Development of a Self Assessment Application to Measure Digital Forensics Readiness in Higher Education Institutions

Tri Rochmadi[ab1], Abdul Fadlil[c2], Imam Riadi[d3], Angga Dwi Wahyudi[e4], Joko Handoyo[f5], Aris Rakhmadi[g6]

[a]Department of Informatics, Universitas Ahmad Dahlan, Indonesia
[b,e]Department of Information System, Universitas Alma Ata, Indonesia
[c]Department of Electrical Engineering, Universitas Ahmad Dahlan, Indonesia
[d]Department of Information System, Universitas Ahmad Dahlan, Indonesia
[f]Department of Informatics, Sekolah Tinggi Teknologi Ronggolawe, Indonesia
[g]Department of Informatics Engineering, Universitas Muhammadiyah Surakarta, Indonesia

e-mail: [1]trirochmadi@almaata.ac.id, [2]fadlil@mti.uad.ac.id, [3]imam.riadi@is.uad.ac.id, [4]223100317@almaata.ac.id, [5]jokohandoyo2013@gmail.com, [6]aris.rakhmadi@ums.ac.id

Abstrak

Perkembangan transformasi digital di perguruan tinggi meningkatkan kebutuhan terhadap kesiapan digital forensik yang terukur, terutama dalam menghadapi risiko kebocoran data, penyalahgunaan akun, serangan siber, dan kebutuhan preservasi bukti digital. Penelitian ini bertujuan mengembangkan aplikasi self assessment untuk mengukur kesiapan digital forensik di perguruan tinggi secara mandiri, terstruktur, dan berbasis indikator. Metode pengembangan menggunakan System Development Life Cycle yang terdiri atas enam tahap, yaitu requirement analysis, design, development, testing, deployment, dan maintenance. Aplikasi yang dikembangkan memiliki tujuh kebutuhan fungsional utama, yaitu login pengguna, pengelolaan indikator, pengisian instrumen, perhitungan skor, klasifikasi tingkat kesiapan, rekomendasi perbaikan, dan laporan hasil. Selain itu, aplikasi juga memenuhi lima kebutuhan nonfungsional, yaitu usability, reliability, security, maintainability, dan portability. Hasil pengujian menggunakan black-box testing terhadap tujuh skenario pengujian menunjukkan bahwa seluruh fitur utama memperoleh status valid. Pada tahap deployment, aplikasi berhasil menghasilkan nilai kesiapan digital forensik pada institusi uji HE1 sebesar 3,2. Hasil ini menunjukkan bahwa aplikasi mampu melakukan proses penilaian secara otomatis, mulai dari input instrumen, perhitungan skor, penentuan maturity level, hingga penyajian rekomendasi perbaikan. Dengan demikian, aplikasi self assessment ini dapat digunakan sebagai instrumen evaluasi mandiri untuk membantu perguruan tinggi memetakan tingkat kesiapan digital forensik, mengidentifikasi kesenjangan implementasi, dan menyusun prioritas peningkatan tata kelola keamanan informasi.

Kata kunci: *Digital Forensic Readiness, Self Assessment, COBIT 2019, SDLC, Black-Box Testing*

Abstract

The advancement of digital transformation in higher education institutions has increased the need for measurable digital forensics readiness, particularly in addressing the risks of data breaches, account misuse, cyberattacks, and the need for digital evidence preservation. This research aims to develop a self assessment application to measure digital forensics readiness in higher education institutions in a self-directed, structured, and indicator-based manner. The development method employs the System Development Life Cycle, which consists of six stages: requirement analysis, design, development, testing, deployment, and maintenance. The developed application features seven primary functional requirements: user login, indicator management, instrument completion, score calculation, readiness level classification,

improvement recommendations, and results reporting. Additionally, the application meets five non-functional requirements: usability, reliability, security, maintainability, and portability. Testing results using black-box testing across seven test scenarios showed that all major features achieved a valid status. During the deployment phase, the application successfully generated a digital forensics readiness score of 3.2031 for the test institution HE1. These results demonstrate that the application is capable of performing the assessment process automatically, from instrument input, score calculation, maturity level determination, to the presentation of improvement recommendations. Thus, this self assessment application can be used as a self-evaluation tool to help universities map their digital forensic readiness levels, identify implementation gaps, and prioritize improvements in information security governance.

Keywords : *Digital Forensic Readiness, Self Assessment, COBIT 2019, SDLC, Black-Box Testing*

1. Introduction

Advances in information technology within the higher education sector have driven digital transformation across various aspects of higher education administration [1], [2], [3]. Academic activities, research, community service, financial administration, student services, human resource management, and even the management of institutional documents are now increasingly reliant on information systems and digital infrastructure [4]. Higher education institutions no longer serve merely as educational institutions but also as data-driven organizations managing various critical information assets, such as student data, faculty data, research data, financial data, academic data, and other institutional documents. This situation positions information technology as a strategic component in supporting service effectiveness, business process efficiency, and institutional decision-making [5], [6].

