Jurnal Sistem Informasi Bisnis 04(2024)
Copyright ©2024, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/60720

Strategic Evaluation of Whistleblower Software Security in Government: ISO/IEC 25010 and AHP Method

Winny Purbaratri*, Irwan Sembiring, Adi Setiawan, Iwan Setyawan

Universitas Kristen Satya Wacana

Received: December 16th, 2023; Accepted: August 8th, 2024
DOI: 10.21456/vol14iss4pp321-328

Abstract

To assess the effectiveness of software security measures in government whistleblower systems, we will utilize the ISO/IEC 25010 standard and the Analytic Hierarchy Process (AHP) methodology. Through the integration of various frameworks, our objective is to build a complete evaluation model that effectively identifies and enhances any vulnerabilities in these crucial systems. The strategy we employ combines the qualitative and quantitative evaluation capabilities of ISO/IEC 25010 and AHP, respectively, to offer a comprehensive perspective on software security performance. The results indicate substantial improvements in the security and reliability of whistleblower software, underscoring the effectiveness of our suggested evaluation technique in identifying crucial areas for refinement. Moreover, the utilization of AHP permitted the ranking of security qualities, guaranteeing focused and efficient improvements. Ultimately, the study emphasizes the significance of thorough security assessments for government whistleblower systems and verifies the effectiveness of utilizing ISO/IEC 25010 and AHP as a methodical approach to improve software security. This research enhances the ongoing endeavor to protect confidential data, fostering a more secure and reliable atmosphere for individuals who expose wrongdoing.

Keywords: Security Measurement; Quality Measurement; ISO 25010; Software Quality; Information System; Smart Government.

1. Introduction

It is a fact that the rise of globalization and digitization has propelled the development of smart cities worldwide but there are still a few software security challenges that needs to be considered especially in security awareness (Alfalasi et al., 2022). Similar study is being conducted to develop a methodology for assessing the quality of security in the realm of Information Security Academic applications. This framework is constructed based on the ISO/IEC 25010 quality model. The methodology demonstrates its capability to assess 20 supplementary security aspects and produce consolidated safety ratings in comparison to current quality evaluation criteria (Saptarini et al., 2017). One of the information security assessment models is the Security Assessment and Testing Tools Information Repository (SATTIR) Model. This repository offers the framework for the community to gather and investigate data regarding network security assessment and testing tools. Additionally, it provides valuable features to the community (including end users, practitioners, researchers, and creators) by indexing tool information from many sources to allow user contributions, facilitating comparison of tool attributes using a relational database approach, and offering advanced assistance. Utilizing information retrieval and data warehousing for information analysis, and employing web-enabled tools for information distribution and sharing (Mendes et al., 2023).

Whistleblowing is a highly successful method for exposing instances of corruption among members. Many firms worldwide establish whistleblowing programs, either to comply with regulations or to genuinely address internal fraud (Gibbs, 2020). One of the studies seeks to identify the vulnerabilities of e-Government in order to enhance computer network security and safeguard computer networks (Alsultanny, 2014). Another research for analysis of the implementation of Static Application Security Testing (SAST) into a human-led security assessment process in an open-source e-government project. We outlined the process of selecting, evaluating, and integrating SASTs into a unique strategy that has been embraced by security professionals for software security evaluation. The given text is incomplete and does not provide enough information to rewrite it in a straightforward and precise manner. Please provide more context or complete the sentence (Nguyen-Duc, et al., 2021).

The research used ISO/IEC 25010, which is a recognized quality standard. This research involved several processes to assess the quality, including the identification of security characteristics, the establishment of measuring attributes, the execution of the measurement process, and the formulation of recommendations (Sekarini et al., 2022). Based on the information ecology theory, this paper construct the

*) Corresponding author: 982022025@student.uksw.edu

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/60720

smart city information security risk evaluation system from six aspects (Zhao et al., 2022). Enhancing security in government whistleblower systems through the integration of ISO/IEC 25010 and AHP methodology is crucial due to the need to address significant vulnerabilities that jeopardize the confidentiality, integrity, and availability of sensitive information disclosed by whistleblowers. Amidst a time characterized by the rising complexity of online dangers, it is crucial to prioritize safeguarding those who expose wrongdoing, as this is essential for upholding openness and responsibility in governmental activities. The objective of this project is to enhance the security of whistleblower systems in order to protect persons who are essential in uncovering corruption and wrongdoing from cyber-attacks. The proposed unique technique aims to provide a more efficient and all-encompassing security framework, filling a notable void in current cybersecurity measures and helping to the establishment of a safer environment for individuals who expose wrongdoing.

