Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012


JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

# DEVELOPMENT OF CYBER SECURITY CULTURE AUDIT SYSTEM USING SEVEN DIMENSIONS OF ISC

Akhyari Nasir[1*], Noor Suhana Sulaiman[2]

[1] Faculty Computer, Media and Technology Management, University College TATI, 24000 Kemaman, Terengganu, Malaysia
Email: akhyari@uctati.edu.my
[2] Faculty Computer, Media and Technology Management, University College TATI, 24000 Kemaman, Terengganu, Malaysia
Email: suhana@uctati.edu.my
[*] Corresponding Author

**Article Info:**

**Article history:**
Received date: 31.03.2025
Revised date: 27.04.2025
Accepted date: 29.05.2025
Published date: 20.06.2025

**To cite this document:**

Nasir, A., & Sulaiman, N. S. (2025). Development Of Cyber Security Culture Audit System Using Seven Dimensions Of ISC. *Journal of Information System and Technology Management, 10* (39), 185-196.

**DOI:** 10.35631/JISTM.1039012



**Abstract:**

This paper presents the design of a Cyber Security Culture Audit (CSCA) system intended to improve cybersecurity practices within organizational settings. The system is built upon seven validated dimensions that define Information Security Culture (ISC), namely: Procedural Countermeasures (PCM), Risk Management (RM), Security Education, Training, and Awareness (SETA), Top Management Commitment (TMC), Security Monitoring (MON), Information Security Knowledge (ISK), and Information Security Knowledge Sharing (ISKS). These dimensions serve as the assessment criteria, ensuring validity and trustworthiness. Implemented as a web-based platform using HTML, PHP, and MySQL, the system offers a user-friendly interface, efficient backend processing, and robust data management. Through iterative deployment and real-world feedback, the system has been refined to provide detailed evaluations of an organization's Cyber Security Culture (CSC). The results demonstrate that the CSCA system is effective in providing comprehensive insights into an organization's cybersecurity posture. This study emphasizes the significance of continuous improvement in CSC and offers a valuable tool for enterprises to increase their security policies and prevent cyber threats. Limitations and future work are discussed to guide further research and development in this critical area.

**Keywords:**

Information Security Culture, Audit System, Cyber Security Culture.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012

## Introduction

The rising frequency and sophistication of cyber threats have made it vital for organizations to not only invest in advanced technological defenses but also create a strong Cyber Security Culture (CSC). CSC relates to the attitudes, beliefs, and behavior of employees toward information security. It is generally recognized that a strong CSC is vital for minimizing human error and improving the overall security posture of a company (Ashenden & Sasse, 2013). Although many scholars have emphasized the importance of cultivating Information Security Culture (ISC), comprehensive systems for assessing either ISC or Cyber Security Culture (CSC) remain limited. This gap in assessment tools poses a significant challenge for organizations striving to improve their security culture. Extensive studies over the years have identified proven criteria that are significant in measuring ISC. However, the translation of these criteria into practical, systematic assessment tools remains limited.

Several academic studies have focused on developing and implementing audit systems using ISC dimensions. For instance, Da Veiga & Eloff (2010) formulated a framework for assessing an organization's ISC, incorporating many characteristics to provide an in-depth assessment. Their study highlights the importance of a multidimensional approach in identifying strengths and weaknesses within an organization's security practices. Another significant contribution is the Information Security Culture Assessment (ISCA) tool developed by Thomas Schlienger & Teufel (2003). This tool employs surveys and interviews to gauge the security culture across various dimensions, enabling organizations to gain insights into their security awareness, behavior, and compliance levels. The ISCA tool has been instrumental in helping organizations identify specific areas for improvement and implement targeted interventions.