However, the increased use of information technology also brings consequences in the form of heightened cybersecurity risks [7]. Higher education institutions have become one of the environments most vulnerable to various forms of digital threats, such as data breaches, identity theft, malware attacks, phishing, account misuse, unauthorized access, manipulation of academic data, and disruptions to campus digital services [8]. These risks are further complicated by the fact that the higher education environment typically features open systems, a large number of users, diverse organizational units, and uneven levels of information security literacy. If security incidents are not properly addressed, the consequences extend beyond technical disruptions to include damage to the institution's reputation, eroded trust among the academic community, non-compliance with regulations, and disruption to academic services [9].

In this context, Digital Forensic Readiness (DFR) is a critical capability that higher education institutions must possess. DFR can be understood as an organization's ability to establish policies, procedures, human resources, infrastructure, technology, and governance mechanisms to ensure that the processes of identifying, collecting, acquiring, preserving, analyzing, and presenting digital evidence can be carried out effectively when a security incident occurs [10]. With DFR, higher education institutions are not only able to respond to incidents reactively but can also establish preventive and systematic mechanisms to ensure that the digital evidence required for investigations can be obtained lawfully, intact, and in a manner that can be accounted for.

The management of digital evidence requires a standardized approach because digital evidence is volatile, fragile, and susceptible to manipulation. ISO/IEC 27037 provides guidelines on the identification, collection, acquisition, and preservation of digital evidence that may have evidentiary value [11]. Additionally, NIST, through its computer security incident response guidelines, emphasizes the importance of the processes of preparation, detection, analysis, response, recovery, and post-incident learning in building an organization's capability to handle security incidents [12], [13]. Both references indicate that digital forensics readiness is not limited to technical aspects but also encompasses governance, operational procedures, personnel competencies, risk management, and adequate documentation.

Nevertheless, the implementation of digital forensics readiness in higher education institutions still faces various challenges. Many institutions already have information systems, security devices, or incident handling procedures, but they do not necessarily have measurable

mechanisms to assess the extent to which digital forensics readiness has been implemented. Readiness assessments are often still partial, not standardized, not supported by comprehensive indicators, and unable to provide an objective picture of the level of maturity. As a result, universities face difficulties in identifying readiness gaps, determining improvement priorities, and formulating strategies for continuous strengthening of digital security and forensics.

To address this need, a self assessment-based tool is required that can be used independently by higher education institutions. The self assessment application enables institutions to conduct an initial evaluation of their digital forensics readiness based on specific indicators, so that the assessment results can be used as a basis for decision-making. Through this application, institutions can determine their current readiness status, identify areas of weakness, assess the maturity level of each domain, and receive recommendations for necessary improvements. Thus, the self assessment application serves not only as an evaluation tool but also as an instrument supporting information security governance and strategic planning for enhancing digital forensics readiness.

In this research, COBIT 2019 was used as a key foundation for developing indicators and the assessment framework [10]. COBIT 2019 is an information technology governance and management framework developed by ISACA to help organizations align information technology with organizational objectives, manage risks, optimize resources, and ensure the achievement of value from the use of information and technology [14]. COBIT 2019 features a core model comprising 40 governance and management objectives that can be used to guide, measure, and evaluate information technology management practices. COBIT 2019 also emphasizes that the governance and management of information and technology must be built through various components [15], such as processes, organizational structure, information, culture and behavior, policies and procedures, services/infrastructure/applications, as well as competencies and skills.

The relevance of COBIT 2019 to digital forensics readiness lies in its ability to provide a comprehensive governance perspective. Digital forensics should not be viewed merely as a technical activity following an incident but must be embedded within a governance framework that encompasses planning, control, risk management, information security, compliance, and continuous improvement [16], [17]. Some COBIT 2019 domains relevant to digital forensics readiness include EDM to ensure governance direction and oversight, APO for strategic planning, risk management, and security, BAI for change management and technology solutions, DSS for service management, operations, security, and incident management, and MEA for monitoring, evaluation, and compliance [4]. By using COBIT 2019, digital forensics readiness indicators can be developed more systematically as they cover strategic, managerial, operational, and control aspects.

The main issues in this research are how to objectively measure the level of digital forensics readiness at universities, how to design a self assessment application that institutions can use independently, and how to ensure that the developed application is valid, practical, and aligned with user needs. These issues highlight the need for an approach that not only produces a conceptual model but also generates an application that can be directly used to support the digital forensics readiness evaluation process. Based on these issues, the objective of this research is to develop a digital-based self assessment application to comprehensively measure digital forensics readiness at universities. The developed application is expected to present assessment results in the form of readiness levels, index scores, maturity categories, and recommendations for improvement.