To assess the efficiency of software security measures in government whistleblower systems, we will utilize the ISO/IEC 25010 standard and the Analytic Hierarchy Process (AHP) approach. Through the integration of various frameworks, our objective is to create a comprehensive evaluation model that can effectively identify and enhance any vulnerabilities in these crucial systems. Our technique combines the evaluative capabilities of ISO/IEC 25010 and AHP, respectively, to comprehensively assess software security performance, utilizing both qualitative and quantitative methods. The results indicate substantial improvements in the security and dependability of whistleblower software, underscoring the effectiveness of our suggested evaluation technique in identifying crucial areas for refinement. Moreover, the utilization of AHP permitted the ranking of security qualities, guaranteeing focused and efficient improvements. Ultimately, the study emphasizes the significance of thorough security assessments for government whistleblower systems and verifies the effectiveness of utilizing ISO/IEC 25010 and AHP as a methodical approach to improve software security.

2. Literature Review

2.1. Whistleblower

A whistleblowing system is a mechanism for reporting and overseeing the activities of an organization or enterprise. The Whistleblowing System consists of four fundamental elements: anonymity, independence, accessibility, and follow-up. The Whistleblowing System is a highly efficient technique for deterring fraudulent activities. The successful execution of this needs the company's dedication to safeguarding the whistleblower's information, an open and accountable reporting process, and the assessment and enhancement of the system (Meitasir et al., 2022). Whistleblowers have a crucial function in the realm of monitoring. Within nearly all employment sectors, individuals who expose purported infractions are safeguarded against retaliation. The challenge of validating charges of violations in the national security domain hinders the ability to impact the dispensation of justice and consequences for truthfulness (Joseph et al., 2022).

2.2. E-Government Security Assessment

The security of the state and its citizens is contingent upon the security of information and IT systems. Instances of cybercrime are documented on a daily basis inside the public administration sectors of all nations. The security of information and IT systems is crucial for the well-being of citizens (Ubowska and Królikowski, 2022). Static Application Security Testing (SAST) is an established quality assurance method in the field of software engineering. Nevertheless, including Static Application Security Testing (SAST) tools into the process of developing products at an industry level and evaluating their security presents a range of technological and management obstacles (Nguyen-Duc, et al., 2021).

2.3. Security Based On ISO/IEC 25010:2011

Based on ISO/IEC 25010:2011, security is used to assess the extent to which a system protects information and data. Security has five sub characteristics. Explanation of each sub characteristics existing on security characteristic are as follows (ISO/IEC, 2011), Show in Figure 1.

Security:

1) Confidentiality: The software ensures that sensitive information is kept private and secure.
2) Integrity: The software maintains data accuracy and prevents unauthorized modifications.
3) Availability: The software is available and accessible when needed.
4) Non-Repudiation: The software provides evidence of actions to prevent denial of performed actions.
5) Authenticity: Degree to which the identity of a subject or resource can be proved to be the one claimed.

Figure 1. Security Characteristic-Sub Characteristic

2.4. Analytic Hierarchy Process (AHP)

The Analytic Hierarchy Process (AHP) is a fundamental methodology for facilitating the decision-making process. The design of this system is to effectively handle both logical and intuitive aspects in order to determine the optimal choice from a set of options, which are assessed based on many criteria.

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/60720

During this procedure, the individual responsible for making decisions engages in the evaluation of pairwise comparisons, which are then used to establish comprehensive priorities for the purpose of rating the available choices. The Analytic Hierarchy Process (AHP) accommodates the presence of inconsistency in judgements while also offering a mechanism to enhance consistency (Saaty, 1990).

In order to effectively address issues using the Analytic Hierarchy Process (AHP), it is important to grasp the fundamental principles.

