*JINAV: Journal of Information and Visualization* *ISSN: 2746-1440 (online)*
*Vol. 5 No. 1 (2024)*
https://doi.org/10.35877/454RI.jinav2747

# Recommendations for a Framework for Handling Security Incidents of Electronic-Based Government Systems (SPBE) using the ISO/IEC 27035:2023 Standard

Stefanus Lugas Prastowo* & Dodi Sudiana

*Master of Electrical Engineering Department, Faculty of Engineering, Universitas Indonesia, Depok, 16424, Indonesia*

**Abstract**

The rapid development of Electronic Government Systems (EoBS) has brought significant improvements in the efficiency and accessibility of public services. However, the increasing reliance on these systems has also increased concerns about their security and the potential impact of security incidents on government operations and citizen trust. In order to address these challenges, this study proposes a framework for handling security incidents using the ISO/IEC 27035:2023 standard as a reference. The ISO/IEC 27035:2023 standard provides a comprehensive approach to incident management, covering the entire life cycle from preparation and identification to containment, eradication, and recovery. The recommended institution is the Ombudsman of the Republic of Indonesia, a government institution that carries out the function of overseeing the implementation of public services and receiving public complaints regarding alleged maladministration of public services. The preparation of the framework begins with a thorough analysis of the Ombudsman's existing security practices and potential threats to its electronic systems. This assessment is used as a basis for ensuring that the proposed solution is tailored to the specific needs and vulnerabilities of the institution. The stages carried out are preparation, identification, containment, eradication, recovery, and lessons learned. The recommendations produce a framework and insights that government agencies can use to adopt the ISO 27035:2023 standard. This study also shows that the implementation of the standard is relevant and in line with the SPBE policy in Indonesia.

*Keywords:* electronic government system (SPBE), security incident management, ISO/IEC 27035:2023, indonesian ombudsman.

Received: 14 February 2024 Revised: 27 June 2024 Accepted: 16 July 2024

## 1. Introduction

Electronic materials have brought significant improvements in the efficiency and accessibility of public services. However, increasing reliance on these systems has also led to increasing concerns about their security and the potential impact of security incidents on government operations and citizen trust (Bohme, 2013). Implementing information security policies and controls in all types of organizations is a must. This has a positive impact on government agencies to improve services for users. The Indonesian Ombudsman is a government institution with the task of supervising public services, which in carrying out its duties and authority is based on the principle of confidentiality.

In carrying out this function, the Indonesian Ombudsman utilizes an electronic system for managing public complaint data. However, the use of electronic systems does not escape information security threats. To ensure that information can be distributed in a timely, valid, and targeted manner, the Indonesian Ombudsman is required to have high service availability and reliability.

As the number of public complaints against public services increases, the Indonesian Ombudsman needs to improve the information security system so that public complaint data can be accounted for in terms of confidentiality integrity and availability (CIA). If the security system is not managed properly, it will result in financial loss, reputation, disruption to business continuity and loss of life.

In protecting government agencies from the threat of incidents, BSSN evaluates the Indonesian Ombudsman through a Cyber Security Maturity assessment (CSM). This assessment aims to determine the maturity level of stakeholders in

* Corresponding author.
*E-mail address*: stefanus.lugas@ui.ac.id

handling cyber security incidents and is expected to provide what should be the follow-up by both stakeholders and the National Cyber and Crypto Agency (BSSN) to improve the ability to handle cyber security incidents. In the assessment results report, there are three electronic systems that are categorized as High risk.

Following up on this occassion, risk-analysis and incident management design are required. These can be used as a guide in implementing incident handling at the Indonesian Ombudsman, which has been recognized or standardized in Indonesia and becomes a reference in handling incidents by government agencies. The design of an incident management framework can be prepared based on ISO/IEC 27035:2023 and become a reference for BSSN in National Cyber and Crypto Agency Regulation Number 10 of 2020 concerning Cyber Incident Response Teams. With the availability of information security incident management using ISO/IEC 27035:2023, it is expected that it can improve the Indonesian Ombudsman's information security system (“Information Technology-Information Security Incident Management,” 2023).

## 2. Method

In this research, qualitative and quantitative methods were used. A qualitative approach can help the researchers comprehend the understanding of employees involved in handling incidents, while a quantitative approach can provide data that can be measured in identifying existing patterns. The implementation of qualitative methods in this research is a case study, which is used to obtain information on activities and processes by the incident handling team in handling incidents so that they can be adapted to the ISO/IEC 27035:2023 framework. In the quantitative method, assessment of electronic system assets with a high category carried out by BSSN in the CSM assessment is used to identify the risk analysis. Data sources used primary data and secondary data. Primary data was obtained by interviews and observations. Secondary data was obtained through related scientific literature, journals and books.