The urgency of this research lies in the need for higher education institutions to have a standardized, user-friendly evaluation tool capable of supporting strategic decision-making in strengthening information security. With the self assessment application, higher education institutions can map DFR more effectively, identify implementation gaps, and prioritize improvements based on assessment results. This research is expected to provide practical contributions in the form of a digital forensics readiness evaluation application, as well as academic contributions in the form of the development of an assessment model that integrates the concept of DFR and information technology governance based on COBIT 2019.

2. Research Method

The development of the digital forensics readiness self assessment application in this research utilized the System Development Life Cycle (SDLC) approach [18]. The SDLC was chosen because it is suitable for developing information systems that require systematic stages, ranging from requirements analysis, design, development, testing, implementation, to evaluation [19]. Through this approach, the developed application is not only oriented toward fulfilling technical functions but also toward aligning with user needs and the objectives of measuring digital forensics readiness in higher education institutions, as shown in Figure 1.

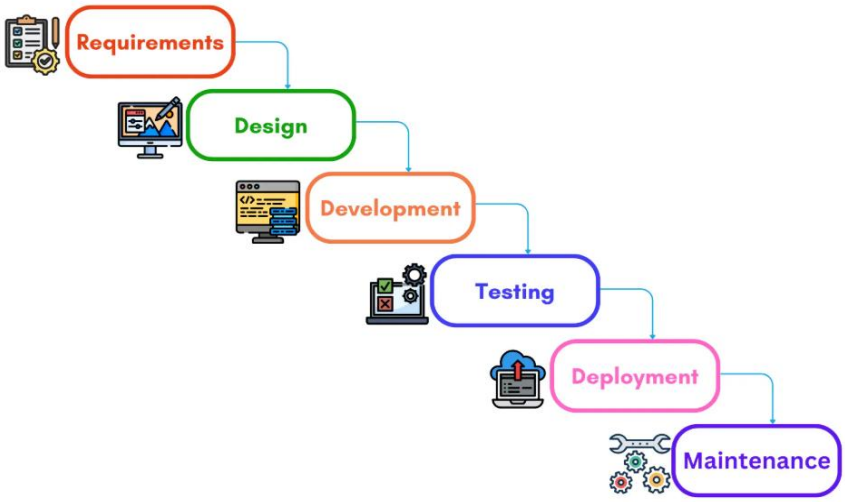


Figure 1. SDLC-based application development workflow

Table 1 shows that the SDLC approach provides a systematic development workflow for building a digital forensics readiness self assessment application. The requirements analysis phase serves as the foundation for determining system indicators and functions, while the design phase translates these requirements into an application design. The implementation phase produces a system prototype, which is then tested to ensure the correctness of its functions and outputs. After the application is deployed to users, evaluation and maintenance are conducted to address shortcomings and enhance the application's suitability [20] as a self assessment tool in higher education institutions.

Table 1. Stages of self assessment application development using the SDLC

SDLC stage	Main Activities	Output Generated
Requirement	Identify user needs, system requirements, Digital Forensic Readiness indicators, and their relationship to COBIT 2019.	System requirements document and initial assessment indicators.
Design	Design application architecture, assessment instruments, measurement scales, process flows, databases, and user interfaces.	System design, database design, and application interface design.
Development	Develop a self assessment application based on the established design.	Application prototype with key self assessment features.
Testing	Test system functionality, input-output validity, scoring process, and assessment result accuracy.	System testing results and a list of improvements.
Deployment	Deploy the application to users or test institutions for use in the digital forensic readiness assessment process.	Application usage data and user feedback.
Maintenance	Evaluate application feasibility, correct errors, and enhance features based on test results and feedback.	A final application that is more valid, practical, and usable.

3. Result and Discussion

In general, the application development results indicate that the system is capable of performing its main functions, namely managing assessment indicators, facilitating the completion of self assessment instruments, calculating readiness scores, displaying readiness level categories, and providing recommendations for improvement. These results demonstrate that the SDLC approach can be used systematically in the development of digital forensics readiness evaluation applications.

3.1. Requirement Results

The requirements analysis phase identified system requirements that served as the basis for application development. These requirements were derived from an analysis of the Digital Forensic Readiness concept, digital evidence management standards, information technology governance, and the needs of higher education institutions for conducting self assessments. Based on the initial analysis, the application needed to be able to manage user data, manage assessment indicators, input answers, calculate readiness scores, display assessment results, and provide recommendations for improvement. The system requirements in this research were divided into functional and non-functional requirements.

Functional requirements directly relate to the features that must be available in the application. Non-functional requirements, on the other hand, relate to system quality, such as ease of use, access security, processing speed, and display clarity, as shown in Table 2.

