Journal of Information Systems and Informatics
Vol. 6, No. 2, June 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i2.717 Published By DRPM-UBD

Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis

Arif Faizal[1], Ahmad Luthfi[2]

[1,2] Informatics Department, Indonesian Islamic University, Yogyakarta, Indonesia
Email: [1]21917024@students.uii.ac.id, [2]ahmad.luthfi@uii.ac.id

Abstract

To ensure a comprehensive and scientifically rigorous analysis, adhering to standardized procedures serves as the foundation of any investigation. In the realm of digital forensics, the establishment of well-defined protocols for generating exhaustive reports to analyze digital evidence holds paramount importance. These reports not only carry significance in legal contexts but are also increasingly valuable across various industries for internal purposes. Esteemed organizations like the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) have played a pivotal role in shaping recognized standards in this domain. The primary goal of this report is to conduct an in-depth comparison between two prominent digital forensics standards: ISO/IEC 27037, widely embraced in industries, and NIST SP 800-86, predominantly prevalent in academic circles. Through this comprehensive analysis, the report aims to provide valuable insights to Digital Evidence First Responders (DEFR), including law enforcement, academia, and industry professionals. By elucidating the discrepancies, scopes, and limitations inherent in each standard, DEFRs can bolster their understanding, thus empowering them to make well-informed decisions during digital investigations. Future works in this field should focus on the continual evolution of digital forensic practices, adapting to new technologies and challenges, and ensuring that standards remain up to date with the dynamic digital landscape.

Keywords: NIST SP800-86, ISO 27037, digital evidence framework, digital forensic standard.

1. INTRODUCTION

The use of a standard for a framework in an organization requires a measurement to assess the effectiveness and maturity of the implementation of the standard. This measurement can be used to track the progress of the organization in implementing the standard, and to identify areas where improvements can be made. Some of the factors that can be measured include the level of compliance with the standard, the effectiveness of the organization's processes, and the satisfaction of the organization's stakeholders [1].

The integrated implementation of forensic standards offers a multitude of benefits, ranging from enhanced comprehensiveness to elevated quality in forensic investigations. By skillfully applying one forensic standard in conjunction with another or seamlessly integrating both standards, forensic investigators gain a substantial advantage in conducting highly effective and efficient investigations [2]. Such a comprehensive approach empowers them to navigate complexities with utmost proficiency, ensuring meticulous scrutiny and strategic analysis of digital evidence, ultimately leading to more robust outcomes and greater success in their investigative endeavors. The measurement of the implementation of a standard can be a valuable tool for organizations that are committed to improving their information security practices. By tracking their progress and identifying areas where improvements can be made, organizations can ensure that they are implementing the standard effectively and that they are protecting their information assets from unauthorized access, use, disclosure, disruption, modification, or destruction [3].

The use of this standard enables organizations to reduce risks, either by reducing the likelihood or impact of the risk, or both, for risks associated with the limitations of the standard used [4]. This can be achieved by identifying and addressing the limitations of the standard used. In situations where a standard falls short of encompassing all the potential risks an organization might encounter, the organization could find it necessary to devise supplementary controls to address and mitigate those specific risks effectively. Alternatively, when a standard lacks explicit directive on risk mitigation strategies, seeking guidance from an expert might be indispensable for crafting a well-structured plan tailored to the organization's unique circumstances [5]. One of the potential guidance provided by standards includes the concept of decision-making, outlining choices or steps through a flowchart or framework [6], as depicted in the illustration Figure 1.

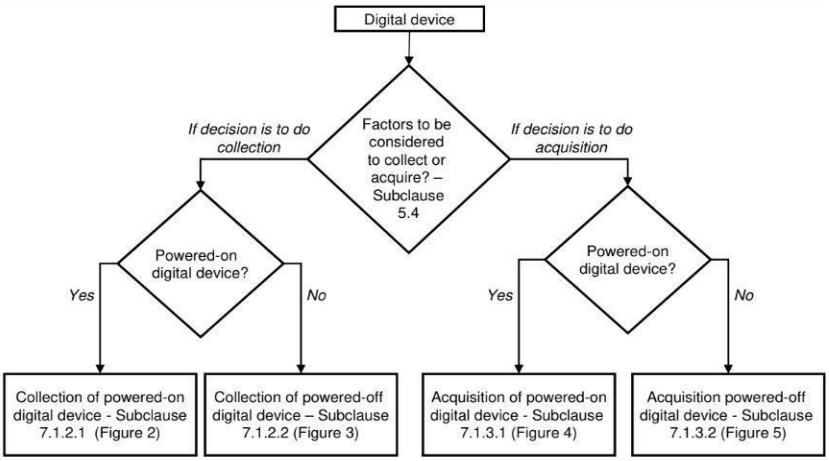

Figure 1. Decision Making Framework

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

By identifying and addressing the limitations of a standard, organizations can reduce the risks they face and protect their assets. One of the implications of using these standards is an organization's ability to mitigate risks by either reducing the likelihood of their occurrence, minimizing their impact, or a combination of both, concerning issues related to the limitations imposed by the standard being employed [7].