Additionally, research on organizational ISC highlights the significance of structured approaches to security management. For example, studies on information security in critical infrastructure emphasize that organizations must follow continuous monitoring practices, regular security audits, and employee engagement initiatives to effectively enhance their security posture and respond to evolving threats (Nævestad et al., 2018). Despite these developments, there is a high demand for robust and comprehensive systems specifically developed to monitor and improve ISC. Nasir et al. (2019) identified seven new criteria for assessing ISC's impact on Information Security Policy (ISP) compliance behavior. The study was carried out at 19 of Malaysia's 21 public universities and validated using Partial Least Square Structural Equation Modelling (PLS-SEM). The findings revealed that all seven components contribute significantly to the concept of ISC, with Information Security Knowledge being the most relevant. The study demonstrated that this ISC model could effectively influence employees' security behavior, emphasizing the need for practitioners to adopt these dimensions to assess, improve, and cultivate a positive ISC.

In conclusion, the development of comprehensive audit systems based on the seven dimensions of ISC represents a significant advancement in the field of cyber security. These systems enable organizations to systematically assess their security culture, identify areas for improvement and apply effective actions to establish a resilient and adaptive security environment. As cyber threats continue to evolve, the importance of cultivating a strong CSC cannot be overstated. Through rigorous assessment and continuous improvement, organisations can better protect their assets and preserve stakeholder trust in an increasingly digital world. Therefore, the dimensions identified by Nasir et al. (2019) should be utilized to develop these assessment systems, ensuring a comprehensive approach to enhancing ISC.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012

## Literature Review

This literature review section provides an overview of the current state of study on the construction of a Cyber Security Culture Audit (CSCA) system, specifically employing the seven aspects of ISC. The review is organized into two main subsections: "Auditing Cyber Security Culture" and "ISC Dimensions." The first subsection examines various models and frameworks that have been proposed and implemented to assess and enhance CSC within organizations, highlighting their methodologies, effectiveness, and practical applications. The second subsection delves into the specific ISC dimensions identified by Nasir et al. (2019), exploring their empirical validation and significance in shaping employees' security behavior and compliance within higher educational institutions. This structured approach provides a thorough foundation for understanding the multifaceted nature of CSC and its critical role in strengthening organizational resilience against cyber threats.

### Auditing Cyber Security Culture

In today's connected digital environment, organizations facing escalating cyber risks must prioritize safeguarding information assets. A core strategy for mitigating these risks is developing a robust Cyber Security Culture (CSC), which encompasses the collective behaviors, beliefs, and attitudes toward security within an organization (Ashenden & Sasse, 2013). To this end, various models and frameworks have emerged to evaluate and strengthen CSC. For example, T. Schlienger & Teufel (2005) developed the Information Security Culture Assessment (ISCA) tool, which supports security officers by identifying strengths and weaknesses through surveys and proposing measures to improve an organization's security culture. This tool emphasizes a cyclical management process, incorporating analysis, planning, implementation, and evaluation to foster a lasting security culture. Similarly, Da Veiga & Eloff (2010) proposed a framework that integrates technical, procedural, and human behavior components, focusing on employee actions and fostering a security-aware environment. Their work highlights the critical role of both organizational and individual behavioral factors in cultivating a security-minded workforce. The framework by Albrechtsen & Hovden (2010) complements these approaches by emphasizing employee participation, collective reflection, and feedback in maintaining security awareness across all levels of an organization. These models collectively underscore the importance of evaluating CSC as a multi-dimensional and continuous process, essential for building resilient security practices.

Nasir et al. (2019) introduced and validated a model consisting of seven key dimensions to assess Information Security Culture (ISC), which include: Procedural Countermeasures (PCM), Risk Management strategies (RM), Security Education, Training, and Awareness initiatives (SETA), Top Management Commitment (TMC), continuous Monitoring efforts (MON), Information Security Knowledge (ISK), and the practice of Information Security Knowledge Sharing (ISKS). Their study, conducted in Malaysian higher educational institutions, validated these dimensions' significance in influencing employees' security behavior, underscoring the need to integrate such dimensions into audit systems. Additionally, Greig et al. (2015) conducted an ethnographic study revealing discrepancies between policy and practice in a retail store's security culture, highlighting the importance of practical assessment methods to bridge policy implementation gaps and enhance CSC effectively. Sabillon et al. (2017) established the Cyber Security Audit Model (CSAM), a comprehensive way to assessing cybersecurity controls across all corporate operations. CSAM, which was tested in a Canadian higher education institution, improves cybersecurity assurance in the face of evolving threats. Shkarlet et al. (2020) proposed a model for estimating information security

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012
culture levels using fuzzy decision-making methods, considering the competence of security specialists and integrating qualitative relationships to assess and improve ISC effectively.