Table 2. Self assessment application needs

No	Functional Requirements	Description
1	User login	The system provides authentication for institutional administrators and users.
2	Indicator management	Admins can add, edit, and delete assessment indicators.
3	Instrument completion	Users can complete the digital forensics readiness instrument.
4	Score calculation	The system calculates a readiness score based on user responses.
5	Readiness level classification	The system displays a readiness category based on the final score.
6	Improvement recommendations	The system provides recommendations based on the scores for each domain.
7	Results report	The system provides a summary of the assessment results in tabular or graphical form.
No	Non-Functional Requirements	Description
1	Usability	The application is easy to use for college users.
2	Reliability	The system is capable of calculating scores consistently.
3	Security	User access is restricted through a login mechanism.
4	Maintainability	Assessment indicators and categories can be updated by the administrator.
5	Portability	The application can be accessed through any device that supports a web browser.

Based on Table 2, the developed application emphasizes not only measurement functionality but also ease of use and flexibility in indicator management. This is important because digital forensic readiness instruments have the potential to change according to evolving institutional needs, regulations, and information technology governance practices.

3.2. Design Results

The system design phase produces an application design consisting of actor design, process flow, data structure, interface design, and assessment mechanisms. Generally, there are two main actors in the application: the administrator and the institutional user. The administrator is responsible for managing indicators, assessment domains, readiness categories, and user data. Meanwhile, the institutional user completes the self assessment instrument and views the assessment results, as shown in Table 3.

Table 3. Actors and system access rights

Actors	Access
Administrator	Manage domains, indicators, rating scales, users, and assessment reports.
User	Complete self assessment instruments, view scores, view readiness categories, and read recommendations.

The application workflow begins with the login process, confirmation of readiness, instrument completion, receipt of results, including determination of readiness category, and presentation of recommendations. A schematic of this process flow can be seen in Figure 2.

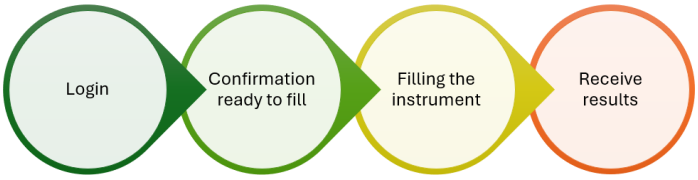
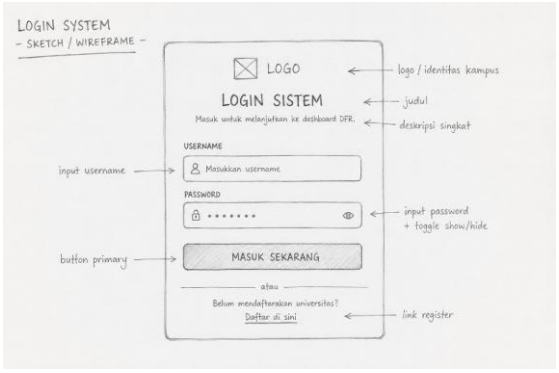
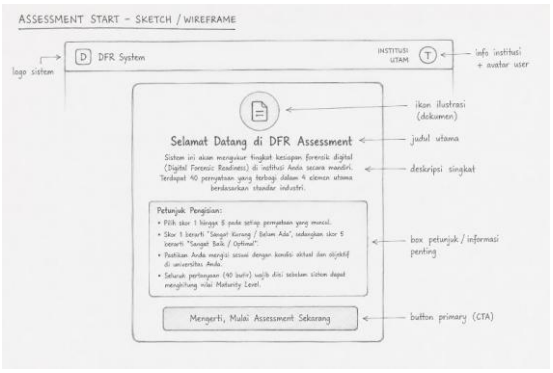


Figure 2. Application business process flow

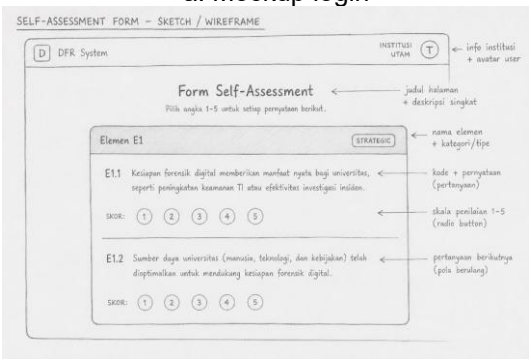
The mockup design of each flow can be seen in Figure 3. Explanation of the mockup in Figure 3 as follows (a) to begin the process, users must first access their personal account, (b) users are required to review the provided information and instructions, (c) users must carefully navigate through the instrument, providing accurate responses to each item, (d) immediately following submission, users can view their comprehensive results.



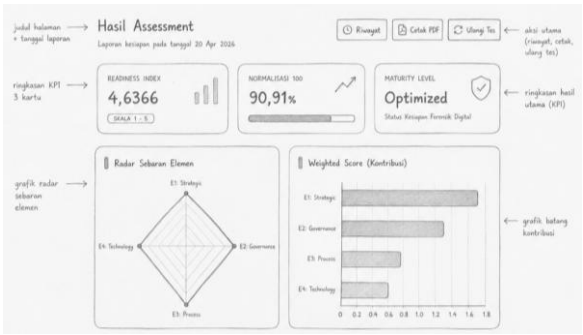
a. Mockup login



b. Mockup confirmation ready to fill



c. Mockup filling the instrument



d. Mockup receive result

Figure 3. Application mockup

3.3. Development Results

The development phase resulted in a self assessment application prototype developed based on the system design. Key features developed include user login, dashboard, weight management, indicator management, instrument completion, score calculation, results visualization, and improvement recommendations. The application was designed as a web-based application for easy access by institutional users via a browser, as seen in Figure 4.