In the realm of forensic practices, guidelines play a pivotal role as a fundamental framework for reference. The selection of appropriate guidelines tailored to the specific field becomes an unavoidable consideration. In practice, choosing the right guidelines becomes a critical factor in executing forensic investigations with utmost effectiveness and efficiency [8]. These guidelines serve as the bedrock for well-structured and dependable investigative procedures, ensuring the integrity and precision of investigation outcomes. By adhering to suitable guidelines, forensic processes can be executed with a more targeted and comprehensive approach, leading to meaningful and reliable results applicable in various legal, security, and information management contexts [9].

The significance of establishing standardized guidelines for digital evidence analysis cannot be overstated. These standards serve as a cornerstone for ensuring the integrity, consistency, and reliability of the investigative process, fostering trust and transparency within the legal system [10], [11]. Two prominent standards that have gained widespread recognition and adoption are the NIST SP 800-86 and the ISO/IEC 27037.

NIST SP 800-86, provides a comprehensive framework for conducting digital forensics investigations. It outlines a structured approach encompassing the identification, preservation, collection, examination, analysis, and reporting of digital evidence [11]. The guide emphasizes the importance of maintaining a documented chain of custody to ensure the evidentiary trail remains unbroken and verifiable. ISO/IEC 27037 delves specifically into the handling and preservation of digital evidence. It establishes best practices for ensuring the integrity and authenticity of evidence throughout the investigative process [12]. The standard outlines procedures for identifying relevant evidence, collecting it without compromising its state, acquiring it in a forensically sound manner, and preserving it securely to prevent any alterations or loss.

There are many strong advantages to digital forensics practitioners adhering to these standards, like NIST SP 800-86 and ISO/IEC 27037. In the first place, it ensures that evidence is handled and examined consistently and reproducibly by promoting standardization and consistency throughout investigations. Maintaining the integrity of the judicial system and guaranteeing the admission of evidence in court proceedings depend heavily on this consistency. Further, these standards improve the dependability and legitimacy of digital

evidence [13]. Investigators can reduce the possibility of contaminating evidence or making mistakes when handling and analysing it by adhering to established protocols. This in turn reinforces the prosecution's case and the evidentiary basis of the investigations.

Furthermore, established techniques promote collaboration and knowledge exchange among digital forensics investigators. Investigators can successfully communicate findings, share expertise, and stay up-to-date on evolving methodologies and technology when they use a shared language and structure. This collaborative approach fosters continual advancement in the field of digital forensics[13][14]. The importance of standards such as NIST SP 800-86 and ISO/IEC 27037 in directing the digital evidence analysis process cannot be overemphasized. These standards establish a solid framework for safeguarding the integrity, consistency, and dependability of digital evidence, thereby aiding in the pursuit of justice in the digital age [15]. Their widespread acceptance by digital forensics practitioners is critical to preserving the credibility and effectiveness of digital investigations.

2. METHODS

To obtain the comparison results of the two standards used in this research, a descriptive method was employed. This method utilized a literature review of the NIST SP 800-86 document, which was then compared with the ISO 27037 document. In this research, the descriptive method was used to provide a detailed and systematic overview of the phenomena or objects under study. The approach involved analyzing the literature of both standards, NIST SP 800-86 and ISO 27037, with a particular focus on the digital forensics acquisition process [16].
The steps in the descriptive method for this research may include:
Thoroughly reading NIST SP 800-86 and ISO 27037 to understand their context, scope, and objectives[15].

1) Identifying sections in the documents that pertain to the digital forensics acquisition process.
2) Noting and examining the guidelines, procedures, and recommendations provided in each document related to the acquisition process.
3) Comparing and analyzing the differences and similarities between the two standards in the context of the acquisition process.
4) Organizing the comparison results in the form of narrative or tables to present a clear understanding of the differences and similarities between the two standards.

The outcome of this descriptive method is expected to provide a deeper understanding of the commonalities and differences between NIST SP 800-86 and ISO 27037:2012 regarding the digital forensics acquisition process. Additionally,

these results may serve as a foundation for further research or practical implementation in the field of digital forensics[17].
To obtain the comparison results of the two standards used in this research, a descriptive method is employed. This method involves a literature review of the NIST SP 800-86 document, which will be contrasted with the ISO 27037 document.