1) One approach to comprehending complex systems involves the process of creating hierarchies. By deconstructing these systems into constituent pieces, organizing them in a hierarchical manner, and then integrating or synthesizing them, a deeper understanding may be achieved.
2) Evaluation of criteria and alternatives: The assessment of criteria and alternatives is conducted via the use of pairwise comparisons. According to (Saaty, 1990), a scale ranging from 1 to 9 is considered the most suitable for expressing ideas on many matters. The assessment and characterization of a qualitative judgment derived from the Saaty comparison scale may be quantified via the use of an analysis table, shown in Table 1:

Table 1. The fundamental scale (Saaty, 1990)

Intensity of Importance	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective
2	Weak	
3	Moderate importance	Experience and judgment slightly favor one activity over another
4	Moderate plus	
5	Strong importance	Experience and judgment strongly favor one activity over another
6	Strong plus	
7	Very strong or demonstrated importance	An activity is favored very strongly over another; its dominance demonstrated in practice
8	Very, very strong	
9	Extreme importance	The evidence favoring one activity over another is of the highest possible order of affirmation

3) Synthesis of Priority

To properly assess each criterion and alternative, it is crucial to perform a pairwise comparison. The relative comparison values of various criteria can be adjusted according to predefined judgments to determine weights and priority. The determination of weights and priority is accomplished through the manipulation of matrices or the resolution of mathematical equations.

4) Logical Consistency

The term "consistency" has two distinct interpretations. To begin with, objects that share similarities can be categorized based on their uniformity and importance. Furthermore, concerning the degree of correlation between things according to specific criteria. The process of determining logical consistency involves the following steps:

a. Perform matrix multiplication by multiplying each element of the matrix with its associated priority value.
b. Calculate the sum of the products obtained from each line.
c. The summation of each line is divided by the corresponding priority and then aggregated.
d. The quotient of c divided by the total number of elements yields the maximum value of π.
e. The formula for calculating the Consistency Index (CI) is given by $(\pi max-n)/(n-1)$.
f. The consistency ratio (CR) may be calculated by dividing the consistency index (CI) by the random index of consistency (RI), show in Table 2. If the value of the consistency ratio is less than or equal to 0.1, it is possible to provide a valid justification for the conclusions obtained from the data calculations.

Table 2. Random Index Value

n	RI
1	0
2	0
3	0.58
4	0.9
5	1.12
6	1.24
7	1.32
8	1.41
9	1.45
10	1.49
11	1.51
12	1.48
13	1.56
14	1.57
15	1.59

3. Research Method

This study has provided an overview and evaluation of the ISO/IEC 25010 criteria. The security quality assessment of e-government software may be conducted by the use of several methodologies such as AHP, SAW, and other similar approaches. For research step is show in Figure 2. This study makes a significant contribution by including the ISO/IEC 25010 standard for assigning weights. In order to facilitate further measurements using diverse AHP method. Model weighting characteristic show in Figure 3.

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/60720

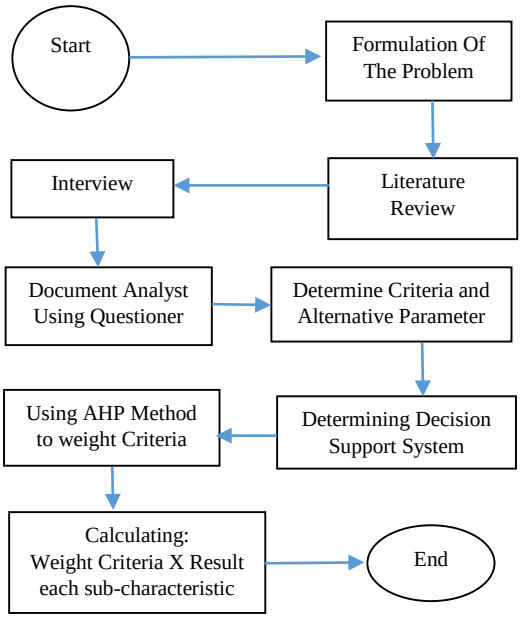

Figure 2. Research Steps

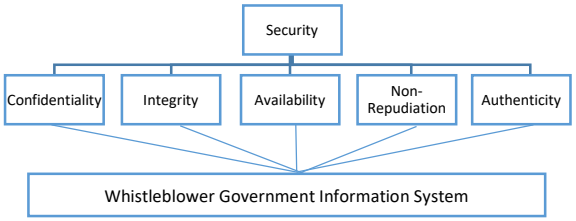

Figure 3. Software Security quality model defined in ISO/IEC 25010 comprises the five sub-characteristics

4. Result And Discussion

In this study the expert will be given a questionnaire to determine the weight of the criteria to be used by the AHP method.