## 3. Result and Discussion

Information data obtained through interviews with officials and employees who were directly involved was used as supporting data in creating a framework for handling SPBE incidents.

Asset Assessment was carried out on the electronic system of Ombudsman RI in the Cyber Security Maturity (CSM) activity conducted by BSSN in 2023. This assessment was used to categorize the risk level of electronic systems based on the National Cyber and Crypto Agency Regulation No. 8 of 2020 concerning Security Systems in the Implementation of Electronic Systems. From the assessment of 23 electronic systems at the Indonesian Ombudsman, the results were five electronic systems in the High Category and eighteen electronic systems in the low category, and there were no electronic systems in the Strategic Category.

### *3.1. Risk Assessment*

Risk assessments were carried out on Electronic System assets in the High Category based on Ombudsman Regulation Number 54 of 2022 concerning Risk Management within the Indonesian Ombudsman. This risk assessment is carried out in two major stages, risk identification and risk analysis.

#### *3.1.1. Risk Identification*

Risk identification was carried out by identifying and describing all things that have the potential for risk, both originating from internal and external factors according to table 1.

At this stage, the context is filled in according to the strategic targets of the business processes of the work unit whose risks want to control. The method for achieving SPIP objectives is a selection of the four SPIP objectives as stated in Government Regulation Number 60 of 2008 concerning the Government Internal Control System.

#### *3.1.2. Risk Analysis*

Risk analysis is a stage for determining risk levels, sorting risks based on levels and compiling risk maps.

In table 2, the results of the probability assessment are given a value of 3 (Sometimes Happens) considering that from the interview results regarding the frequency of downtime that occurs in 1 year it occurs quite often (6 times to 9x), with an impact score of 5 which is considered Very Significant because apart from affecting KPI, it is feared that the institution's reputation will also decrease and increase to negative coverage in national and international mass media. Considering that, there is personal data from the public that is embedded in the High Category Electronic System. Because there is no control, this risk has an unchanged Residual Risk Value, namely 22 (Very High Risk Level).

**Table 1**. Conformity Context

| No | Type of Context | Context Name | Indicator | Risk Code | Risk Statement | Risk Category | Impact Description | Achievement Method SPIP objectives |
|---|---|---|---|---|---|---|---|---|
| 1. | Performance Agreement | Implementation of quality Information Technology services | Electronic system service SLA 95% | HMTI.5.4 | High Category Electronic System Server is Down | Operational Risk | Applications are inaccessible and organizational services are disrupted | Securing State Assets |

**Table 2**. Risk Maps

| **Code** | **Risk Statement** | **Inherent Risk Score/Value** | | | **Existing Controls** | | | **Residual Risk Score/Value after Control** | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Probability Score | Impact Score | Risk Level | Yes/Not yet | Description | Adequate/ Not yet | Probability Score | Impact Score | Risk Level |
| HMTI.5.4 | High Category Electronic System Server is Down | 3 | 5 | 22 | Not yet | - | Inadequate | 3 | 5 | 22 |

The next step is to create a Root Cause Analysis. In table 3 to conclude the root cause of the risk statement. From the investigation, several factors were found that influenced the High Category Electronic System in a down condition, including vulnerabilities that caused the system to be hacked, hardware constraints and building electrical constraints. Then from the statement, the cause was pursued again until the root cause of not having a security incident response plan for SPBE was found.

**Table 3**. Root Cause Analysis

| **Risk Statement** | **Why 1** | **Why 2** | **Why 3** | **Root Cause** | **Cause Code** | **Control Activities** |
|---|---|---|---|---|---|---|
| High Category Electronic System Server is Down | - system vulnerabilities<br>- Hardware constraints<br>- Electrical constraints | - There are no regular monitoring activities<br>- Outdated server<br>- no UPS | Do not have an incident response plan | Does not have a SPBE incident response plan | HMTI.5.4. MC.4 | Preparation of SPBE security incident response framework |

*3.2. Framework Recommendation*

From results analysis, several steps were done, which can followed in planning information security incident management framework for the Indonesian Ombudsman based on the ISO/IEC 27035:2023 standard. The design of this framework aims to assist the Indonesian Ombudsman through the Planning phase and Preparation (Plan and prepare), Detection and reporting (detection and reporting), Evaluation and decision (assessment and decision), Responses and lessons learned in dealing with the threat of information security incidents, and ensuring the security of agency information data ,

BSSN as the SPBE security development agency also issued BSSN Regulation Number 1 of 2024 concerning Cyber Incident Management, which contains a Cyber Incident Management Guide. This can be a supplement to recommendations for a framework for handling cyber incidents.

