# Data Center Information Security Analysis Based on ISO 27001:2022 Standard Using the FMEA Method at PT XYZ

**Muhammad Figo Haffidz Akbar[*1], Yopie Hidayat[2], Imelda[3]**
[1,2] Magister of Computer Science, Faculty of Information Technology, Budi Luhur University, Indonesia
[3] Master of Computer Science, Faculty of Information Technology, Budi Luhur University, Indonesia
E-mail: [*1]**2311601211@student.budiluhur.ac.id**, [2]2311600346@student.budiluhur.ac.id, [3]imelda@budiluhur.ac.id

***Abstract***

*PT XYZ is an IT distribution company playing a crucial role in supplying technology products in Indonesia. As a company operating in the field of information technology, PT XYZ has a data center that stores various critical information. Ensuring the security of data within this data center is essential, and it must be protected with adequate security standards. Following the Information Technology Security and Decision Directives of PT XYZ, an evaluation of the information security within the company's data center was conducted to achieve ISO 27001 certification for information security. This research aims to assess and evaluate the level of information security in PT XYZ's data center using the SSE-CMM assessment index and to identify the Risk Priority Number (RPN) for each identified risk using the FMEA method. The findings indicate that the maturity level of information security in the data center is at Level 3 (defined process) in the SSE-CMM model. Additionally, risk assessment using the FMEA method identified that 14 risks are in the Very Low category, 2 risks are in the Low category, and 2 risks are in the High category. The overall evaluation suggests that PT XYZ's data center is sufficiently prepared to achieve ISO 27001 certification. One recommended improvement is to periodically update the Work Instructions (WI) related to information security policies and to regularly review these security policies.*

***Keywords*** — *Data Center, FMEA, ISO 27001, Information Security, SSE-CMM*

## 1. INTRODUCTION

Information systems have a crucial role in supporting various operational activities, decision-making, and business strategies in various types of organizations, such as private companies, government agencies, and non-profit organizations. In the rapidly growing digital era, the need for a reliable information system is becoming increasingly urgent. The system is not only required to be able to process data quickly and accurately but also must provide optimal protection for information from various threats, both from inside and outside the

organization. Failure to maintain information security can cause various negative impacts, ranging from loss of strategic data, leakage of confidential information, to cyber-attacks that have the potential to cause material and reputational losses. Therefore, the implementation of integrated and effective information security management is an essential step for every organization in ensuring the confidentiality, integrity, and availability of their data [1] [2] [3] [4] .

PT XYZ manages a data center that contains critical and confidential information that must be protected to prevent security threats. Based on interviews with the company's Information Technology team, this potential attack on [5] *the data center* can cause various losses, both directly such as damage to hardware, and indirectly such as disruption to operations, marketing, and other business activities. [6]

In an effort to strengthen information security, PT XYZ is preparing for ISO 27001 certification, which is known as the international standard for information security management. This study aims to analyze the condition of information security in the company's data center, assess the completeness and maturity level of the information security system using the SSE-CMM assessment index, and evaluate the risk by calculating the Risk Priority Number (RPN) through the FMEA method. In addition, this study also provides relevant recommendations based on the ISO 27001:2022 framework to support the improvement of information security across the board. This evaluation is designed to ensure that the Information Security Management System (SMKI) can be implemented effectively, so that existing security controls are able to protect company information while providing an adequate level of trust in the protection of digital assets. ISO 27001:2022 as an international standard plays an important role in helping organizations protect information and communication technology (ICT) assets through the implementation of structured SMKI. In this study, information security was measured using the SSE-CMM model to evaluate the level of maturity of the information security system in the data center, in accordance with the ISO 27001:2022 standard. In addition, risk analysis is carried out using the FMEA method, where the results are used to support certification preparation and produce risk priority recommendations that are aligned with ISO 27001:2022. [7] [8] [9] [10] [11] [12]

Information systems evaluation covers various aspects, including the hardware, software, networking, data, and human resource capabilities involved. This evaluation aims to improve the performance, function, and quality of information system maintenance. At PT XYZ, information security is designed to protect information assets from various threats, so that it can support the company's operational sustainability, mitigate risks, and contribute to increased ROI (Return on Investment) and greater business opportunities [13] [14] .