2.1. NIST SP 800-86

The National Institute of Standards and Technology (NIST) SP 800-86 standard provides general guidelines for the handling of electronic and/or digital evidence. The standard focuses on the acquisition of computer forensic evidence, and the guidance is still relevant for the handling of digital evidence as of the date of this report. The standard provides guidance on the following topics: identification, collection, preservation, examination, and reporting of electronic and/or digital evidence[18][11].

NIST SP 800-86 provides clear guidelines for the handling of electronic and/or digital evidence in general. Despite this, the guidance remains relevant and reliable for addressing cyber-attacks on smart homes[18]. The investigation process outlined by NIST encompasses the stages of collection, examination, analysis, and reporting, as depicted in the figure below.

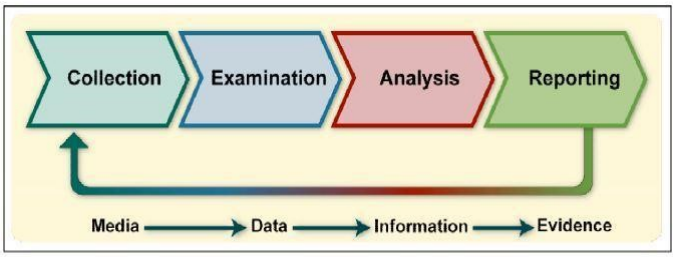

Figure 2. NIST SP 800-86 Framework

The guidance offered by NIST is firmly rooted in rigorous research, meticulously capturing both its merits and limitations, and subsequently disseminated through scholarly publications[19]. The iterative enhancement of the quality and validity of this guidance is a testament to the scientific rigor embedded in its development methodology[20].

2.2. ISO 27037

ISO/IEC 27037 is an internationally recognized standard that offers comprehensive recommendations for the effective management of electronic evidence. It encompasses critical aspects, including the identification, collection,

acquisition, and preservation of electronic evidence that holds potential probative value, i.e., its capacity to establish or refute facts in legal proceedings[21]. Electronic evidence encompasses diverse data types like computer files, emails, text messages, and social media posts.

This standard equips organizations with valuable guidance on preserving the probative value of electronic evidence throughout its lifecycle. It emphasizes the need to safeguard evidence against any alterations or destruction, ensuring its accessibility for thorough analysis. Additionally, the standard addresses specific or unique scenarios that may arise during electronic evidence management, such as dealing with evidence dispersed across multiple jurisdictions[22]. Its comprehensive approach establishes a reliable framework for handling electronic evidence in a manner that upholds its integrity and admissibility in legal proceedings. The standard is specifically developed to assist organizations in fulfilling their legal requirements and ensuring that the management of electronic evidence aligns with widely accepted best practices in the field [23]. ISO/IEC 27037 provides recommendations for specific tasks in the management of electronic evidence, including identification, collection, acquisition, and preservation of electronic evidence that may have probative significance.

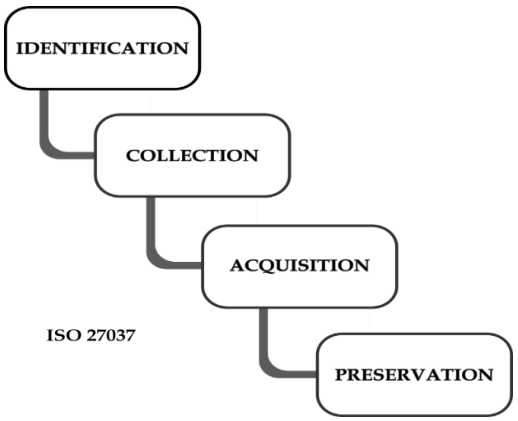

Figure 3. ISO 27037 Framework

This standard offers guidance to organizations regarding specific or unique scenarios they may encounter during the management of electronic evidence, helping them establish disciplined protocols and facilitating the possibility of conducting analysis on electronic evidence across different jurisdictions [24]. In the context of managing digital evidence, this standard encompasses several critical aspects, namely auditability, justifiability, and either repeatability or reproducibility, contingent upon the specific field conditions [25].

A proficient and experienced DEFR should possess the capability to perform all procedures outlined in the documentation and achieve consistent results without the need for external guidance or interpretation [26]. However, the DEFR must be mindful that certain situations may prevent the possibility of repeating a specific test, such as when an original hard drive has been copied and reintroduced for use, or when dealing with items involving volatile memory. In such instances, the DEFR must ensure the reliability of the acquisition process. To ensure repeatability, it is crucial to establish quality control measures and maintain comprehensive documentation of the entire process [27].