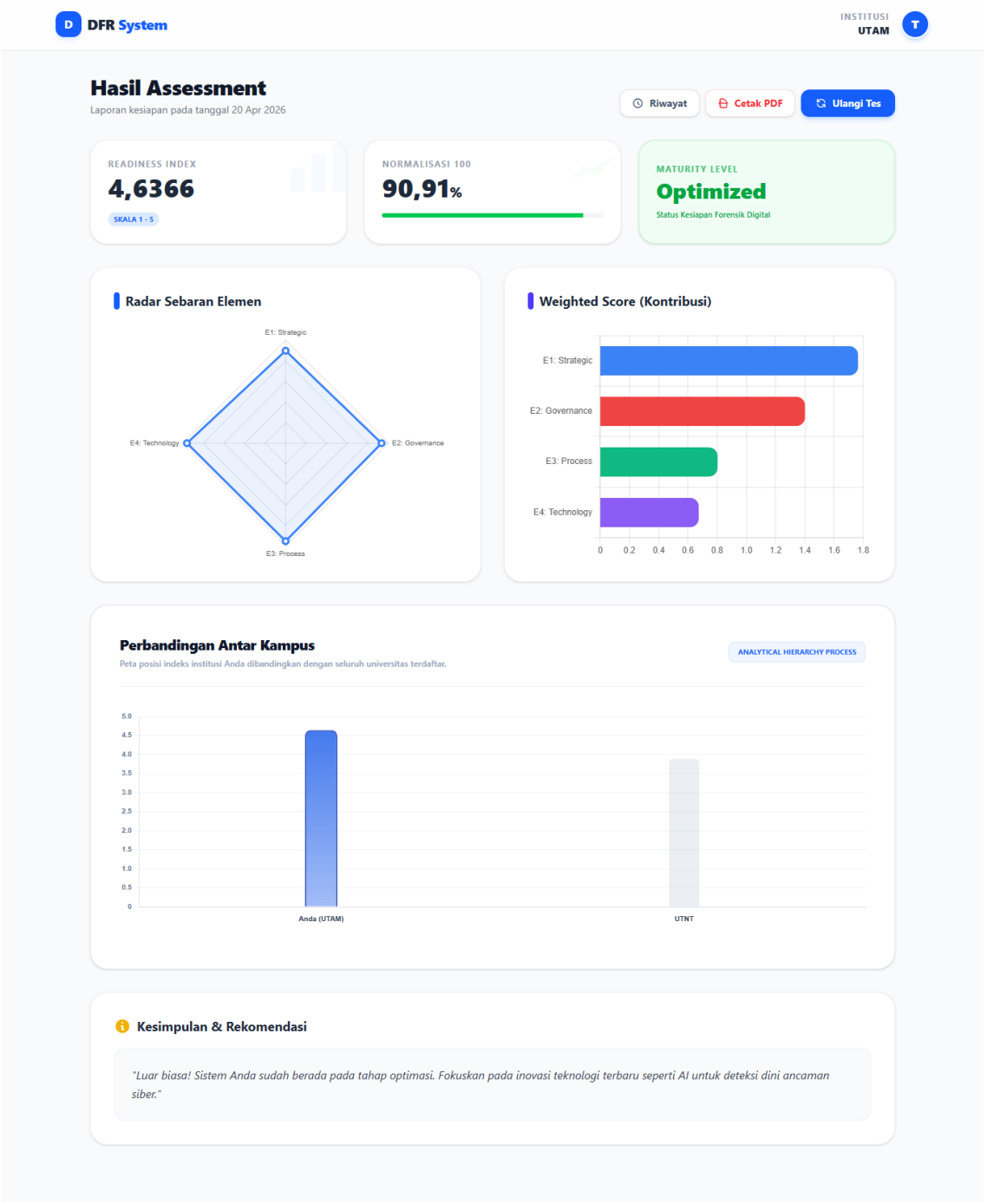


Figure 4. Example application display

The development results show that the application is capable of integrating the assessment process from input to output. The feature automates the score calculation process, reducing the potential for manual calculation errors. Furthermore, presenting the results in a domain summary format helps users identify areas for improvement.

3.4. Testing Results

The testing phase is conducted to ensure that each application feature operates according to predetermined requirements. Testing is conducted using black-box testing scenarios, which focus on system input and output without examining the program code structure. This testing aims to ensure that the application's main functions function correctly.