ISO 27001:2022 has two parts, one of which is Annex A which establishes the security controls that need to be implemented in the SMKI, consisting of 14 clause areas, 35 control objectives, and 114 information security controls. Failure Mode and Effect Analysis (FMEA) is used to identify potential failures in the process with three main indicators: severity (S), occurrence (O), and detection (D), which results in a Risk Priority Number (RPN). The [15] *System Security Engineering-Capability Maturity Model* (SSE-CMM) was then used to determine the level of compliance of PT XYZ with information security standards, with a score from 0 to 5 in each selected process area. [16]

## 2. RESEARCH METHOD

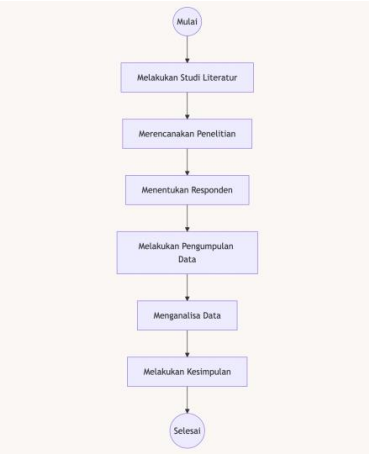



**Figure 1.** Research Method Flow

This research is carried out through several systematic stages. The first stage is to conduct a literature study using scientific journals to determine the right method, namely SSE-CMM, FMEA, and ISO 27001:2022 standards. The next stage is to design a research that focuses on the evaluation of information security in PT XYZ's data center. Furthermore, the research respondents were selected based on a specific category, and they were asked to fill out an ISO 27001:2022 evaluation assessment sheet with the SSE-CMM index approach. The data collection process is carried out through filling out an assessment and verification sheet by the selected respondents. The data obtained were analyzed with reference to the results of the ISO 27001:2022 control evaluation using the SSE-CMM index, as well as the risk assessment based on the FMEA method. The results of the analysis are then used to compile relevant recommendations. Sixth, providing conclusions and suggestions for data center information security of PT. XYZ.[17] [18] [19]

## 3. DATA COLLECTION AND PROCESSING

The first step in the data collection process is for the researcher to set the initial value on the assessment sheet to be used. This assessment sheet is then submitted to the selected respondents, accompanied by a brief introduction to the purpose and how to fill out the form. The data collection process is focused on filling out an evaluation sheet for the level of information security maturity using the SSE-CMM method. This method allows researchers to evaluate the level of maturity of the information security systems implemented in the data center [20] . The additional data collected includes information related to assets and potential risks that can pose a threat to the smooth operation of the data center. This assessment is carried out by applying the FMEA method to identify risk opportunities and their impacts. In addition, respondents were also given the opportunity to review the assessment and evidence included in

the evaluation sheet that had been provided.

The analysis model used in this study is the SSE-CMM (System Security Engineering-Capability Maturity Model) method. Calculations were made to determine the level of information security maturity using the SSE-CMM assessment index. This process involves

measuring the maturity level from level 0 to level 5 for each relevant clause area, as described in Table 1. Furthermore, the calculation of the aggregate maturity level is carried out for all selected clauses, in order to obtain an overall picture of information security achievements. [21]

**Table 1.** Maturity Level Assessment Index Criteria

| Range | Level | Information |
|---|---|---|
| **0 – 0.50** | **0** | *Not Performed* |
| **0.51 – 1.50** | **1** | *PerformedInformally* |
| **1.51 – 2.50** | **2** | *Planned&Tracked* |
| **2.51 – 3.50** | **3** | *WellDefined* |
| **3.51 – 4.50** | **4** | *QuantitativelyControlled* |
| **4.51 – 5.00** | **5** | *ContinuouslyImproving* |

The next stage of analysis involves risk assessment using the FMEA method. This assessment is carried out by considering three main aspects, namely severity, likelihood of occurrence, and detection ability. These three aspects are then multiplied to produce a Risk Priority Number (RPN) value for each data center asset item. After the RPN value is obtained, the risk rating process is carried out by classifying the risks into categories, ranging from very high to very low. This rating aims to identify risk priorities that need more attention on each data center asset. [22]

**Table 2.** RPN Criteria

| Range | Information |
|---|---|
| **0 – 25** | Very Low |
| **26 – 50** | Low |
| **51 – 75** | Medium |
| **76 – 100** | High |
| **>100** | Very High |