2.3. Differences

In order to facilitate a more profound comparison, a comprehensive table encompassing the aforementioned standards is presented below. Table 1 is thoughtfully designed to offer a holistic view of the commonalities and differences between the standards, as well as their respective limitations. It is envisioned that this table will provide practitioners with clearer guidance in comprehending the intricacies and relevance of both standards, assisting in making strategic decisions pertaining to digital security and evidence management.

Table 1. Process Summarizes

No	Comparison	NIST SP 800-86	ISO 27037
1	Investigation	N/A	Available
2	Collection	Available	Available
3	Examination	Available	N/A
4	Analysis	Available	N/A
5	Acquisition	N/A	Available
6	Preservation	N/A	Available
7	Reporting	Available	N/A

The analysis of the table reveals that both standards, NIST SP 800-86 and ISO 27037, share similarities in the data collection phase of forensic investigations. However, significant differences arise in other critical stages, including examination, analysis, acquisition, preservation, and reporting[28]. While NIST SP 800-86 may primarily focus on aspects related to digital evidence collection[29], ISO 27037 offers a more comprehensive and holistic guidance[30].

NIST SP800-86 and ISO 27037 are two widely recognized information security standards. Despite their differing focus, these two criteria are critical in directing the analysis of digital evidence[31][32]. This comprehensive comparison examines the various perspectives that distinguish NIST SP 800-86 and ISO 27037, putting light on their distinct contributions to the complex process of digital evidence analysis. This comparison reveals the strengths and nuances of each standard by examining the methodologies they advocate, the investigative approaches they

promote, the identification processes they recommend, the acquisition techniques they endorse, the analysis methods they support, and the reporting guidelines they establish [33]. This allows for a better understanding of their complementary roles in the pursuit of justice in the digital age. Here's a comparison of the two standards from several perspectives as shown in Table 2.

Table 2. A Comprehensive Framework Focus

No	Feature	NIST SP 800-86	ISO 27037
1	Main focus	Guide to computer forensic investigation and incident response	Standard for information security management systems (ISMS)
2	Objective	Provides a structured framework for digital forensic investigations, from identification to reporting	Establish requirements for effective implementation and maintenance of ISMS
3	Target User	Digital forensic investigators, incident response team	Organizations that want to improve their information security posture

A thorough awareness of these variances and similarities enables forensics practitioners to select the guidelines that are most appropriate for their organization's needs and specific investigative scenarios, eventually enhancing the efficiency and efficacy of forensic operations [34]. While NIST SP 800-86 and ISO/IEC 27037 are both important digital forensic standards, their fundamental objectives and guiding principles differ [35]. The following explanation will demonstrate how each standard influences digital forensic investigation procedures, as well as potential outcomes and variances in efficiency.

These standard addresses various subjects, the first of which is Standardization Methodology. Well-defined protocols for identification, preservation, collecting, inspection, analysis, and reporting [36]. The second component is the Chain of Custody, which has a standard scope and includes traces of specific documentation to show the evidence's integrity throughout the investigation [37].

The use of measures to prevent random or deliberate changes to digital evidence is covered in the third part of the read-only acquisition process, followed by forensic tools and procedures that deal with using special tools for in-depth analysis to reveal buried information and recreate timelines[38]. It enables researchers to blend data from several sources to form a comprehensive picture of the issue.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 3. Key Aspects of Digital Evidence Analysis

No	Feature	NIST SP 800-86	ISO 27037
1	Standardized Methodology	Promote a structured approach consisting of six stages: identification, preservation, collection, inspection, analysis, and reporting	Emphasizes risk management and risk assessment, which can be applied in prioritizing digital evidence checks
2	Chain of Custody	Recommend approaches like keyword search and hashing to discover relevant digital evidence.	Encourages data classification based on sensitivity to help identify digital evidence.
	Read-Only Acquisition	Emphasizes the need of maintaining custody chains and employing read-only acquisition procedures to ensure evidence integrity.	It does not specifically address evidence collecting, but its principles can be used to assure good evidence processing.
3	Forensic Tools and Techniques	Recognize the use of specialist forensic instruments and techniques for thorough analysis.	Instead, then directly discussing evidence analysis, emphasis is placed on correct documentation and reporting.
4	Data Correlation	It necessitates extensive and well-documented reporting, including methodology, instruments employed, analysis results, and chain of custody.	It does not directly address the reporting of digital evidence, but the principles can be used to ensure accurate and concise reporting.