4.1. Result

4.1.1. AHP Method

In this study the expert will be given a questionnaire to determine the weight of the criteria to be used by the AHP method. Expert value is show in Table 3.

Table 3. Experts Value

Criteria	C01	C02	C03	C04	C05
C01	1,000	1,000	2,000	2,000	1,000
C02	1,000	1,000	2,000	1,000	1,000
C03	0,500	0,500	1,000	0,500	0,500
C04	0,500	1,000	2,000	1,000	1,000
C05	1,000	1,000	2,000	1,000	1,000
Total	4,000	4,500	7,500	5,500	4,500

Next, a normalization matrix is generated by dividing each pairwise comparison result by the sum of the outcomes of the criterion. Show in formula (1). Subsequently, the value is included into the right-hand side of the equation, and subsequently divided by the total number of criteria in order to determine the priority weight. Result normalization is show in Table 4.

$$\text{Initial Element Value} = \frac{\text{The Value of each initial matrix element}}{\text{Number of initial columns}} \quad (1)$$

Normalization First line:
Addition of Research Column:

a. Confidential:
   1,000+1,000+2,000+2,000+1,000= 4,000
b. Integrity:
   1,000 +1,000+0,500+1,000+1,000= 4,500
c. Availability:
   2,000+ 2,000+ 1,000+2,000+2,000= 9,000
d. Non-Repudiation:
   2,000 + 1,000+ 0,500+1,000+1,000 = 5,500
e. Authenticity:
   1,000+1,000+0,500+1,000+1,000= 4,500
f. (Functional Suitability / Functional Suitability) / SUM = 1.000 / 4 = 0,25

Then each line is divided by the Total Value per Criteria.

Table 4. Normalization (Eigen Value)

Criteria	C01	C02	C03	C04	C05
C01	0,25	0,22	0,22	0,364	0,22
C02	0,25	0,22	0,22	0,182	0,22
C03	0,125	0,11	0,11	0,091	0,11
C04	0,125	0,22	0,22	0,182	0,22
C05	0,25	0,22	0,22	0,182	0,22
Total	1,000	1,000	1,000	1,000	1,000

If the value has been normalized the priority weight is searched by adding the first row and the next row. Formula for Priority Weight is shown in formula (2) And for the result is shown in Table 5.

$$Priority\ \ Weight = \frac{Number\ \ of\ \ Rows}{Number\ \ of\ \ Criteria} \quad (2)$$

Table 5. Criteria Weight Calculation AHP

Criteria	Sum	Priority Weight	%
C01	1,280	0,256	25,6 %
C02	1,098	0,219	21,96 %
C03	0,549	0,1098	10,98 %
C04	0,973	0,1946	19,46 %
C05	1,098	0,2196	21,96 %
Total	5,000	1,000	100%

Example of calculating Priority Weight
Research Priority Weight:
0,250+0,222+0,222+0,364+0,222=1,280/5=0,256

Next, we need to compute the maximum value of lambda. For formula show in equation (3). To determine lambda max, follow these two steps: first, multiply the value of each criterion's relevance by its weight, then aggregate the results and divide by the total weight. The next phase involves incorporating the value obtained in the initial step, which is then divided by the total number of criteria.

$$\lambda = \begin{bmatrix} \Sigma\ row\ \ K1 \\ \vdots \\ \Sigma\ row\ \ Kn \end{bmatrix} x \begin{bmatrix} BP1 \\ \vdots \\ BPn \end{bmatrix} = \begin{bmatrix} \lambda max\ \ K1 \\ \vdots \\ \lambda max\ \ Kn \end{bmatrix} \quad (3)$$