## 4. RESEARCH RESULTS AND DISCUSSION

### *4.1. Respondent Proof Assessment Sheet*

The questionnaire was filled out by the respondents presented in Table 3:

**Table 3.** Questionnaire Respondents

| No | Name | Position | Information |
|---|---|---|---|
| 1. | Adhitia | IT Infrastructure Team Leader | In this study, it will be filled in the proofing of assessment sheets on information security policies, system and application access control, physical entry control, control against *malware* threats, log information 3.protection, clock synchronization, operational software control, technical vulnerability management, and network security management, and FMEA. |

| | | | |
|---|---|---|---|
| 2. | Ruswandy | Team Leader IT Network | In this study, it will be filled in the proof of assessment sheets on asset management, business requirements for access control, secure areas, equipment, *backup*, *logging* and *Monitoring*. |
| 3. | Rizwan | Software and Platform Supervisor | In this study, it helps in fulfilling the proof of each clause. |

### *4.2. Information Security Policy*

In clause 5, especially sub-clause A.5.1.1, the results of the assessment sheet show that the two questions asked received a maximum score, namely 5. This is due to the existence of planning that has produced operational standards that run effectively and have been reviewed periodically. Therefore, clause 5 is considered to have a *maturity level* at level 4, which is *quantitatively controlled*.

**Table 4.** Clause 5 Assessment Sheet

| **A.5.1.1** | **Policy for Information Security** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **No** | **Statement** | **0** | **1** | **2** | **3** | **4** | **5** | **Value** |
| 1. | A set of policies for information security is already established by Management | | | | | | √ | 5 |
| 2. | The policy for information security has been communicated to employees and external parties who related | | | | | | √ | 5 |
| | Ability Level | | | | | | | 5 |

**Table 5.** Outcome of Maturity Level Clause 5

| **Clause** | **Control Objectives** | **Control Security n** | **Level Ability** | **Flat-Average/Object Control** |
|---|---|---|---|---|
| A.5 Information Security Policy | A.5.1 Management Instructions for Information Security | A.5.1.1 Policy for Information Security | 5 | 3.75 |
| | | A.5.1.2 Policy for Security Review Information | 2.5 | |
| | Value of Clause 5 | | | 3.75 |
| | Maturity Level Clause 5 | | | 4 |

### *4.3. Asset Management*

In clause 5, especially sub-clause A.5.1.1, the results of the assessment sheet show that the two questions asked received a maximum score, namely 5. This is due to the existence of planning that has produced operational standards that run effectively and have been reviewed periodically. Therefore, clause 5 is considered to have a *maturity level* at level 4, which is *quantitatively controlled*.

### *4.4. Access Control*

In clause 9, specifically in point A.9.1.1, the results of the evaluation show that of the two questions asked, the score obtained is 4. This shows that planning has been done well, resulting in standards that are defined and monitored consistently. However, there is still a shortcoming, namely that policies related to access control have not been reviewed periodically. Therefore, clause 9 is considered to have a *maturity level* at level 3, which indicates that the process is *well-defined*.

### *4.5. Physical and Environmental Safety*

In clause 11, specifically A.11.1.3, the assessment results show that out of the three questions asked, a score of 1 was obtained. This is because the security of offices, rooms, and facilities is still limited to basic practices that are carried out informally. In addition, there has been no planning or policy update that supports the security. With this condition, clause 11 is at maturity level 3, which illustrates that the process is well-defined, although it still needs further improvement.

### *4.6. Operation Security*

Clause 12, especially A.12.4.1, obtained a score of 1 from the evaluation of two questions, indicating that event logging is still carried out on a basic and informal basis without structured planning or policies. Under this condition, the clause is assessed at maturity level 3 (*well-defined*), reflecting implementation efforts that have not fully met systematic standards to support optimal operational safety.

### *4.7. Communication Security*

An assessment of clause 13, A.13.1.2, of the two questions asked, this clause obtained a score of 5. This assessment shows that the communication security planning process has resulted in standards that are well implemented, consistently monitored, and reviewed regularly. With this achievement, clause 13 is at maturity level 3 (well-defined), which reflects the implementation of structured and standard-compliant processes to support optimal communication security.