While there isn't necessarily a significant difference in the outcome of a digital forensics' investigation based solely on the standard used (both aim to uncover evidence), their efficiency in different aspects may vary [39], [35]. NIST SP 800-86 offers a broader and more comprehensive framework, potentially requiring less upfront planning but demanding a thorough understanding of the entire investigation process [40]. ISO/IEC 27037 provides a more granular focus on evidence handling, potentially requiring a more meticulous approach to acquisition and preservation but streamlining those specific activities [27].

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3. RESULTS AND DISCUSSION

In order to facilitate a comprehensive understanding, a meticulously crafted and in-depth elaboration of each aspect governed by both standards has been presented in the following highly professional and detailed table. Table 4 is thoughtfully designed to provide a holistic overview of the differences and similarities between NIST SP 800-86 and ISO 27037, enabling practitioners to gain valuable insights into these guidelines and their implications for digital forensic investigations.

Table 4. Software and Supporting Hardware

No	Comparison	NIST SP 800-86	ISO 27037
1	Purpose	Provide a framework for storing and managing digital forensic data	Provide a management framework for protecting digital forensic data
2	Technology	Provides specific recommendations for tools and technologies that can be used to store and manage digital forensic data	Does not make specific recommendations
3	Scope	Specific techniques and procedures for storing and managing digital forensic data	Technical and non-technical aspects of storing and managing digital forensic data
4	Phases	Provides a more detailed step-by-step process for storing and managing digital forensic data	Provides a more general overview of the process
5	Certifiable	Not Available	Yes
6	Audience	Forensic professionals	Information security professionals

Upon thorough examination of the presented table, it becomes unequivocally apparent that both standards exhibit remarkable congruity in the data collection phase, exemplifying their harmonized approach to digital forensic investigations. However, strikingly fundamental differences surface in nearly all other stages. Nevertheless, it is worth emphasizing that both standards unequivocally acknowledge the paramount significance of the collection phase as the very bedrock of any forensic endeavor, underscoring the pivotal role of accurate and dependable digital evidence gathering in both frameworks.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

This table provides a comprehensive exposition of how NIST SP 800-86 and ISO 27037 play pivotal roles in handling digital forensics. The analysis reveals how both standards emphasize the vital importance of meticulous and purposeful handling of digital evidence to ensure the highest integrity of collected data. While they may employ different approaches and emphasize distinct aspects, they converge in addressing the myriad challenges of digital forensics. By harnessing the strengths of both standards, professionals and organizations can holistically confront digital forensic challenges, optimize investigation processes, and attain heightened information security levels in an ever advancing and complex era.

The opinion differs from the explanation on the aspects outlined above, given that the instructions on the treatment of digital evidence under these two standards provide considerably different guidance. This affects the efficiency and anticipated outcomes of the digital evidence investigation process. This in-depth study investigates the effects of NIST SP 800-86 and ISO/IEC 27037 on important phases of digital investigation, focusing on potential discrepancies in efficacy and output from each standard's use. The study's findings will be presented below.

1) Methods and approaches for investigation
   NIST SP 800-86 gives explicit recommendations on structured methodology, including six stages (identification, preservation, collection, inspection, analysis, and reporting). It ensures systematic and repeated investigations, reducing the likelihood of surveillance or error. Furthermore, he urged investigators to meticulously document each stage, fostering transparency and aiding eventual legal action. However, stiff structures may be less adaptable to highly complex or quickly changing conditions.
   ISO/IEC 27037 does not prescribe specific methodologies, promoting a more adaptable approach. However, he emphasized the significance of risk assessment, which can be incorporated in the study. Researchers might optimize their efforts by prioritizing evidence evaluation based on its potential significance (as indicated by risk assessment). This flexibility can be useful in dynamic situations, but it necessitates experienced researchers who can make sound risk-based decisions.
2) Identification process
   To identify potentially relevant digital evidence, NIST SP 800-86 supports active techniques such as keyword search and hashing during the identification stage. Organizations can improve identification procedures by using sensitivity-based data classification (as driven by ISO 27037). However, this technique may overlook buried or encrypted material, necessitating additional investigation.
   Unlike ISO/IEC 27037, this standard emphasizes data classification as a preventive step. Organizations can design a system to prioritize the identification of significant evidence during an inquiry by classifying data

ahead of time. This strategy ensures that investigators start with the most crucial data source and rely on precise pre-incident categorization.