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/60720

Information:
BP: Priority Weight
K: Column

The example of calculating lambda max uses data from the previous step. Looking for Lamda Max with a formula (4).

$$\lambda = \frac{\text{Number of elements in the matrix}}{\text{m}} \quad (4)$$

$$\lambda \max = (((4{,}000 * 0.256) + (4{,}500 * 0{,}219) + (9 * 0{,}1098) + (5{,}500 * 0{,}1946) + (4{,}500 * 0{,}219) = 5{,}053$$

Then the Lambda value is 5,053

The final step is to calculate the consistency index value (CI) used to calculate the consistency ratio value that will determine whether the pairwise comparison matrix to be obtained from the results of the questionnaire has a consistent or not. Formula Consistency Index show in equation (5). The purpose of the consistency test is to determine the consistency of the answers that have been filled in by the respondents which will affect the stability of the results. By being declared consistent, the data can be used and processed to the next stage.

$$CI = \frac{\lambda max - n}{(n-1)} \quad (5)$$

Information:
n: number of criteria

$$\text{CI} = \frac{(5{,}053 - 5)}{4} = 0{,}01325 \ \textbf{Consistent}$$

Next, we will determine the ratio consistency value (CR) using the method CR = CI / RI. The Random Index (RI) value is derived from the L.Saaty Table 1. The random index value will be used to calculate the consistency ratio (CR). And formula show in equation (6). The CR value will determine if the paired comparison matrix, obtained from the questionnaire data, demonstrates consistency. The index's random value can be noticed in the Random Index Table 2. A consistency ratio (CR) is deemed genuine or consistent if its value is below 0.1 or comparable to less than 10%. On the other hand, the CR is said to be invalid or inconsistent if its value is more than or equal to 0.1. The determination of the CR value is contingent upon its formulation:

$$CR = \frac{CI}{RI} \quad (6)$$

CR = 0.15/1.12 = 0,1

In the two tables above the consistency ratio (CR) obtained a value of 0. This means that the ratio is considered consistent (CR <0.1) so that the assessment given by the respondents in the questionnaire is considered feasible. Result Security Criteria Weight use AHP method is show in Figure 4.

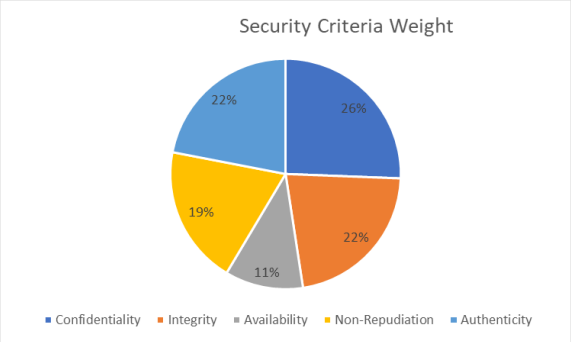

Figure 4. Result Criteria Weighting AHP Method

4.1.2. Result Security Characteristic

The evaluation of the "Security" attribute within the framework of ISO/IEC 25010, a software quality standard, entails assessing multiple facets that ensure the protection of data and the proper functioning of the system. Calculation of the value of each Security sub-criteria can use the following formula number (7), (8), (9), (10), (11), and for total value Security Characteristic use equation number (12).

$$\text{Confidentiality} = \frac{\sum \text{Confidential}}{10} \times 26\% \quad (7)$$

$$\text{Integrity} = \frac{\sum \text{Integrity}}{7} \times 22\% \quad (8)$$

$$\text{Availability} = \frac{\sum \text{Availability}}{10} \times 11\% \quad (9)$$

$$\text{Non} - \text{Repudiation} = \frac{\sum \text{Non-Repudiation}}{7} \times 19\% \quad (10)$$

$$\text{Authenticity} = \frac{\sum \text{Authenticity}}{5} \times 22\% \quad (11)$$

$$\text{Total Security Characteristic} = \frac{\sum \text{Confidential+Integriry+Availability+Non-Repudiation+Aunthenticity}}{5} \quad (12)$$

1) Confidentiality

Confidentiality evaluates the level of safeguarding against unauthorized disclosure of data/information within the system, without the authorization of the Reporter (Saptarini et al., 2017).