### *4.8. Results of the Discussion of Data Center Information Security Checks*

The calculation results of all clauses get a *maturity level value of* 3.25, which means that it is included in level 3, namely *Well Defined* where the definition can be controlled quantitatively, where the standard process has run according to the definition. [23]

**Table 6.** Maturity Level Calculation Results

| Clause | Maturity Level |
|---|---|
| A.5 Information Security Policy | 3.75 |
| A.8 Asset Management | 3.58 |
| A.9 Access Control | 2.83 |

| Clause | Maturity Level |
|---|---|
| A.11 Physical and Environmental Safety | 3.27 |
| A.12 Operational Safety | 2.7 |
| A.13 Communication Security | 3.33 |
| Maturity Level Value | 3.25 |

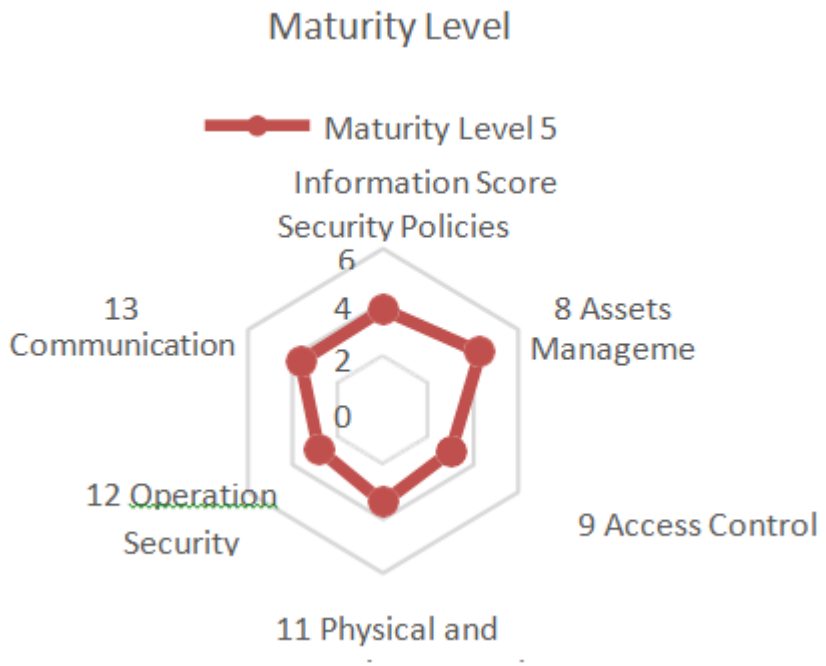



**Figure 2.** Representation of Measurement Graphs at *Maturity Level*

### *4.9. Failure Mode and Effect Analysis*

The evaluation of data center-related risks was carried out using the FMEA method, starting with data collection through an interview with one of the respondents, Helmi. The data obtained can then be grouped based on the category of information assets. The assessment sheet related to data center assets in the platform and security division was filled out by the researcher and presented in table 7, which contains PT XYZ's data center assets. . [24]

**Table 7.** PKT Data Center Assets

| Assets | Kind | Information |
|---|---|---|
| **Browse** | Information Technology Infrastructure Implementor | Information Technology infrastructure operational manager |
| | Information Systems Engineer | The workforce that designs and builds applications |

| | | |
|---|---|---|
| | IT Infrastructure & Data Center Engineer | Workforce that designs and builds IT infrastructure and Data Center |
| | Information Technology Consultant | A third-party workforce that designs and builds Infrastructure and Information Systems |
| **Data** | Business process data stored in the app | All the data that stored in the data center |
| | Data Center Assets | All asset data stored in the data center |

| Assets | Kind | Information |
|---|---|---|
| **Hardware** | Server | Application servers and Company Data |
| | Notebook Client | Computing equipment used by IT implementers |
| | Physical Security | Data security hardware center |
| | Cooling device | Hardware Data Center Cooler |
| | Supply Power | Electrical power provider hardware Data Center |
| **Software** | Operating System | Operating system is on the server |
| | Web Server Application | Web server applications Installed on the server |

In the evaluation of the three indicators adjusted to the FMEA assessment template, *the severity* assessment includes the identification of potential failure modes and the Impacts, *the occurrence* assessment in volves the identification of the causes of failure, the detection assessment includes the identification of the detection method of failure, and the proof of each indicator. [25]

### *4.9.1. People Assets*

In the people asset item, there are 4 sub-items, one of which is the IT Infrastructure Implementer which obtained an RPN value of 3, included in the *very low category*.