*3.2.1. Planning and Preparation (Plan and Prepare)*

Effective information security incident management necessitates thorough planning and preparation. It's crucial to maintain composure throughout all stages of incident response and to ensure the response time is carefully managed. Failure to do so can prolong the incident's duration, potentially exacerbating its negative impact on the organization.

*a. Determination Security Policy Information*

Information security incident management policy in accordance with objectives and needs Indonesian Ombudsman. This policy covers responsibilities, procedures and reporting of information security incidents. This process aims to ensure that information security incident management was carried out consistently and effectively, which included allocating tasks and responsibilities related to handling information security incidents and weaknesses. An overview of the policies that organizations must make according to ISO 27035:2023 recommendations, it can be seen in Table 4.

**Table 4.** Identification Policy

| No | Policy | Information |
|---|---|---|
| 1. | Appointment of Incident Management Team and Incident Coordinator | - Senior management is committed to fully supporting the effective implementation and maintenance of the ISMS, including information security incident management.<br>- A competent information security incident management person must be appointed to lead and manage the ISMS program. |
| 2. | SPBE Risk Management Policy | - Organizations must conduct comprehensive and ongoing information security risk assessments to identify information assets, threats, vulnerabilities and potential impacts.<br>- Based on the results of the risk assessment, the organization should develop and document a comprehensive risk management strategy, including appropriate prevention and control measures to minimize the likelihood and impact of an information security incident. |
| 3. | Training Program and Information Security Awareness Program | - An ongoing information security training and awareness program should be implemented for all employees, including senior management, staff and contractors.<br>- This training should cover important topics, such as: Introduction to ISMS and information security incident management policies, Information security incident recognition and reporting, Incident response procedures, Information security controls and best practices, as well as Awareness of information security threats and vulnerabilities |
| 4. | Incident Response Policy | - Organizations must develop and document clear and structured procedures and guidelines for information security incident management.<br>- These documents should include: Definition and classification of information security incidents, Incident reporting and escalation processes Incident response teams and their roles and responsibilities, Incident investigation and analysis procedures, Incident response and recovery actions, Post-incident documentation and learning<br>- This policy should be reviewed and updated periodically to reflect changes in the business environment, information technology, and information security threats.<br>- Records and documentation related to information security incident management must be stored properly and easily accessible for auditing and learning purposes. |
| 5. | Collaboration with external stakeholders | - Effective communication channels must be established to facilitate the reporting, investigation and coordination of information security incidents.<br>- The organization must establish communication and coordination with relevant internal and external parties, such as law enforcement, security vendors, and the public, if necessary. |

*b. Identification of Vulnerability and Incident*

Identification of vulnerabilities is very important to prevent similar incidents in the future and to learn lessons for better handling. Incident and vulnerability data was taken from January - June 2024 as follows:

**Table 5.** Identification of Vulnerability and Incident

| No | Electronic System Security Incident / Vulnerability Report | Information | Recovery efforts |
|---|---|---|---|
| 1. | Social Media Phishing | The social media admin at one of the Indonesian Ombudsman Representative Offices was phished and resulted in his Instagram account being hacked. | It was not handled because the account had already been taken over by the attacker. |
| 2. | Web Defacement | Defacement on the main website ombudsman.go.id in the leadership profile section. From the results of the investigation, it was discovered that the attacker carried out the action from CMS using a leaked account of one of the admins. | Remove defacement content and deactivate affected user accounts. |
| 3. | Remote access/shell backdoor | Found a shell backdoor on the server of one of the e-office applications | Remove backdoor shells and other malicious files from the server. |
| 4. | Phishing mail | phishing attacks on employee emails | Conduct outreach to all employees about the dangers of phishing emails and how to identify phishing emails. |
| 5. | Judol Defacement Web | one of the web-based applications that is no longer in use installed online gambling web content | Disabling the affected site. |
| 6. | Credential leak | Employee usernames and passwords leaked on the darkweb | Create notifications to affected users to immediately change passwords |
| 7. | Bottleneck / Performance Issue in Core Business Applications | The Core Business Application (SIMPEL) which was installed at the Kominfo National Data Center (PDN) experienced performance problems (slow) and received complaints from all employees | Move the application to the office server |
| 8. | Building power failure | Electrical problems at the MCB of the Indonesian Ombudsman building resulted in the server being completely down | Moving and reinstalling applications to colocation |
| 9. | Forgery of electronic documents | Forgery of letters with digital signatures of leaders | Disseminate electronic certificates to all employees |

The cases in table 5 show the importance of regularly identifying vulnerabilities to prevent security incidents. This can be done by conducting a security audit, system scanning, and penetration testing. Employees need to be equipped with knowledge about cyber security and how to identify threats, such as phishing and malware. This can be conducted with regular training and education as well as creating an incident response plan (Malik, 2021).