Access to an Agency's Whistleblower data/information is restricted to the Agency's stakeholders alone. In this scenario, the individuals residing in a certain country and the governing authorities. Confidentiality encompasses 10 metrics that include access control, control over access to the Whistleblower source code, safeguarding of log information, protection of Whistleblower test data, control over malicious code, management of

removable media, session timeout, strength of cryptographic algorithms, accuracy of data encryption, and management of cryptographic keys.

Table 6. Confidentiality Evaluates

Metric Name	Result
Access control	1
Control over access to the Whistleblower source code	0,8
Safeguarding of log information	1
Protection of Whistleblower test data	0,7
Control over malicious code	0,8
Management of removable media	1
Session timeout	1
Strength of cryptographic algorithms	0,2
Accuracy of data encryption	0,76
Management of cryptographic keys	0
Total	7,26

$$\text{Confidentiality} = \frac{7,26}{10} \times 26\% = \mathbf{18,876}\%$$

2) Integrity

Acts like as illegal access, unauthorized alterations, data manipulations, audit tampering, data backdating, data fabrication, phishing, and spoofing are no longer limited to individual wrongdoers. They are also widespread in organized institutions and even governments. Consequently, ensuring data security necessitates the implementation of robust data integrity safeguards and corresponding technical controls (Duggineni, 2023). Integrity evaluates the precision and comprehensiveness with which Whistleblower assets are upheld. In the Whistleblower, the asset under security is data or information pertaining to the complaint handling systems within government institutions, including citizen data. Integrity encompasses **seven** metrics, namely data integrity compliance, prevention of internal data corruption, inventory of assets, information back-up, documented operating procedures, fault logging for whistleblowers, and security of whistleblower documentation.

Table 7. Integrity Evaluates

Metric Name	Result
Namely data integrity compliance	1
Prevention of internal data corruption	0,7
Inventory of assets	0,6
Information back-up	1
Documented operating procedures	0,9
Fault logging for whistleblowers	0,9
Security of whistleblower documentation	0,8
Total	5,9

$$\text{Integrity} = \frac{5,9}{7} \times 22\% = 18,5\%$$

3) Availability

Ensures efficient system functionality and prevents authorized users from being denied service (Khan et al., 2022). When assessing the availability of a system or application, certain crucial metrics are commonly employed. Availability pertains to the capacity of a system to consistently function and be easily accessible as required. There are 10 metrics that will be assessed, including Uptime/Downtime, Mean Time Between Failures (MTBF), Mean Time to Repair (MTTR), Availability Rate, Rate of Failure Occurrence, Response Time, Service Level Agreement (SLA) Compliance, Redundancy and Failover Capabilities, Load Balancing Efficiency, and Disaster Recovery and Backup Effectiveness.

Table 8. Availability Evaluates

Metric Name	Result
Uptime/Downtime	0,7
Mean Time Between Failures (MTBF)	0,7
Mean Time to Repair (MTTR)	0,6
Availability Rate	0,8
Rate of Failure Occurrence	0,9
Response Time	0,8
Service Level Agreement (SLA) Compliance	0,9
Redundancy and Failover Capabilities	0,5
Load Balancing Efficiency	0,5
Disaster Recovery and Backup Effectiveness	0,7
Total	7,1

$$\text{Availability} = \frac{7,1}{10} \times 11\% = 7,81\%$$

4) Non-Repudiation

The necessity for non-repudiation is widely recognized as a significant security requirement on a global scale. An adequate level of non-repudiation can effectively enforce security measures and hence guarantee the security of deployed software (Pandey and Mustafa, 2012). When assessing the inclusion of "Non-Repudiation" in system or application security, various metrics and criteria can be utilized or taken into account. Non-Repudiation refers to the system's capacity to offer indisputable proof of transactions or acts carried out, hence preventing users from denying their participation. Have 7 metric for evaluate: The reliability of digital signatures and electronic certificates, the integrity of logs and audit trails, the effectiveness of authentication mechanisms, the retention time and accessibility of evidence, and compliance with standards and regulations. Capability to produce and retain evidence while also demonstrating resilience against fraudulent activities and manipulation.