**Table 8.** People Asset Assessment

| ID | Item | S | O | D | RPN |
|---|---|---|---|---|---|
| People | | | | | |
| 1. | Implementation of Information Technology Infrastructure | 1 | 1 | 3 | 3 |
| Evidence of *Severity*:<br>- Not considered<br>Evidence of *Occurrence*:<br>- Almost unlikely to occur<br>Evidence of *Detection*:<br>- Easy to detect and control because the guidance was provided during the construction of the new factory, as shown in Appendix B of the ToR for Infrastructure Development, and the guidance documentation is shown in Appendix B of the Infrastructure Management Guidance. | | | | | |

### *4.9.2. Data Assets*

In the data asset item, there are 2 sub-items, one of which is Business Process Data Stored in the Application, which obtains an RPN value of 32 and is included in the *low category*.

*4.9.3. Hardware Assets*

In the hardware asset item, there are 5 sub-items, one of which is Server 1 which has an RPN value of 81, which means it is in the *high category*.

*4.9.4. Software Assets*

In the software asset item, there are 3 sub-items, one of which is the Operating System which gets an RPN value of 3, which is included in the *very low category*.

*4.9.5. Network Assets*

In the network asset item, there are 3 sub-items, one of which is the Core Network which gets an RPN value of 9, which is included in the *very low category*.

*4.9.6. Prioritization*

After calculation and ranking based on the RPN value, the risk priority for the PT. XYZ is determined to provide proposed improvements to the identified risks. The priority order is taken from items with risk levels ranging from high to low, so the focus is on higher severity risks first before moving on to lower risks.

**Table 9.** Prioritization

| Category | Item | RPN | Level | Rank |
|---|---|---|---|---|
| Network | Access network | *84* | *High* | 1 |
| Hardware | Server 1 | *81* | *High* | 2 |
| People | Consultant TI | *40* | *Low* | 3 |
| Data | Business process data stored in the application | *32* | *Low* | 4 |
| Hardware | Physical Security | *18* | *Very Low* | 5 |
| Hardware | Supply Power | *18* | *Very Low* | 6 |
| Network | Distribution Network | *15* | *Very Low* | 7 |
| People | Information Systems Engineer | *12* | *Very Low* | 8 |
| Network | Core Network | *9* | *Very Low* | 9 |
| Hardware | Perangkat pendingin | *7* | *Very Low* | 11 |
| Hardware | Server 2 | *5* | *Very Low* | 12 |
| People | IT Infrastructure & Data Center Engineer | *5* | *Very Low* | 13 |
| Data | Data center asset data | *4* | *Very Low* | 14 |
| People | Implementation of Information Technology Infrastructure | *3* | *Very Low* | 15 |
| Software | Operating System | *3* | *Very Low* | 16 |
| Hardware | Notebook Client | *2* | *Very Low* | 17 |
| Software | Web Server Application | *2* | *Very Low* | 18 |

*4.10. Recommended Data Center Assessment Sheets Using SSE-CMM*

The recommendations provided are based on the ISO 27001:2022 standard which is needed for information security in *data centers*. With the existence of the assessment and proof sheet, it can be seen the shortcomings of each ISO 27001:2022 control clause that has been selected. Recommendations are given to clauses 5, 8, 9, 11, 12, and 13 which are adjusted to the findings of each clause. Table 9 shows an example of the recommendations given for Clause 9 of Access Control.

**Table 10.** Recommended Clause 9 Access Control

| Clause | Control Objectives | Security Controls | Findings | Recommendations |
|---|---|---|---|---|
| 9 Control Access | 9.4 Access Control System and Application | 9.4.1 Restriction Access Control | Exist restriction Access information in the system and applications, but still Done informally, but there aredocumentation Distribution of rights access. | - Create a WI to limit access to information on Data Center.<br>- Create a WI for the level Access information on the data center.<br>- Use Role-Based Access Control (RBAC) for limit System Access<br>- Create a WI to limit Exodus information on Data Center |
| | | 9.4.2 Procedure Log-on Safe | Not yet Log - on, thereis documentation Log-on control, Log-On theotherhand, Done informally (none procedures and WI). | - Make Log-on procedure safe.<br>- Create a WI to Log-on successful and no succeed. |