*c. Creating an Incident Response Plan*

To resolve an incident, a guide is required to assist the IRT in the process of handling the incident.

*d. Formation Team Incident Response*

The Indonesian Ombudsman has formed the Ombudsman-CSIRT with the registration number BSSN 022/CSIRT.01.01/BSSN/06/2021. BSSN facilitates the formation of CSIRT in the Ombudsman as a follow-up in handling information security incidents and acts as a Cyber Incident Response Team / IRT in every government agency.

Apart from IRT, ISO/IEC 27035:2023 also recommends the formation of a new role, namely the Incident Management Team (IMT), which aims to focus on incident management planning and prevention.

*e. Making Procedure Handling and Evaluation Incident Security Information*

Creating procedures is important in handling information security incidents that occur at the Indonesian Ombudsman, so that the impact of incidents can be minimized and prevent incidents from recurring. This procedure aims to serve as a guideline in ensuring rapid detection of weaknesses and incidents as well as rapid follow-up and response to incidents at the Indonesian Ombudsman.

*f. Reporting Incident in System Security Information*

All Indonesian Ombudsman personnel and third parties report identified information security incidents as quickly as possible through the incident reporting mechanism at the Indonesian Ombudsman as shown in Figure 1.

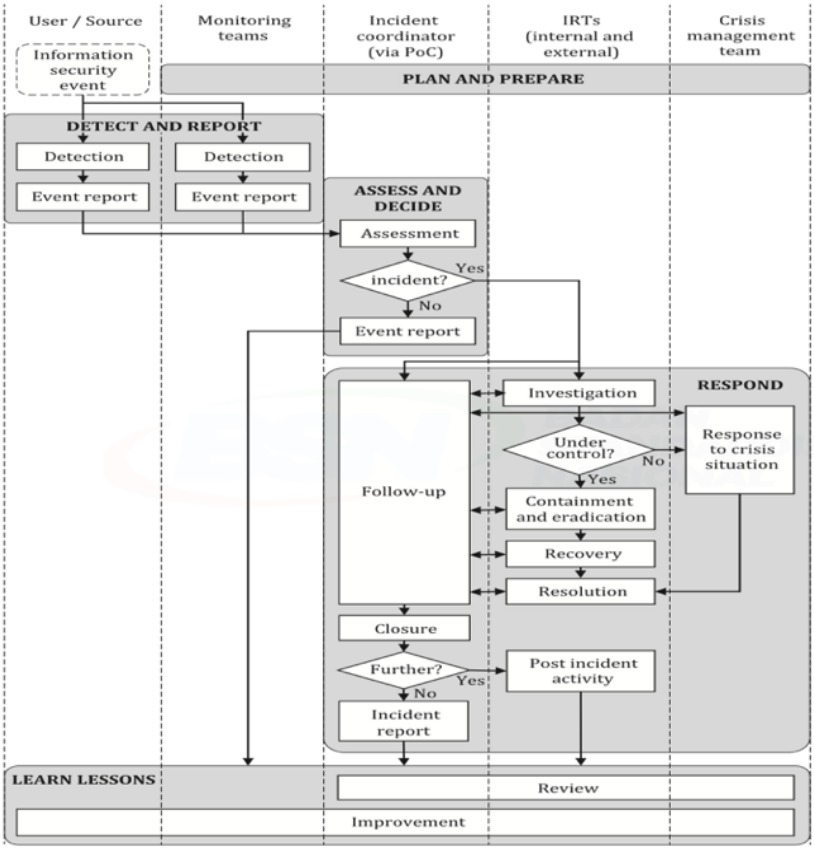


**Figure 1.** Diagram channel incident and incident security information (ISO 27035-2:2023, 2023)

In Figure 1, it is shown that incident reporting is carried out according to the phases in ISO 27035:2023 starting from the planning and preparation phase, which contains documents and guidelines. Then phase detection and reporting containing process detection was done by IRT team or from reporter to PoC, next evaluation and a decision on the incident by the Incident Coordinator, then followed up with a resolution response incident by team housewife, if need higher escalation, so the IRT team will coordinate with BSSN. After the incident is closed, the IRT team will document report and evaluate document incident in a way periodically.

