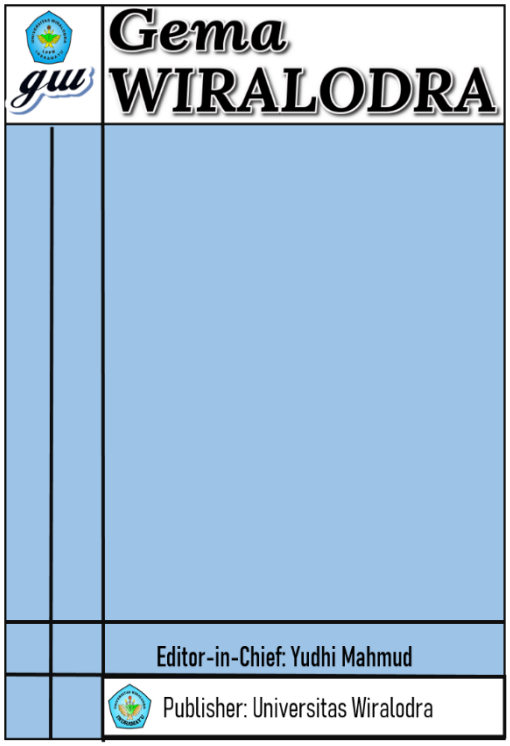
Gema Wiralodra

Publication details, including instructions for authors and subscription information:
https://gemawiralodra.unwir.ac.id



Information security incident management using iso 27035 standard

Ignatius Frank Zinatra Poetiray[a], Muhammad Salman[b]
University Indonesia, Indonesia,
ignatius.frank@ui.ac.id
University Indonesia, Indonesia,
salman@eng.ui.ac.id

To cite this article:
Poetiray, I.F.Z & Salman, M. (2023). Information security incident management using iso 27035 standard. *Gema Wiralodra, 14*(3), 1069-1078.
To link to this article:
https://gemawiralodra.unwir.ac.id/index.php/gemawiralodra
Published by:
Universitas Wiralodra
Jln. Ir. H. Juanda Km 3 Indramayu, West Java, Indonesia

Gema Wiralodra, 14(3), 1069-1078
https://gemawiralodra.unwir.ac.id/index.php/gemawiralodra
p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

Orginal Article

Information security incident management using iso 27035 standard

Ignatius Frank Zinatra Poetiray[a], Muhammad Salman[b]
University Indonesia, Indonesia, ignatius.frank@ui.ac.id
University Indonesia, Indonesia, salman@eng.ui.ac.id

Submit 11-06- 2023, accepted 18-09-2023, published 19-09-2023
*Corresponding author: ignatius.frank@ui.ac.id

Abstract
The data and information management process at BMKG entails certain risks related to information security incidents. There needs to be more emphasis on addressing these incidents regarding policies, procedures, technology, and human resources. This research project aims to develop an incident management system by ISO 27035 standards. Qualitative research methods have been employed for BMKG Communication Network Center case studies. The approach involves aligning information security incident management with BMKG's business processes. The outcome of this research includes creating policies, documents, and standardized procedures designed to enhance BMKG's capabilities in effectively managing and mitigating incident threats.
Keywords: Risk, Information Security Management, Incident, ISO 27035

1. Introduction

The imperative need for public access to vital information aligns closely with the rapid advancements in information technology. Consequently, implementing robust information security policies and controls has become an unequivocal necessity across diverse organizational landscapes (Böhme, 2013). This practice profoundly benefits government agencies, empowering them to elevate their service delivery to end-users. The Meteorology, Climatology, and Geophysics Agency (BMKG) stands as a governmental institution entrusted with the responsibility of furnishing the public with comprehensive information services spanning Meteorology, Climatology, Air Quality, and Geophysics (MKKuG) (BMKG, 2023).

In strict accordance with Law No. 31 of 2009, governing Meteorology, Climatology, and Geophysics, BMKG bears the mandate of disseminating MKKuG information, data services, and early warnings to pertinent stakeholders and the broader public. In executing this pivotal function, BMKG relies extensively on the BMKG Communication Network Center. While BMKG leverages its official website as a conduit for information dissemination to the public, it is paramount to recognize that websites remain susceptible to information security threats. The government, cognizant of the profound importance of safeguarding public interests against disruptions arising from the misuse of electronic information and electronic transactions, has proactively addressed this concern through Government Regulation No. 71 of 2019, particularly encapsulated within Article 94 (Elektronik, 2016).