Table 4. Application black-box testing results

Features Tested	Test Scenarios	Expected Results
Login	The user enters a valid username and password.	The system provides authentication for institutional administrators and users.
Login	The user enters an incorrect password.	Admins can add, edit, and delete assessment indicators.
Instrument	The user completes all the indicators.	Users can complete the digital forensics readiness instrument.
Score	The system calculates the score based on the answers.	The system calculates a readiness score based on user responses.
Readiness	The final score is converted to the maturity level.	The system displays a readiness category based on the final score.
Recommendations	The user receives the results.	The system provides recommendations based on the scores for each domain.
Report	The user opens the results page.	The system provides a summary of the assessment results in tabular or graphical form.

Based on the test results in Table 4, all main features are declared valid because they produce output according to the designed scenario.

3.5. Deployment Results

The deployment phase involves deploying the application to test users or institutions. At this stage, users complete a self assessment instrument based on the institution's actual conditions. The system then calculates a score for each domain and displays a digital forensics readiness category.

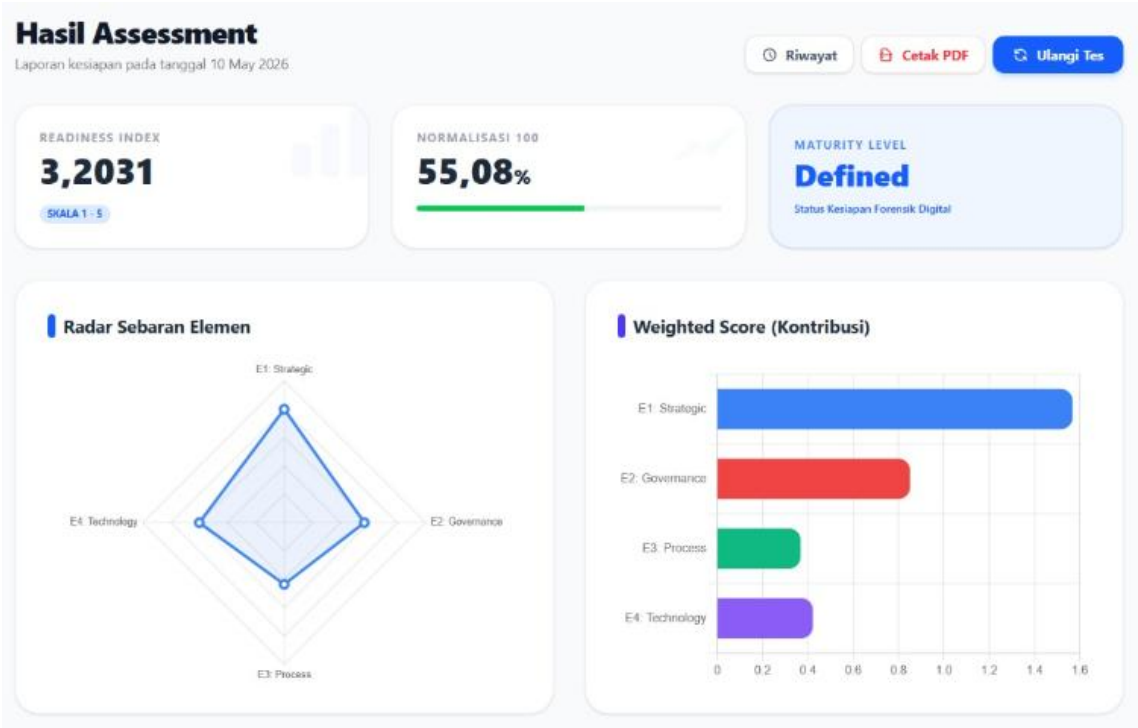


Figure 5. Digital forensic readiness score at HE1 institution

Based on the data in Figure 5, the digital forensic readiness score is 3.2031. This result indicates that the application is capable of assessing HE1's digital forensic readiness level based on input provided by the IT governance officer at HE1.

3.6. Maintenance

The maintenance phase is carried out to assess the application's suitability after testing and user deployment. The evaluation is conducted by reviewing test results, user feedback, and the suitability of the system's output to the research objectives. Based on the evaluation results, the application is deemed capable of supporting the digital forensics readiness self assessment process because it provides a structured assessment mechanism, easy-to-understand scoring results, and domain-based improvement recommendations.

Table 5. User feedback and action plan

User Feedback	Follow-up
Recommendations need to be more specific.	Adding an AI feature or special recommendation formula based on input rather than level category.
The input process needs to be simplified.	Adding a progress bar and temporary storage feature.

The evaluation results in Table 5 indicate that improvements to the application are needed, particularly in terms of progress and outcomes. By making these improvements, the application is expected to provide greater benefits to universities in understanding their digital forensics readiness and developing targeted improvement measures.