Table 9. Non-Repudiation Evaluates

Metric Name	Result
The reliability of digital signatures and electronic certificates	0
The integrity of logs and audit trails	0,8
The effectiveness of authentication mechanisms	0,9
The retention time and accessibility of evidence	0,7
Compliance with standards and regulations.	0,9
Ability to Generate and Store Evidence	0,3
Resistance to Fraud and Manipulation	0,5
Total	4,1

$$\text{Non} - \text{Repudiation} = \frac{4,1}{7} \times 19\% = 11,12\%$$

5) Authenticity

Authenticity or credibility check of applications or softwares, to be installed on a system (Naeem et al.,

2019). Authenticity evaluates the degree to which the identity of a topic, whether it is a user or a system, can be verified as genuine. Whistleblowing involves multiple people with diverse interests and varying levels of access privileges. It is necessary to authenticate the user's identity in order to safeguard the data from unauthorized disclosure. The concept of authenticity is measured by five metrics, which include adherence to authentication protocols, user registration, management of user passwords, privilege management, and restrictions on information access.

Table 10. Authenticity Evaluates

Metric Name	Result
Include adherence to authentication protocols	0,8
User Registration	1
Management of user passwords	1
Privilege management	1
Restrictions on information access	1
Total	4,8

$$\text{Authenticity} = \frac{4,8}{5} \times 22\% = 21,12\%$$

$$\text{Total Security Characteristic} = \frac{\sum 18.876 + 18.5 + 7.81 + 11,12 + 21.12}{5} = 77,426\ \%$$

4.2. Discussion

The security of government whistleblower applications was assessed using ISO/IEC 25010 criteria for software security and the AHP technique. The resulting weight values for each criterion were as follows: Confidentiality 22%, Integrity 19%, Availability 11%, Non-Repudiation 22%, and Authenticity 26%. These data indicate that the Authenticity criterion carries the highest weight compared to the other criteria.

Once the criteria weight values have been obtained, an evaluation of each criterion is conducted. Subsequently, the scores for each category are aggregated, resulting in a final evaluation of 77.42 % for the government whistleblower application. This demonstrates the efficacy of the security software. This study employs a quantitative methodology, gathering data through questionnaires and interviews administered to security professionals and whistleblowers.

The purpose of this study is to assess the security of whistleblower apps by employing ISO/IEC 25010 standards and utilizing the Analytic Hierarchy Process (AHP) methodology. The user emphasizes the significance of upholding data integrity, confidentiality, and availability in software security. Data integrity is a notable advantage, although confidentiality and availability are regarded as disadvantages. This study emphasizes the disparities between existing security demands and real-world implementation, emphasizing the significance of employing the ISO/IEC 25010 standard in software development and assessment to enhance security and safeguard individuals who expose wrongdoing in governmental settings. This underscores the necessity of implementing a comprehensive security policy that encompasses not only the prevention of data breaches but also the guarantee of ongoing accessibility and reliability for users.

5. Conclusion

The results of this study clearly show that using ISO/IEC 25010 and AHP techniques effectively improves the security frameworks of government whistleblower systems. The strategic evaluation has successfully achieved its goal by significantly enhancing the safeguarding and safety of those who expose wrongdoing, therefore fostering a more reliable and secure atmosphere for reporting misconduct in government contexts.

To enhance future work, it would be beneficial to investigate the incorporation of real-time threat detection algorithms into the existing security architecture of the government whistleblower software. Furthermore, exploring the suitability of blockchain technology could provide improved confidentiality and authenticity for individuals who expose wrongdoing. Including a more extensive array of cybersecurity standards and procedures in the research would offer a more comprehensive outlook on techniques for enhancing security. Conducting empirical research to validate the effectiveness of the proposed enhancements in real-world settings would be extremely beneficial for ongoing improvement and adjustment to emerging cyber threats.