Ensuring the punctual, precise, and targeted distribution of information necessitates that BMKG uphold an elevated service availability and reliability level. The specter of information security incidents looming over the data and information management process engenders a significant risk for the BMKG Communication Network Center. A failure to diligently manage these threats within a timely framework can precipitate financial losses, tarnish the organization's reputation, and instigate disruptions to business continuity (Singh & Cobbe, 2019; Tosun, 2021).

The BMKG Communication Network Center has substantially invested in fortifying its technological infrastructure, with expenditures consistently increasing each fiscal year. The escalating threat of information security incidents targeting government entities remains a

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

persistent concern, as underscored by data from the cyberthreat.id website. Notably, this source reported 741,441,648 cyberattacks that besieged Indonesia between January and July 2021. Significantly, these attacks are characterized by a 45.5 percent incidence rate against the government sector, followed by 21.8 percent in the financial sector, 10.4 percent in telecommunications, transportation, and law enforcement, and 2.1 percent directed at other state-owned enterprises (NEWS: First Half of 2021, Number of Cyber Attacks in Indonesia Reaches 741.44 Million, Exceeding Last Year's Total Attacks, Cyberthreat.Id, nd).

The pivotal role played by proficient human resources (HR) emerges as one of the most critical and vulnerable aspects of information security incident management (Stewart & Jürjens, 2017; Maglaras et al., 2018). In this context, it is incumbent to establish and disseminate policy guidelines and procedures governing the management of information security incidents. This proactive measure is paramount to ensure the seamless continuity of BMKG's mission and functions in delivering essential public services, ultimately exerting a pivotal influence on public trust and the agency's overarching reputation. Many standards and guidelines focusing on incident management stand readily available, and numerous variables interplay in gauging the efficacy of an organization's response to an information security incident.

2. Methods

To enhance information security incident management at the BMKG Communication Network Center, the researchers adopted a qualitative research approach. Qualitative research focuses on understanding complex phenomena by collecting and analyzing non-numerical data, such as written or spoken words derived from observations (Firmansyah et al., 2021).

To comprehensively investigate the intricacies of information security at BMKG, the researchers employed a mix of data collection methods: (1). Literature Study: They initiated their research by conducting an extensive literature review. This phase involved delving into academic publications, relevant documents, and materials concerning information security incident management, ISO 27035 standards, and the specific operations of BMKG. (2). Observation: A crucial aspect of the research involved on-site observations at the BMKG Communication Network Center. By directly witnessing the center's activities, processes, and potential vulnerabilities, the researchers gained invaluable insights into the real-world operations of information security. (3). Interviews: To gain a comprehensive understanding of the perspectives and experiences of key stakeholders, experts, and BMKG personnel involved in information security, the researchers conducted interviews. These interviews served as a means to collect qualitative data through dialogues and discussions.

The researchers then embarked on a qualitative analysis with the data collected through these diverse methods. This analytical phase involved identifying recurring patterns, themes, and concepts within the data. By doing so, the researchers aimed to gain a deep and nuanced understanding of the current state of information security management at BMKG and its specific challenges.

3. Results and Discussion

Basic Information Concepts

According to Ismail & Awaludin (2017), information refers to processed data to have more significant value for the recipient. In general, information can be interpreted as the result of processing data converted into a more helpful form and has a more significant meaning for the recipient. The source of information is data. Data is reality that describes events that occurred at a particular time.

Definition of Information

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

Information is data that has been processed into a valuable form for the recipient and has a value that can be understood in current and future decisions (Mardi, 2014). Meanwhile, Heriyanto (2018) stated: "Information is the result of data processing, but not all results can be Information because Information must have meaning, significance, and benefits relevant for the individual. The data processing results that do not provide purpose or meaning and are not helpful for a person cannot be categorized as that person's information.

From the definitions above, it can be concluded that information is data that has been processed and converted into a valuable form for the recipient. The information must have meaning, significance, and benefits relevant to the individual to be categorized as information. Data processing results that do not provide meaning, meaning, or benefit to a person cannot be considered information for that person. Thus, information plays a vital role in decision-making and influencing the future.