3.7. Discussion

The application development results demonstrate that the SDLC approach provides a systematic workflow for developing a digital forensics readiness self assessment application. The requirements analysis phase helps researchers identify system needs and assessment indicators, while the system design phase translates these needs into an application design. The development phase produces a system prototype that can be used for measurement, while the testing phase ensures that key features function as intended. Furthermore, deployment and evaluation provide an overview of the application's usability and any necessary improvements.

The developed self assessment application plays a crucial role as a self-evaluation tool for higher education institutions. Through this application, institutions can determine their digital forensics readiness status based on specific domains. The assessment results not only display a final score but also demonstrate the achievements of each domain. This allows institutions to identify areas of strength and areas requiring improvement. For example, if the technology and infrastructure domain scores low, the institution can prioritize the procurement of forensic tools, improving the logging system, strengthening backups, and developing digital evidence acquisition procedures.

Furthermore, the results of the domain-based assessment can assist higher education institutions in developing strategies to improve digital forensics readiness. Digital forensic readiness is not only supported by technological devices; it also requires policies, procedures, human resource competency, incident management, and continuous evaluation. Therefore, this application is expected to be a supporting instrument for information security governance in higher education. From a system perspective, the developed application provides efficiency in the assessment process because users do not need to perform manual calculations. The system automatically processes user answers, calculates scores, determines readiness categories, and generates recommendations. This can reduce calculation errors and expedite the evaluation process. Furthermore, the reporting feature can help institutions document assessment results as a basis for developing improvement plans.

Overall, the development results indicate that the digital forensic readiness self assessment application is worthy of development as a self assessment instrument. However, because the data used in this example is still dummy, actual research requires further testing using real respondents, expert validation, and more comprehensive system testing. This will ensure the final application has a stronger level of validity, practicality, and usefulness.

Based on Table 6, each SDLC stage contributes to the success of application development. The analysis and design stages ensure the application meets measurement requirements, while the development and testing stages ensure the system functions as intended. The deployment and evaluation stages provide the basis for assessing application usability and determining further improvements.

Table 6. Development based on SDLC

SDLC stage	Main Activities	Output Generated
Requirement	System requirements and DFR indicators were successfully identified.	The system has a clear baseline of needs.
Design	Instruments, system flows, scoring, and interfaces were successfully designed.	Application development is more focused.
Development	An application prototype was successfully developed.	The system can be used for self assessment.
Testing	Key features were implemented according to the test scenario.	The application meets basic functional requirements.
Deployment	The application can be used to generate readiness scores.	Institutions can determine their DFR readiness status.
Maintenance	Feedback was obtained for application improvements.	The system can be improved in terms of usability and recommendations.

5. Conclusion

This research successfully developed a self assessment application to measure digital forensic readiness in higher education institutions using the SDLC approach. The development results showed that the application has seven main functional features and five non-functional aspects that support the self-evaluation process. System testing was conducted through black-box testing on seven scenarios, including valid logins, invalid logins, instrument completion, score calculation, readiness category classification, improvement recommendations, and results reporting. All scenarios achieved a valid status, resulting in a 100% test success rate. These findings indicate that the application met basic functional requirements and was able to carry out the assessment process as designed.

During the deployment phase, the application was successfully used to measure the digital forensic readiness of HE1 institutions, with a score of 3.2031. This score demonstrates the system's ability to automatically calculate readiness scores and present assessment results in an easy-to-understand format. The application also reduced the potential for manual calculation errors because the assessment process, maturity level classification, and recommendations were computerized. Practically, this application can help higher education institutions determine their digital forensic readiness status, identify areas that need improvement, and develop data-driven improvement strategies.

References

[1] D. Ardiansyah, “Transformasi Digital Perguruan Tinggi Menggunakan Prinsip Smart Education,” *Fahma : Jurnal Informatika Komputer, Bisnis dan Manajemen*, vol. 20, no. 1, Jan. 2022, doi: https://doi.org/10.61805/fahma.v20i1.43.

[2] T. Rochmadi, A. Fadlil, and I. Riadi, “Tinjauan Pustaka Sistematis: Tantangan dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital,” *CyberSecurity dan Forensik Digital*, vol. 7, no. 2, pp. 81–89, Dec. 2024, doi: 10.14421/csecurity.2024.7.2.4861.

[3] T. Rochmadi, V. P. Widartha, T. A. Sarmento, A. A. Harahap, and I. Ajis, “Forensic Investigation of SEO Manipulation in Moodle LMS: Uncovering Illegal Content in Educational Platforms,” *Indonesian Journal of Information Systems*, vol. 8, no. 1, pp. 1–9, Aug. 2025, doi: 10.24002/ijis.v8i1.12222.

[4] T. Rochmadi, A. Fadli, I. Riadi, K. Nisa Panilestari, and Y. Wicaksono, “Analisis Teknologi dan Prosedural dalam Penanganan Insiden untuk Mendukung Forensik Digital,” *Jurnal Mahasiswa Teknik Informatika*, vol. 10, no. 2, Apr. 2026, doi: https://doi.org/10.36040/jati.v10i2.17792.