### *4.11. Recommendations for Data Center Assessment Sheets Using FMEA*

Risks that get *high* and *low* RPN levels, namely in *people*, *hardware, and network assets*, relevant risk control recommendations will be made based on the ISO 27001:2022 control clause needed for information security in *data* centers. The following is an example of *a People asset* with an Information Technology Consultant item:

**Table 11.** People Asset Recommendations

| ASSET CATEGORIES | ITEMS | RISK IDENTIFICATION | CONTROL RECOMMENDATIONS |
|---|---|---|---|
| *Browse* | *IT Consultant* | *Lost Business Opportunity* | *A.7.1.1 Screening*<br>*A.7.2.2 Information security alert* |

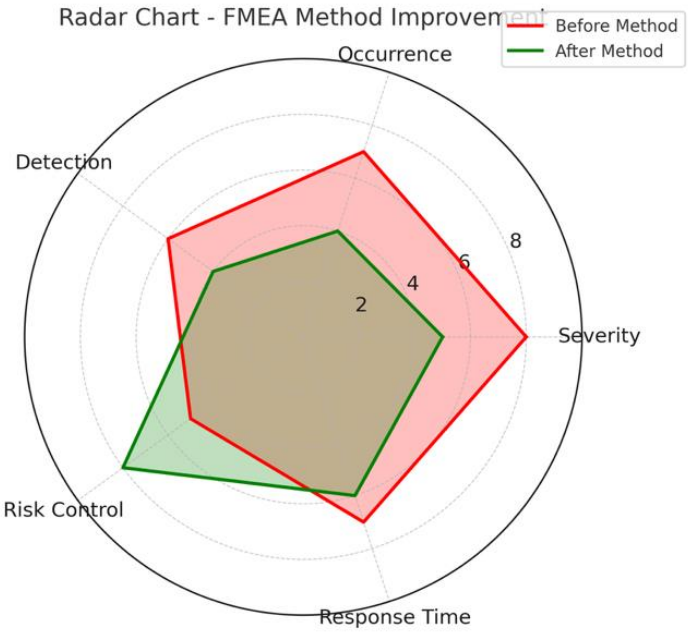



**Figure 3.** Chart Radar FMEA Method

The radar chart illustrates a comparative analysis of system performance before and after applying the proposed method. The chart evaluates multiple dimensions, including Accuracy, Reliability, Risk Reduction, Efficiency, and Adaptability. From the visualization, the baseline (before applying the method) exhibits lower and imbalanced performance across the evaluated dimensions. For example, risk reduction and adaptability remain weak, while accuracy and reliability also show only moderate results. After implementing the proposed method, the chart demonstrates a significant improvement across all dimensions, with the plotted area becoming larger and more balanced. Accuracy and reliability increase considerably, indicating a more consistent output. Risk reduction shows the most prominent improvement, highlighting the method's effectiveness in minimizing potential failures. Efficiency and adaptability also rise, which reflects that the method not only strengthens the system but also makes it more flexible against varying conditions.

Overall, the radar chart confirms that the proposed method contributes to a more robust, reliable, and adaptive system. This graphical evidence supports the claim that the method provides tangible benefits compared to the baseline approach.

## 5. CONCLUSIONS AND SUGGESTIONS

Based on the results of research conducted on the data center of PT. XYZ, it canbeconcludedthat:

1. Information Security Completeness and Maturity Level:

   The level of information security of the data center of PT. XYZ is considered quite high by being at level four (defined process). The details are as follows:

   - Information security policy clauses are at level four (quantitativelycontrolled).
   - The asset management clause is at level four (quantitativelycontrolled).
   - Access control clauses are at level three (definedprocess).
   - The physical and environmental security clauses are at the third level

(definedprocess).

- The operation security clause is at the third level (definedprocess).
- The communication security clause is at level four (managed).