Information Characteristics

Information is the result of data processing. Various parties widely use information to find out something and make decisions based on that information. To make the right decision, good information is needed. In order to produce good information, specific characteristics are needed. According to Romney in Mardi (2014), the characteristics of information are as follows:

a) Relevant information must have high meaning so that it does not raise doubts for those who use it and can be used appropriately to make decisions.
b) Reliable information must have high reliability; the information used as a decision-making tool is an actual event in the company's activities.
c) Complete The Information must have a detailed and clear explanation of every aspect of the event involved.
d) Timely All Information must be updated, so it is essential for decision-making.
e) Understandable: Information presented in a clear form will make it easier for people to interpret it.
f) Verifiable: This Information does not have an ambiguous meaning. It has the same understanding of the user.

Syaifullah (2018) said that characteristic information must have the following characteristics:

a) Accurate information must reflect the actual situation.
b) Timely information must be available or available when the information is needed, not tomorrow or not in a few hours.
c) Relevant: The Information provided must be what individuals at various levels and parts of the organization need.
d) Complete information must be provided completely. For example, there is no monthly sales information or invoice data.

Information Security

Through observations and interviews, the risk that has occurred is that *server downs* occur every month and make the BMKG system inaccessible, which impacts employee performance because they cannot input and send data. Then, there is the risk of *connection errors* with user IDs on the system caused by the internet network being down, and for this reason, the provider is slow to respond; this impacts the BMKG system being inaccessible and hampering employee performance productivity. Climatology station. Apart from that, we also experienced the threat of human error risk in the data input process; this impacted the average calculation results during data analysis carried out by climatology station employees, making the data inaccurate. Another threat that can disrupt the information security of other agencies is that it can result in more significant losses and disrupt the agency's business processes and operations.

Risk management of information technology assets is required to maintain information security and reduce losses. An organization must pay high attention to maintaining the integrity of information technology assets to avoid damage loss and remain well managed. Considering technological developments, risk cannot be avoided (Megawati et al., 2022).

ISO 27035 standard

ISO/IEC TR 18044 has been updated to become ISO/IEC 27035:2005 and adopted as the basis for standardizing SNI 7512:2008 by the Indonesian National Standardization Agency (BSN). This standardization contains information technology – security techniques – management of information security incidents.

ISO/IEC 27035-1:2016 is the basis of an International Standard which consists of several parts. This standard presents the basic concepts and phases of information security incident management. It combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents and applying lessons learned.

The principles provided in ISO/IEC 27035-1:2016 are general and are intended to apply to all organizations, regardless of type, size, or nature. Organizations can adapt the guidance provided in ISO/IEC 27035-1:2016 according to the type, size, and nature of their business about information security risk situations. This applies to external organizations providing information security incident management services (ISO, 2016).

The ISO/IEC 27035 series provides additional guidance for incident management controls in ISO/IEC 27002. These controls should be implemented based on the information security risks an organization faces. Information security policies or controls alone do not guarantee total protection of information, information systems, services, or networks. After controls are implemented, residual vulnerabilities may remain that can reduce the effectiveness of information security and facilitate the occurrence of information security incidents. This could have detrimental or indirect consequences for the organization's business operations.

Additionally, new instances of previously unidentified threats may inevitably lead to incidents. Inadequate preparation by an organization to handle such incidents makes any response less effective and increases potential adverse business consequences. Therefore, it is critical for any organization that desires a robust information security program to have a structured and planned approach to:

a) planning and preparing for information security incident management, including policies, organization, plans, technical support, awareness and skills training, etc.;
b) Detect, report, and assess information security incidents and vulnerabilities associated with such incidents;
c) responding to information security incidents, including activation of appropriate controls to prevent, mitigate, and recover from impacts;
d) Appropriately address reported information security vulnerabilities related to incidents;
e) Learn from information security incidents and the vulnerabilities involved in those incidents, implement and verify preventive controls, and make improvements to the overall approach to information security incident management.

The ISO/IEC 27035 series is intended to complement other standards and documents that guide investigating and preparing to investigate information security incidents. The ISO/IEC 27035 series is a partial guide. However, it refers to certain fundamental principles and established processes intended to ensure that tools, techniques, and methods can be selected appropriately and proven fit for purpose when necessary.