[5] R. A. K. Putera and R. S. Laxsniky, “Peran Sistem Informasi Manajemen Pendidikan dalam Mendukung Pengambilan Keputusan Strategis untuk Peningkatan Kinerja Lembaga,” *Pendas : Jurnal Ilmiah Pendidikan Dasar*, vol. 10, no. 4, pp. 2477–2143, Dec. 2025, doi: https://doi.org/10.23969/jp.v10i4.36493.

[6] B. Suhartono *et al.*, *Manajemen Data Dan Analisis Sistem# 1*, 1st ed. Bekasi: Hadla Media Informasi, 2025.

[7] T. Rochmadi *et al.*, “Pengukuran Kesadaran Keamanan Informasi UMKM terhadap Phising pada Aplikasi Whatsapp,” *Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi*, vol. 11, no. 3, pp. 184–190, Dec. 2025, doi: https://doi.org/10.34010/jtk3ti.v11i3.18935.

[8] M. Febrian Aska, D. pratama Putta, and C. Julyana Magdalena Sinambela, “Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital,” *Journal of Information and Information Security (JIFORTY)*, vol. 5, no. 2, pp. 187–200, Jan. 2025, doi: https://doi.org/10.31599/fzg80847.

[9] A. Erikha and Z. A. Hoesein, “Strategi Pencegahan Kebocoran Data Pribadi melalui Peran Kominfo dan Gerakan Siberkreasi dalam Edukasi Digital,” *Jurnal Retentum*, vol. 7, no. 1, p. 1, Nov. 2025, doi: http://dx.doi.org/10.46930/retentum.v7i1.5272.

[10] T. Rochmadi, A. Fadlil, and I. Riadi, “Developing a Delphi Validated Instrument for Assessing Digital Forensics Readiness Based on COBIT 2019,” *International Journal of Advances in Data and Information Systems*, vol. 6, no. 3, pp. 749–762, Dec. 2025, doi: 10.59395/ijadis.v6i3.1453.

[11] I. Riadi *et al.*, *Analisis Forensik Digital # 1*, 1st ed. Bekasi: Hadla Media Informasi, 2026.

[12] I. Ainur Rafiq, I. Riadi, and Herman, “Perbandingan Forensic Tools pada Instagram Menggunakan Metode NIST,” *Jurnal Informatika Sunan Kalijaga*, vol. 7, no. 2, pp. 134–142, May 2022, doi: https://doi.org/10.14421/jiska.2022.7.2.134-142.

[13] I. Riadi, T. Ruslan, and Sunardi, “Analisis Forensik Digital pada Whatsapp dan Facebook Menggunakan Metode NIST,” *Jurnal Fasilkom*, vol. 13, Aug. 2023, doi: doi.org/10.37859/jf.v13i02.5540.

[14] ISACA, *COBIT 2019 Framework : Introduction and Methodology*. Schaumburg: ISACA, 2019.

[15] H. M. Melaku, “A dynamic and adaptive cybersecurity governance framework,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 3, pp. 327–350, 2023.

[16] M. Kudonu, N. Singh, A. Gosney, and P. B. Hari, “The Role of AI Governance in Digital Forensics: A Framework for Ethical and Reliable Investigations,” in *2025 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 2025, pp. 615–620. doi: 10.1109/ICCIKE67021.2025.11318205.

[17] A. Pooe, “Enhancing Forensic Readiness Through an Integrated Approach to Fraud Risk Management Throughout the Digital Transformation Lifecycle,” in *Information and Cyber Security*, M. and E. J. and B. R. and L. M. and M. U. Venter Hein and Eloff, Ed., Cham: Springer Nature Switzerland, 2026, pp. 124–133.

[18] K. S. C. Risna, I. N. Piarsa, and AA. Kt. A. C. Wiranatha, “Design of IoT-Based Smart Charging Power Supply for Pratima Security,” *JITTER - Jurnal Ilmiah Teknologi dan Komputer*, vol. 6, no. 3, Dec. 2025.

[19] Angelina, C. Yandhika, C. L. Hartanto, M. Graciela, and A. Farisi, “Sebuah Tinjauan Literatur Sistematis Tentang Metode Pengembangan Perangkat Lunak Sistem Informasi Berbasis Web,” *Jurnal Teknologi Sistem Informasi*, vol. 5, no. 1, pp. 181–192, Apr. 2024, doi: https://doi.org/10.35957/jtsi.v5i1.6619.

[20] E. Triandini, S. Jayanatha, A. Indrawan, G. W. Putra, and B. Iswara, “Metode Systematic Literature Review untuk Identifikasi Platform dan Metode Pengembangan Sistem Informasi di Indonesia,” *Indonesian Journal of Information Systems (IJIS*, vol. 1, no. 2, Feb. 2019, doi: https://doi.org/10.24002/ijis.v1i2.1916.