2. Data Center Risk Assessment with FMEA Method:
   Risk assessment of PT. XYZ produces:
   - 14 risks are in the Very Low category with the highest RPN value of 18.
   - 2 risk is in the Low category with the highest RPN value of 40.
   - 2 risks are in the High category with the highest RPN valueof 84.
3. Recommendations for Improving Information Security.
   Based on the analysis, several recommendations have been prepared to improve the information security of PT. XYZ more optimally. These recommendations are designed according to the findings of each clause to ensure continuous improvement and effective risk control:
   - Information security policies are at level 2 (*RepeatableButIntuitive*), soitisnecessarytocreate*WorkInstruction* (WI) toupdate the information security policy periodically and conduct a scheduled review of the information security policy to ensure relevance and effectiveness.
   - Asset inventory is rated level 4 (*Managed*), soitis recommended to manage the information cycle including creation, processing, storage, transmission, deletion, and destruction, as well as create asset use rules that include employees and third parties with access to information assets.
   - Access control is at level 3 (*DefinedProcess*), itisrecommendedtouse*Role-Based Access Control* (RBAC) andcreate a WI for access restrictions, secure log-on procedures, and log-on logging both successful and failed.
   - Physical and environmental security is at level 3 (*DefinedProcess*), soitis necessary to create a WI for physical security testing and monitoring, improve the quality of monitoring physical entry records, prepare room and facility security planning documents, and protect from external and environmental threats.
   - Operation security is at level 3 (*DefinedProcess*), soitis necessary to create a WI for*eventlogging*anditsreview, create a WI for log information protection, and synchronize time as a single reference for all systems.
   - Communication security is at level 4 (*Managed*), soitis necessary to create a WI for risk assessment with additional controls on the public network used.

The suggestions from this study to be carried out in the next research are as follows:

1. Data center *information security* needs to be continuously improved and improved to minimize various potential threats related to data center security. Therefore, data center security evaluations need to be carried out periodically to ensure the effectiveness of thesecuritymeasuresimplemented.
2. Future research is suggested to consider theuseof*maturitymodels*andalternativerisk assessment methods as comparative materials, so as to enrich more comprehensive analyses and outcomes.

## 6. REFERENCES

[1] M. Malatji, "Management of enterprise cyber security: A review of ISO/IEC 27001:2022," in *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, IEEE, Jan. 2023, pp. 117–122. doi: 10.1109/CyMaEn57228.2023.10051114.

[2] H. Taherdoost, "Cybersecurity vs. InformationSecurity," *ProcediaComputSci*, vol. 215, pp. 483–487, 2022, doi: 10.1016/j.procs.2022.12.050.

[3] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," in *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, IEEE, Feb. 2020, pp. 1–3. doi: 10.1109/NCETSTEA48365.2020.9119914.

[4] R. Sinaga, "The Application of ISO/IEC 27001:2022 in Information Systems Security Governance: Process Evaluation and Constraints," 2024. [Online]. Available: https://journal.fkom.uniku.ac.id/ilkom

[5] Dr. C. Sunitha and R. R, "Analysis of ISO/IEC 27001:2013-Information Security Management System in an Organization," *International Journal of Research Publication and Reviews*, vol. 4, no. 10, pp. 3316–3329, Oct. 2023, doi: 10.55248/gengpi.4.1023.102841.

[6] S. F. Aboelfotoh and N. A. Hikal, "A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises," *JOIV: International Journal on Informatics Visualization*, vol. 3, no. 2, pp. 157–176, May 2019, doi: 10.30630/joiv.3.2.239.

[7] D. Achmadi, Y. Suryanto, and K. Ramli, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center," in *2018 International Workshop on Big Data and Information Security (IWBIS)*, IEEE, May 2018, pp. 149–157. doi: 10.1109/IWBIS.2018.8471700.

[8] T. Aprianto, I. Setiawan, and H. H. Purba, "Implementation of Failure Mode and Effect Analysis method in Industry in Asia – Literature Study," *MATRIX*, vol. 21, no. 2, p. 165, Mar. 2021, doi: 10.30587/matrik.v21i2.2084.

[9] A. Kusnandar, "Evaluation of Information System Security Using Fuzzy FMEA Based on ISO/IEC 27001:2013 Framework to Improve Information Security," *Journal of Business Information Systems*, vol. 14, no. 2, pp. 181–190, Apr. 2024, doi: 10.21456/vol14iss2pp181-190.

[10] F. Özsungur, "Business Management and Strategy in Cybersecurity for Digital Transformation," 2021, pp. 144–162. doi: 10.4018/978-1-7998-6975-7.ch008.

[11] M. Alim, I. Rasyid Munthe, and A. Putra Juledi, "Evaluation of Information System Security in a Digital Business Environment," *Journal of Computer Science and Information Systems (JIKOMSI)*, vol. 7, no. 1, pp. 328–332, Mar. 2024, doi: 10.55338/jikomsi.v7i1.3088.