Although the ISO/IEC 27035 series covers information security incident management, it also covers several aspects of information security vulnerabilities. Guidance on vulnerability

disclosure and vendor handling of vulnerabilities is also provided in ISO/IEC 29147 and ISO/IEC 30111.

The ISO/IEC 27035 series also intends to inform decision-makers when determining the reliability of digital evidence presented to them. This applies to organizations that must protect, analyze, and present potential digital evidence. This standard is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

Role and Function of the BMKG Communication Network Center in Information Management and Security

According to Hartanto et al. (2022), the Meteorology, Climatology, and Geophysics Agency carries out the functions of (1) Formulating national policies and general policies in the fields of meteorology, climatology, and geophysics; (2) Formulation of technical policies in the fields of meteorology, climatology, and geophysics; coordinating policies, plans, and programs in the fields of meteorology, climatology and geophysics; (3) Implementation, guidance and control of observations, and processing of data and information in the fields of meteorology, climatology and geophysics. (4) Data and information services in the fields of meteorology, climatology and geophysics; (5) Submission of Information to agencies and related parties as well as the public regarding climate change; (6) Submission of Information and early warnings to agencies and related parties as well as the public regarding disasters due to meteorological, climatological and geophysical factors; (7) Implementation of international cooperation in the fields of meteorology, climatology and geophysics; (8) Implementation of research, assessment and development in the fields of meteorology, climatology and geophysics; (9) Implementation, guidance and control of instrumentation, calibration and communication networks in the fields of meteorology, climatology and geophysics; (10) Coordination and cooperation on instrumentation, calibration and communication networks in the fields of meteorology, climatology and geophysics; (11) Implementation of education and training in government expertise and management in the fields of meteorology, climatology and geophysics; (12) Implementation of professional education in the fields of meteorology, climatology and geophysics; (13) Implementation of data management in the fields of meteorology, climatology and geophysics; (14) Guidance and coordination of the implementation of administrative tasks within the BMKG; (15) Management of state property/wealth which is the responsibility of BMKG; (16) Supervision of the implementation of tasks within BMKG; (16) Submission of reports, suggestions and considerations in the fields of meteorology, climatology and geophysics. (17) In carrying out its duties and functions, BMKG is coordinated by the Minister responsible for the transportation sector.

Information Security Management Designed for the BMKG Communication Network Center based on the ISO 27035 standard.

The Communication Network Center of the Meteorology, Climatology, and Geophysics Agency (BMKG) can design information security incident management based on the ISO 27035 standard. ISO 27035 is an international standard that guides information security incident management. The following are several steps that can be followed in designing information security incident management for the BMKG Communication Network Center based on the ISO 27035 standard:

a) Policy Determination: Determine an information security incident management policy that meets BMKG's goals and needs. This policy should cover information security responsibilities, procedures, and incident reporting.

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

b) Threat Identification and Incident Range: Identify various information security threats that may occur in the BMKG communications network. Review the range of potential incidents covering the types of attacks and threats that may occur.
c) Risk Assessment: Conduct a risk assessment to identify and evaluate potential vulnerabilities in the BMKG communications network system. Review the possible impact if an information security incident occurs.
d) Creation of an Incident Response Plan: Create an incident response plan that includes the steps to be taken when an information security incident occurs. This plan should include recovery actions, damage mitigation, service restoration, and investigations.
e) Establishment of an Incident Response Team: Form an incident response team of members trained in handling information security incidents. Define the roles and responsibilities of each team member.
f) Reporting and Monitoring: Establish procedures for reporting information security incidents and ongoing monitoring of incidents as they occur. Ensure a transparent reporting system and monitoring mechanism to identify information security incidents quickly.
g) Evaluation and Improvement: Regularly evaluate information security incidents and incident management processes. Review the performance of the incident response team the effectiveness of the incident response plan, and identify areas of improvement that may be needed.

In addition to the above steps, ensuring that the management of information security incidents complies with the requirements and guidelines of ISO 27001 on overall information security management is essential. In this way, the BMKG Communication Network Center can increase the reliability and security of its network system by implementing information security incident management by the ISO 27035 standard.

1.