Understanding the relationship between company culture and security results is critical for an effective CSC evaluation. Ashenden & Sasse (2013) suggest that cultural factors significantly shape employees' adherence to security policies and their proactive stance towards cybersecurity, highlighting the importance of integrating cultural assessments into cybersecurity frameworks for holistic risk management. Developing a CSCA system using the Seven Dimensions of ISC represents a significant advancement in cybersecurity management, providing a structured framework to comprehensively evaluate and enhance ISC. Integrating insights from seminal studies and practical assessment methodologies, organizations can strengthen their security posture and effectively mitigate evolving cyber threats.

**ISC Dimensions**

Nasir et al. (2019) investigated how ISC, described through seven distinct characteristics, influences the information security behavior of personnel within Higher Education Institutions (HEIs). The research model was evaluated using data from 604 Malaysian public higher education personnel. The study discovered that these seven dimensions provide a substantial contribution to the ISC concept, which impacts workers' behavior elements such as attitude, normative belief, and self-efficacy, eventually influencing their intention to comply with the ISP. Nasir et al., (2019) developed a model that demonstrated high predictive accuracy and parsimony when compared to previous models for forecasting ISC's perspective on ISP compliance behavior.

Nasir et al. (2019) conducted one of the pioneering studies that utilized a dimension-based ISC model to investigate compliance behavior with ISP. In contrast to other models that included variables such as Job Satisfaction and Perceived Organizational Support (D'Arcy & Greene, 2014), Information Security Awareness (Rocha Flores & Ekstedt, 2016), and Perceived Punishment Certainty, Perceived Punishment Severity, and Organizational Commitment (Dugo, 2007). These models focused on various elements of security behavior, including resistance to social engineering and ISP violations. However, Nasir et al. (2019)'s model focuses primarily on ISC as the dependent variable, offering a more complete and ISC-centric approach to evaluating ISP compliance behavior.

The findings of Nasir et al. (2019) found that the organizational culture-based seven dimensions by Schein (1992) and Niekerk & Solms (2006) are experimentally applicable and significant. All the dimensions contribute to ensure the ISC construct's content validity. Among these, Information Security Knowledge was identified as the most important dimension. The study offered a comprehensive ISC model, addressing the lack of a universally accepted ISC concept and responding to calls for more comprehensive frameworks to guide the establishment of ISC in organizations (Karlsson & Hedström, 2014; Tolah et al., 2017). The findings provide new perspectives on ISC and ISP compliance behavior's relationship, emphasizing the relevance of ISC in cultivating desired behavioral characteristics and enhancing security policy compliance intents among employees.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012

## Methodology

The methodology for the development of the Cyber Security Culture Audit (CSCA) system is grounded in Nasir's et. al research (2019), which identified seven critical dimensions that significantly influence Information Security Culture (ISC). The dimensions outlined comprise Procedural Countermeasures (PCM), Risk Management (RM), Security Education, Training, and Awareness (SETA), Top Management Commitment (TMC), Security Monitoring (MON), Information Security Knowledge (ISK), and Information Security Knowledge Sharing (ISKS). Given the alignment between CSC and ISC, these dimensions serve as a robust framework for the CSC audit system, ensuring its validity and effectiveness in shaping employees' compliance with Information Security Policies. All seven dimensions were utilized as the assessment criteria for the system to evaluate CSC.

