comput. Methods Soc. Sci.*, vol. 4, no. 1, pp. 13–21, 2016, doi: 10.5281/zenodo.1299429.

J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Second Edition*. 2017.

N. K. Avkiran and C. M. Ringle, *Partial Least Squares Structural Equation Modeling: Recent Advances in Banking and Finance*. 2018.

W. W. Chin, "How to Write Up and Report PLS Analyses," in *Handbook of Partial Least Squares*, 2010. doi: 10.1007/978-3-540-32827-8_29.

J. Cohen, "Statistical power analysis for the behavioural sciences. Hillside," *NJ: Lawrence Earlbaum Associates*. 1988.