4. Conclusion

2. The BMKG Communication Network Center can design an information security incident management system in alignment with the ISO 27035 standard. This management framework involves a series of essential steps to ensure the security and resilience of their network systems, safeguard sensitive information, and mitigate the impact of potential information security incidents. These critical steps encompass (1) Establishing Policies: The initial phase involves formulating comprehensive information security policies. These policies serve as a foundational framework outlining the principles and guidelines for securing sensitive data and responding to security incidents effectively. (2) Identifying Threats and Incident Ranges: A crucial aspect is identifying potential threats and delineating incident ranges. This entails a meticulous assessment of the types of security threats the BMKG Communication Network Center may face, encompassing a broad spectrum of possible scenarios. (3) Risk Assessment: A comprehensive risk assessment is essential to gauge the severity and likelihood of different security threats. This step aids in prioritizing resources and efforts based on the identified risks. (3) Creating an Incident Response Plan: Developing a well-structured incident response plan is paramount. This plan outlines the precise procedures to be followed when an information security incident occurs, ensuring a coordinated and effective response. (4) Forming an Incident Response Team: Assembling a dedicated incident response team is essential. This team comprises experts and stakeholders who will lead and execute the incident response plan when required, ensuring a swift and effective resolution. (5) Reporting and Monitoring: Timely reporting of security incidents and continuous monitoring of network systems are crucial components. This real-time vigilance enables the quick detection and containment of security breaches, minimizing potential damage. (6) Evaluation and Improvement: The final step involves a post-incident evaluation to assess the effectiveness of the response and identify areas for improvement. This iterative process ensures that the incident management system evolves and becomes more resilient.

3. By adhering to the ISO 27035 standard and implementing this comprehensive information security incident management framework, the BMKG Communication Network Center can significantly enhance the reliability and security of its network systems. Moreover, this approach enables them to proactively protect sensitive information and minimize the potential impact of information security incidents, bolstering their overall cybersecurity posture.

5. References

BMKG. 2023. Meteorology, Climatology and Geophysics Agency. (nd).

Böhme, R. (2013). The economics of information security and privacy. In *The Economics of Information Security and Privacy*. https://doi.org/10.1007/978-3-642-39498-0

Electronics, T. (2016). *about System*.

Firmansyah, M., Masrun, M., & Yudha S, IDK (2021). The Essence of the Difference between Qualitative and Quantitative Methods. *Elasticity - Journal of Development Economics, 3* (2), 156–159. https://doi.org/10.29303/e-jep.v3i2.46

Hartanto, B., Astriawati, N., Supartini, & Yekti, DK (2022). Search and use of information from the Meteorology, Climatology, and Geophysics Agency (BMKG). *INSOLOGY: Journal of Science and Technology, 1* (5), 553–564.

Heriyanto, Y. (2018). Design of a Web-Based Car Rental Information System at PT. APM Rent Car. *Intra-Tech Journal, 2* (2), 64–77.

Ismail, I., & Awaludin, M. (2017). Implement a Warehouse and Multi Outlet Management Information System Based on Hybrid Technology at Cindy The Smilling Gift Shop Jakarta. *CKI On SPOT , 10* (2), 66–73.

p-ISSN: **1693 - 7945**
e –ISSN: **2622 - 1969**

ISO. (2016). *Part 1: Principles of incident management*.

Maglaras, L., Drivas, G., Noou, K., & Rallis, S. (2018). NIS directive: The case of Greece. *ICST Transactions on Security and Safety*, *4* (14), 154769. https://doi.org/10.4108/eai.15-5-2018.154769

Mardi. (2014). *Accounting Information Systems* (2nd ed.). Ghalia Indonesia.

Megawati, Nisa, F., Hamzah, ML, & Maita, I. (2022). Bmkgsoft System, Security Risk Management Analysis, Using the OCTAVE-S Method. *Scientific Journal of Information Systems Engineering and Management*, *8* (1), 62–67.

NEWS: First Half of 2021, Number of Cyber Attacks in Indonesia Reaches 741.44 Million, Exceeding Last Year's Total Attacks | Cyberthreat. id. (nd).

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

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information and Computer Security*, *25* (5), 494–534. https://doi.org/10.1108/ICS-07-2016-0054

Syaifullah, M. (2018). Quality of Accounting Information Systems. *Journal of Accounting and Business Research*, *10* (2), 136–150.

Tosun, OK (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76* (April), 101795. https://doi.org/10.1016/j.irfa.2021.101795