Communication is the key. The organization should promote incident management as a “no-fault” reporting process to empower personnel to come forward and report incidents without the fear of retribution. Focus should instead be on the positive outcomes that an organization can gain from receiving incident reporting, learning and improving from incidents to become more secure and resilient.

#### *3.2.2. Detection And Reporting*

The second phase of information security incident management involves detection, collection information, which related with reporting incident security event information and the existence of information security vulnerabilities manually or automatically. In this phase, events and vulnerabilities may not yet be classified as information security incidents.

#### *3.2.3. Assesment and Decision*

Fourth phase management incident security information are assesment and decision. Incident coordinator evaluates the event based on the report and declares whether it is an incident or not (false alarm). The incident coordinator must elaborate on incident priorities and incident categorization with internal regulations in the organization.

#### *3.2.4. Response*

Fourth phase management incident security information involve response against information security incidents in accordance with the actions specified in the Assessment phase and Decision.

The IRT will determine whether the information security incident can be controlled, if so, then the IRT takes incident control steps in the form of:

- Containment
  Minimize the impact and prevent further damage from the incident that occurred
- Correction
  Make necessary incident repairs.
- Root cause analysis
  Take corrective action to eliminate the cause of the incident (corrective action). Corrective steps are needed so that the incident does not happen again in the future.

If cyber incident occurs that disrupts the core business services of the Indonesian Ombudsman, then incident handling can refer to BSSN Regulation Number 2 of 2024 concerning Cyber Crisis Management.

#### *3.2.5. Lessons Learned*

Fifth phase of management Lessons can be learned from one or many reported information security incidents or security vulnerabilities. It is critical that lessons learned are correlated to the information security management change capabilities that make business decisions and, if deemed necessary, include proposed modifications in the information security management improvement process.

Incident reports should indicate various situations that lead to various actions that will be carried forward to the information security management improvement process. The report should also make improvements to the information security incident management plan and documentation based on lessons learned.

## 4. Conclusion

The Indonesian Ombudsman is currently facing various challenges related to information security, including potential threats to the electronic system used to store and manage public complaints. This system is the backbone and work facility for Indonesian Ombudsman employees in providing transparent and trustworthy services to the public and BSSN has labeled the electronic system with this high category. Based on risk calculations and analysis from the electronic system, it produces a probability score of 3, an impact score of 5 and a risk level of 22 (Very High). After carrying out a root cause analysis, it was found that the root cause of the risk was the absence of an incident response plan, so it was necessary to prepare a SPBE security incident response framework. Recommendations for the SPBE security incident management framework in the Indonesian Ombudsman can go through the phases of Planning and Preparation, Detection and Reporting, Assessment and Decision, as well as Response and Lessons Learned in accordance with the ISO/IEC 27035:2023 standard proposed in this research.

## References

Akkiyat, I., & Souissi, N. (2019). Modelling Risk Management Process According to ISO Standard. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(2), 5830–5835. https://doi.org/10.35940/ijrte.B3751.078219

Bohme, R. (2013). *The Economics of Information Security and Privacy* (R. Böhme, Ed.). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0

Fathurohman, A., & Witjaksono, R. W. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering*, *1*(1), 1–11. https://doi.org/10.25008/bcsee.v1i1.2

Information Technology-Information security incident management. (2023). *Part 2 : Guidelines to Plan and Prepare for Incident Response*, *I*.

ISO 27035-2:2023. (2023). *Information Technology-Information security incident management - Part 2 : Guidelines to plan and prepare for incident response*.

Kristanto, T., Sholik, M., Rahmawati, D., & Nasrullah, M. (2019). Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ. *JISA(Jurnal Informatika Dan Sains)*, *2*(2). https://doi.org/10.31326/jisa.v2i2.497

Malik, M.S. (2021). *Cybersecurity Incident Response and Management* (pp. 32–44). https://doi.org/10.4018/978-1-7998-4162-3.ch002

Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45–69. https://doi.org/10.1016/j.cose.2014.11.006

Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. *Computer Fraud & Security*, *2021*(1), 14–19. https://doi.org/10.1016/S1361-3723(21)00009-9

Singh, J., & Cobbe, J. (2019). The Security Implications of Data Subject Rights. *IEEE Security & Privacy*, *17*(6), 21–30. https://doi.org/10.1109/MSEC.2019.2914614

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security*, *45*, 42–57. https://doi.org/10.1016/j.cose.2014.05.003

Wahyuni, S., Raazi, I. M., & Dwitawati, I. (2022). Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit. *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *5*(1), 49–55. https://doi.org/10.32672/jnkti.v5i1.3962