3) Acquisition
   The NIST SP 800-86 standard places a high value on maintaining the nursing chain and carefully documenting evidence to ensure that it has not been misused. It also controls the use of read-only acquisition methods in order to prevent evidence from being changed at random or on purpose. Although these techniques are necessary for regulatory compliance, they can be time-consuming, particularly for large data collections.
   In conjunction with NIST SP 800-86 in terms of meticulous storage chain and documentation, the ISO/IEC 27037 standard investigates specific forensic voice-taking procedures such as bitstream copying to reduce the possibility of manipulating or contaminating evidence. While these strategies improve security, they necessitate specialized training and tools, thereby complicating the acquisition process.
4) Analysis and Reporting
   The NIST SP 800-86 standard recognizes the use of sophisticated forensic tools and techniques for in-depth analysis, allowing investigators to uncover buried information, reconstruct timelines, and identify probable culprits. Furthermore, he recommended investigators to combine data from many sources (network logs, system activity logs, and user activity logs) to form a complete picture of the occurrence. Finally, the standard requires extensive and well-documented reporting that includes techniques, tools used, analysis results, and storage chains. This comprehensive report encourages transparency and communication with the legal team. However, in-depth analysis can use a lot of resources, and complete reporting necessitates large time commitments.
   Although ISO/IEC 27037 does not explicitly address analysis, it does emphasize the significance of detailed documentation throughout the process. This documentation, which includes acquisition records, storage chains, and any observations made throughout the investigation, can be combined with the analysis findings to produce a more comprehensive report.

While both criteria attempt to uncover evidence and promote a successful investigation, their effectiveness varies. NIST SP 800-86 provides a comprehensive framework that may need less planning but necessitates a full understanding of the entire process. In typical cases, this systematic method can lead to faster case settlement. However, rigidity might be detrimental to adaptation in complex investigations. ISO/IEC 27037 provides a more detailed focus on evidence processing, which may necessitate a more specialized approach to collecting and preservation, but simplifies such processes. This emphasis on detail can help to ensure the integrity of evidence, but it can drag down the entire investigation process.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Some of the distinctions mentioned above are rather significant. The exposure provides a more detailed look at the guidelines provided by each standard. NIST SP 800-86 provides broader coverage of the digital investigative lifecycle, from evidence identification to findings reporting. ISO/IEC 27037, on the other hand, focuses its coverage on specific aspects of digital evidence processing and management.

ISO 27037 is intended for a broader audience of information security professionals. These professionals are responsible for ensuring that the organization's information assets are protected from unauthorized access, modification, or destruction.

The comparative analysis reveals significant differences in the adoption and scope of the two standards. NIST SP 800-86's widespread acceptance within the digital forensics' community can be attributed to its comprehensive nature, which encompasses the entire spectrum of forensic activities. This emphasis on a well-structured and thorough process ensures that digital evidence is handled meticulously from the initial stages of identification and collection to the final stages of preservation and analysis. As a result, NIST SP 800-86 provides a robust framework for practitioners and researchers seeking a detailed and methodical approach to digital investigations.

On the other hand, ISO 27037 adopts a more targeted and specialized perspective, placing digital evidence at the forefront of its guidelines. By focusing primarily on the characteristics and uniqueness of electronic evidence, ISO 27037 provides essential recommendations for handling and managing this evidence effectively. This approach caters specifically to professionals in the digital forensics field who need to deal with complex and intricate electronic evidence. Moreover, ISO 27037's inclusive nature allows it to address the needs of various stakeholders beyond the traditional digital forensics community, such as industry professionals and organizational stakeholders involved in managing and responding to digital incidents.

The distinctive features of each standard are reflective of their respective origins and intended purposes. NIST SP 800-86, being a product of the NIST, embodies the rigor and comprehensiveness associated with a government agency's guidelines. On the other hand, ISO 27037, developed under the auspices of the ISO and the IEC, emphasizes international consensus and strives to cater to a global audience with diverse needs and perspectives.

The choice of which standard to adopt depends on the specific requirements and objectives of the digital forensic investigation or incident response. Organizations seeking a more structured and all-encompassing approach may find NIST SP 800-86 preferable, while those primarily concerned with the effective handling of

digital evidence may lean towards ISO 27037. Both standards serve as valuable resources for digital evidence first responders, but their distinct focuses and scopes make them complementary rather than mutually exclusive.

In future works, researchers and practitioners could delve deeper into the strengths and weaknesses of each standard, conducting case studies to evaluate their real-world applicability and effectiveness in various scenarios. Additionally, efforts to bridge the gap between the two standards and explore opportunities for convergence could lead to the development of a more comprehensive and unified framework that leverages the best aspects of both guidelines. This unified approach would cater to the evolving needs of the digital forensics community, academia, industry, and other stakeholders, fostering a more cohesive and efficient ecosystem for digital evidence management and analysis.