[12] A. P. Subriadi and N. F. Najwa, "The consistency analysis of failure mode and effect analysis (FMEA) in information technologyriskassessment," *Hell*, vol. 6, no. 1, Jan. 2020, doi: 10.1016/j.heliyon.2020.e03161.

[13] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluation of Information Technology Security Using the Information Security Index 5.0 and ISO/EIC 27001:2022," *SAINTEKOM Journal*, vol. 14, no. 1, pp. 84–94, Mar. 2024, doi: 10.33020/saintekom.v14i1.623.

[14] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluation of Information Technology Security Using the Information Security Index 5.0 and ISO/EIC 27001:2022," *SAINTEKOM Journal*, vol. 14, no. 1, pp. 84–94, Mar. 2024, doi: 10.33020/saintekom.v14i1.623.

[15] I. G. P. K. Juliharta, N. K. S. Febriani, and K. Q. Fredlina, "EVALUATION AND RECOMMENDATION OF SPBE INFORMATION SECURITY MANAGEMENT SYSTEM (SMKI) GUIDELINES AT XYZ AGENCY," *Journal of Information and Computer Technology*, vol. 9, no. 1, Jan. 2023, doi: 10.36002/jutik.v9i1.2348.

[16] A. C. Wicaksono, S. Prabowo, and D. Oktaria, "Risk and Security Measurement Based on ISO 27001 Using FMEA Methodology Case Study: National Government Agency," in *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, IEEE, Nov. 2022, pp. 6–11. doi: 10.1109/ICoSEIT55604.2022.10029988.

[17] M. Aldenny, H. Kristian, F. L. Gaol, T. Matsuo, and A. Nugroho, "The Implementation of Failure Mode and Effects Analysis (FMEA) of the Information System Security on the Government Electronic Procurement Service (LPSE) System," 2022, pp. 1–12. doi: 10.1007/978-981-16-5640-8_1.

[18] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM Journal*, vol. 33, no. 7, pp. 76–105, Dec. 2021, doi: 10.1108/TQM-09-2020-0202.

[19] Y. S. Triana and R. A. M. Pangabean, "Risk Analysis in the Application of Financore Information Systems Using FMEA Method," in *JournalofPhysics: ConferenceSeries*, IOP Publishing Ltd, Jan. 2021. doi: 10.1088/1742-6596/1751/1/012032.

[20] Mayank Hindka, "Design and Analysis of Cyber Security Capability Maturity Model," *International Research Journal of Modernization in Engineering, Technology and Science*, Mar. 2024, doi: 10.56726/IRJMETS50400.

[21] A. Kusnandar, A. F. Rochim, and V. Gunawan, "Measurement of Information Risk and Security Levels Using the ISO/IEC 27001-Based FMEA Method in XYZ Agencies for Information System Security," *Journal of Business Information Systems*, vol. 14, no. 4, pp. 375–384, Oct. 2024, doi: 10.21456/vol14iss4pp375-384.

[22] Abram Leonard, "Information System Security Risk Management E-Learning Using FMEA in University," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 5, pp. 7565–7568, Oct. 2020, doi: 10.30534/ijatcse/2020/93952020.

[23] P. Nuchpho, S. Nansaarng, and A. Pongpullponsak, "Modified Fuzzy FMEA Application in the Reduction of Defective Poultry Products," *Engineering Journal*, vol. 23, no. 1, pp. 171–190, Jan. 2019, doi: 10.4186/ej.2019.23.1.171.

[24] L. P. S. Hartanti, J. Mulyono, and V. Mayang, "APPLICATION OF FMEA AND FUZZY FMEA IN LEAN WASTE RISK ASSESSMENT IN THE MANUFACTURING INDUSTRY," *JST (Journal of Science and Technology)*, vol. 11, no. 2, pp. 293–304, Aug. 2022, doi: 10.23887/jstundiksha.v11i2.50552.

[25] J. Balaraju, M. Govinda Raj, and C. S. Murthy, "Fuzzy-FMEA risk evaluation approach for LHD machine-A case study," *JournalofSustainable Mining*, vol. 18, no. 4, pp. 257–268, Nov. 2019, doi: 10.1016/j.jsm.2019.08.002.