Reference

Alfalasi, S., Akmal, S., Kamalrudin, M., Hakimi, H., 2022. An Awareness Model for Software Security in Smart Government: A Systematic Review. *Mathematical Statistician and Engineering Applications*, 71(3), 54-66. https://doi.org/10.17762/msea.v71i3.106

Alsultanny, Y.A., 2014. Assessment of E-Government Weak Points to Enhance Computer Network Security. *International Journal of Information Science*, 4(1), 13-20. https://doi.org/10.5923/j.ijis.20140401.03

Duggineni, S., 2023. Data Integrity and Risk. *Open Journal of Optimization*, 12(2), 25-33. https://doi.org/10.4236/ojop.2023.122003

Gibbs, T., 2020. Whistleblowing: protection or discouragement. *Journal of Money Laundering Control*, 23 (3), 591-600. https://doi.org/10.1108/JMLC-03-2020-0031

ISO/IEC, 2011. INTERNATIONAL STANDARD ISO / IEC 25010 (Vol. 2011).

Joseph, M. F., Poznansky, M., Spaniel, W., 2022. Shooting the Messenger: The Challenge of National Security Whistleblowing. *Journal of Politics*, 84(2), 846-860.

https://doi.org/10.1086/715595

Khan, R.A., Khan, S.U., Khan, H.U., Ilyas, M., 2022. Systematic Literature Review on Security Risks and its Practices in Secure Software Development. *IEEE Access*, 10, 5456-5481. https://doi.org/10.1109/ACCESS.2022.3140181

Meitasir, B.C., Komalasari, A., Septiyanti, R., 2022. Whistleblowing System and Fraud Prevention: A Literature Review. *Asian Journal of Economics, Business and Accounting*, 22(18), 23-29. https://doi.org/10.9734/ajeba/2022/v22i1830644

Mendes, N., Durães, J., Vieira, M., Madeira, H., 2023. Security Assessment and Testing Tools Information Repository. *Anais do IX Workshop de Testes e Tolerância a Falhas*, 87-100. https://doi.org/10.5753/wtf.2008.23148

Naeem, R.Z., Abbas, H., Shafqat, N., Saleem, K., Iqbal, W., 2019. A framework to determine applications' authenticity. P*rocedia Computer Science*, 155(2018), 268-275. https://doi.org/10.1016/j.procs.2019.08.038

Nguyen-Duc, A., Do, M.-V., Luong-Hong, Q., Nguyen-Khac, K., Truong-Anh, H., 2021. On the Combination of Static Analysis for Software Security Assessment – A Case Study of an Open-Source e-Government Project. *Advances in Science, Technology and Engineering Systems Journal*, 6(2), 921-932. http://dx.doi.org/10.25046/aj0602105

Nguyen-Duc, A., Do, M. V., Hong, Q.L., Khac, K.N., Quang, A.N., 2021. On the adoption of static analysis for software security assessment–A case study of an open-source e-government project. Computers and Security, 111, 102470. https://doi.org/10.1016/j.cose.2021.102470

Pandey, S.K., Mustafa, K., 2012. Security assurance by efficient non-repudiation requirements. *Advances in Computer Science, Engineering & Applications*, 167, 905-912. https://doi.org/10.1007/978-3-642-30111-7_87

Saaty, T.L., 1990. How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, 48(1), 9-26. https://doi.org/10.1016/0377-2217(90)90057-I

Saptarini, I., Rochimah, S., Yuhana, U.L., 2017. Security Quality Measurement Framework for Academic Information System (AIS) Based on ISO/IEC 25010 Quality Model. *IPTEK Journal of Proceedings Series*, (2), 128-135. http://dx.doi.org/10.12962/j23546026.y2017i2.2310

Sekarini, D., Alfiani, F.S., Rochimah, S., 2022. Security Characteristic Evaluation Of New Student Admission Information System Based on ISO/IEC 25010 Quality Standard. *ACM International Conference Proceeding Series*, 120-124. https://doi.org/10.1109/ICITEE49829.2020.9271756

Ubowska, A., Królikowski, T., 2022. Building a cybersecurity culture of public administration system in Poland. *Procedia Computer Science*, 207, 1242-1250. https://doi.org/10.1016/j.procs.2022.09.180

Zhao, H., Wang, Y., Liu, X., 2022. The assessment of smart city information security risk in China based on zGT2FSs and IAA method. Scientific Reports, 12(1), 1-14. https://doi.org/10.1038/s41598-022-07197-1