4. CONCLUSION

This study has comprehensively compared the NIST SP 800-86 and ISO/IEC 27037 guidelines in digital forensics, revealing their distinct advantages and limitations. ISO/IEC 27037 offers a holistic approach with a continuous improvement philosophy and certification benefits, but it is complex and resource-intensive, focusing more on prevention than incident response. Conversely, NIST SP 800-86 provides specific procedures for digital forensic investigations, making it accessible and practical, but lacks the comprehensive framework of ISO/IEC 27037. The choice between these standards depends on organizational needs, and future research should aim to develop a unified framework that integrates their strengths to enhance digital forensic practices.

REFERENCES

[1] N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," *Journal of Reliable Intelligent Environments*, vol. 7, no. 2. Springer Science and Business Media Deutschland GmbH, pp. 69–84, Jun. 01, 2021. doi: 10.1007/s40860-020-00115-0.

[2] A. Ajijola, P. Zavarsky, and R. Ruhl, *A Review and Comparative Evaluation of Forensics*. 2014.

[3] H. Sama *et al.*, "Studi Komparasi Framework NIST Dan ISO 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka," *Rabit : Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 6, no. 2, pp. 116–121, Jul. 2021, doi: 10.36341/rabit.v6i2.1752.

[4] R. Umar, I. Riadi, and E. Handoyo, "Analisis Tingkat Keamanan Informasi : Studi Komparasi Framework COBIT 5 Subdomain Manage

Security Services (DSS05) dan NIST 800-55," *Jurnal Sistem Komputer*, vol. 1, no. 1, 2020, doi: doi.org/10.37859/coscitech.v1i2.2199.

[5] E. Koza, "Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security Citation: Erfan Koza. 'Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consisten-cies in the Context of Operational and Strategic Information Security,'" 2022.

[6] R. D. Alexander and S. Panguluri, "Cybersecurity Terminology and Frameworks," in *Cyber-Physical Security*, Springer International Publishing, 2017, pp. 19–47. doi: 10.1007/978-3-319-32824-9_2.

[7] A. P. Putra and B. Soewito, "Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector," *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, 2023, [Online]. Available: www.ijacsa.thesai.org

[8] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS."

[9] R. Umar and G. M. Zamroni, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," 2017. [Online]. Available: www.ijacsa.thesai.org

[10] K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," *Comput Secur*, vol. 105, p. 102237, 2021, doi: https://doi.org/10.1016/j.cose.2021.102237.

[11] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *NIST Special Publication 800-86*, 2006.

[12] P. Sundari, "SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)," *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, vol. 12, no. 1, p. 35, 2021.

[13] M. Fitriana, K. Ar, J. M. Marsya, P. T. Informasi, F. Tarbiyah, and D. Keguruan, "Penerapan Metode National Institute Of Standards And Technology (NIST) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Jurnal Pendidikan Teknologi Informasi*, vol. 4, no. 1, pp. 29–39, 2020.

[14] D. S. salsabila, "Analisis Digital Forensics Pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST) SP 800-86," Universitas Muhammadiyah Purwokerto, 2024.

[15] A. Yuda Prasetya, D. Al Dzaky Bewasana, F. Keamanan Siber, P. Studi Rekayasa Keamanan Siber, and P. Siber dan Sandi Negara, "Analisis Scalpel sebagai File Carving Tools untuk Forensik Docker Linux

Berdasarkan NIST SP 800-86," *Jurnal Riset Informatika dan Inovasi*, vol. 1, no. 7, pp. 784–789, Feb. 2024.

[16] I. Irwansyah and H. Yudiastuti, "Analisis Digital Forensik Rekayasa Image Menggunakan JPEGSnoop dan Forensically Beta," *Jurnal Ilmiah Matrik*, vol. 21, no. 1, 2019.

[17] M. Rifqi, S. J. I. Ismail, and M. F. Rizal, "Analisis Forensik Untuk Penanganan Cyber Crime Pada Aplikasi Whatsapp Menggunakan Metode National Institute Of Standard And Technology (Nist Sp 800-86)," *e-Proceeding of Applied Science*, vol. 9, no. 6, pp. 3017–3022, 2023.

[18] D. Hariyadi, M. Kusuma, and A. Sholeh, "Digital Forensics Investigation on Xiaomi Smart Router Using SNI ISO/IEC 27037:2014 and NIST SP 800-86 Framework," 2021.

[19] 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)*, 2020, pp. 1–3. doi: 10.1109/NCETSTEA48365.2020.9119914.

[20] S. Almuhammadi and M. Alsaleh, "Information Security Maturity Model for Nist Cyber Security Framework," Academy and Industry Research Collaboration Center (AIRCC), Feb. 2017, pp. 51–62. doi: 10.5121/csit.2017.70305.

[21] A. Yeboah-Ofori, E. Yeboah-Boateng, and H. Gustav Yankson, "Relativism digital forensics investigations model: A case for the emerging economies," in *Proceedings - 2019 International Conference on Cyber Security and Internet of Things, ICSIoT 2019*, Institute of Electrical and Electronics Engineers Inc., May 2019, pp. 93–100. doi: 10.1109/ICSIoT47925.2019.00023.

[22] R. A. Ramadhan, P. Rachmat Setiawan, and D. Hariyadi, "Digital Forensic Investigation for Non-Volatile Memory Architecture by Hybrid Evaluation Based on ISO/IEC 27037:2012 and NIST SP800-86 Framework," *IT Journal Research and Development*, pp. 162–168, Feb. 2022, doi: 10.25299/itjrd.2022.8968.

[23] A. Calder and S. G. Watkins, "The ISO 27001 Risk Assessment," in *Information Security Risk Management for ISO 27001/ISO 27002,* 3rd edition., IT Governance Publishing, 2019, pp. 87–93. [Online]. Available: https://doi.org/10.2307/j.ctvndv9kx

[24] D. Nikitin, "Achieving Privacy And ISO 27001 Standard," Southern-Eastern Finland University, 2023.

[25] R. Umar, I. Riadi, and E. Handoyo, "Manage Security Services (DSS05) Dan NIST SP 800-55," 2020.

[26] B. Esanu, "An Assessment of, and Improvements to, the Digital Forensics Acquisition Process of a Law Enforcement Agency."

[27] "SNI ISO/IEC 27037:2014." Badan Standarisasi Nasional, 2014.

[28] D. D. Prasetyowati, I. Gamayanto, S. Wibowo, and S. Suharnawi, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang," *Journal of Information System*, vol. 4, no. 1, pp. 65–75, May 2019.

[29] M. W. Indriyanto, D. Hariyadi, M. Habibi, U. J. Achmad, and Y. Yogyakarta, "Investigasi Dan Analisis Forensik Digital Pada Percakapan Grup Whatsapp Menggunakan NIST SP 800-86 dan Support Vector Machine," *CyberSecurity dan Forensik Digital*, vol. 3, no. 2, pp. 34–38, Nov. 2020.

[30] R. Fúska, "Implementation of ISO27001 Standard in Startups," 2022.

[31] P. Kanantyo, F. S. Papilaya, K. S. Wacana, J. Blotongan, K. Salatiga, and J. Tengah, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)," *Jurnal Teknik Informatika dan Sistem Informasi* , vol. 8, no. 4, pp. 1896–1908, 2021, [Online]. Available: http://jurnal.mdp.ac.id

[32] A. Mariza, L. Abdurahman, and I. Santosa, "Analisis Risiko Dan Kontrol Pada SIMRS Gudang Obat Berdasarkan ISO 31000 (Studi Kasus: Rumah Sakit Khusus Ibu Dan Anak Kota Bandung)," *e-Proceeding of Engineering*, vol. 7, no. 2, pp. 6984–6992, Aug. 2020.

[33] A. Efe, "A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT," *Journal of Auditing and Assurance Services*, vol. 3, no. 2, 2023, [Online]. Available: http://orcid.org/0000-

[34] M. Yan Fikri Hendrawan and A. Hadinegoro, "Analisis Bukti Digital Pada Discord Browser Menggunakan Teknik Live Forensic Dengan Metode NIST SP 800-86," *Jurnal Infomedia:*, vol. 8, no. 2, 2023.

[35] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," *Sustainability (Switzerland)*, vol. 15, no. 7, Apr. 2023, doi: 10.3390/su15075828.

[36] D. Julian and T. Sutabri, "Analisa Kinerja Aplikasi Digital Forensik Autopsy Untuk Pengembalian Data Menggunakan Metode NIST SP 800-86," *Jurnal Informatika Terpadu*, vol. 9, no. 2, pp. 136–142, 2023, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[37] R. N. Dasmen, M. Reihan Pratama, H. Yasir, and A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86," *Jurnal Ilmiah Informatika*, Mar. 2024.

[38] K. U. maheswari and G. Shobana, "The State of the art tools and techniques for remote digital forensic investigations," 2021, pp. 464–468. doi: 10.1109/ICSPC51351.2021.9451718.

[39] Y. Kurii and I. Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013," in *Cybersecurity Providing in Information and Telecommunication System*, 2022.

[40] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response Recommendations of the National Institute of Standards and Technology."