To enhance accessibility and usability, the CSC audit system is designed as a web-based platform. This decision allows users to access the system conveniently from any location and at any time using their smartphones or computers. The web-based interface, crafted using HTML, provides an intuitive and user-friendly experience. The backend processing of user inputs and generation of outputs is handled by PHP, chosen for its versatility and robustness. This combination ensures that the system can efficiently handle complex calculations and present clear and concise results to users. Data management is a crucial aspect of the CSC audit system. For storing and retrieving information, the system leverages a MySQL database, known for its speed and security in handling large datasets. This database management system enables the CSC audit system to efficiently store assessment data, support data analysis, and facilitate decision-making processes for organizations aiming to improve their cybersecurity culture.

By integrating the validated dimensions from Nasir et al. (2019) research with the convenience of a web-based platform powered by HTML, PHP, and MySQL, the CSC audit system provides a comprehensive evaluation of an organization's cybersecurity posture. This holistic approach encompasses PCM, RM, SETA, TMC, MON, ISK, and ISKS. The utilization of this audit system holds the potential to drive positive changes, leading to strengthened security practices, increased employee compliance, and a culture of vigilance in safeguarding sensitive information and assets from cyber threats.

Figure 1 illustrates the methodology for developing the CSCA system. The development process begins with Nasir et al. (2019) study, which provides a foundational framework by identifying seven critical dimensions of ISC. These dimensions are adopted and adapted to form the assessment criteria for the CSC audit system, ensuring the system's validity and trustworthiness. The audit system is built on a web-based platform, with HTML for the user interface, PHP for backend processing, and MySQL for efficient data storage and retrieval. Following this initial development, the system is deployed and constantly refined via an iterative approach guided by real-world applications and user input. Following this initial development, the system is deployed and constantly refined via an iterative approach guided by real-world applications and user input. This constant improvement guarantees that the system remains responsive to changing business needs and cybersecurity issues. Regular upgrades, based on user feedback, include interface enhancements, improved data visualization, and the incorporation of new features. Such enhancements demonstrate the CSCA system's dedication to continual improvement, eventually providing organizations with a realistic, relevant, and effective instrument for measuring and building cybersecurity culture.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012

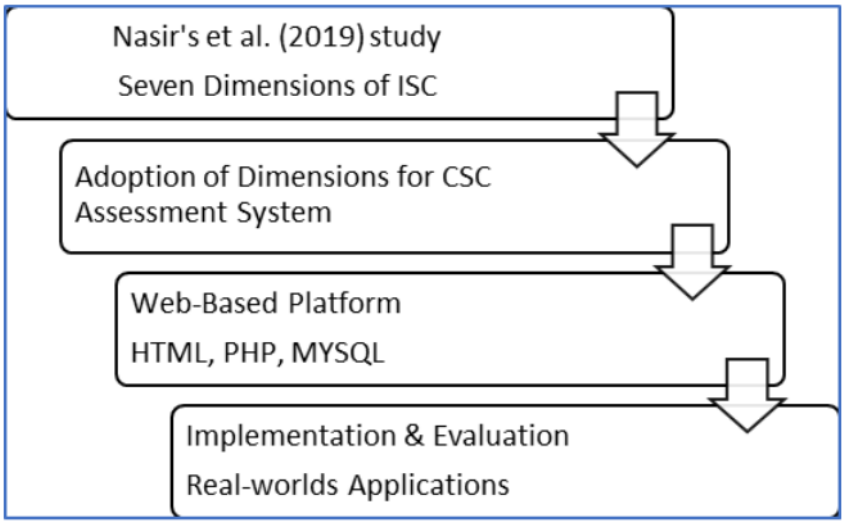


**Figure 1: Process of CSCA Development**

**Result**

The development of the CSCA system, based on the methodology outlined in the previous section, was successfully executed and implemented on a server. The system can be accessed via mobile phones or computers, providing flexibility and convenience. The initial interface of the system is depicted in Figure 2, which shows the login page designed for administrative access. Administrators need a verified account, including a username and password, to utilize the system.


**Figure 2: Login Page for Admin**

Once logged in, administrators can create and manage surveys by completing various required fields in the provided forms. The administrator is required to input information across multiple forms to configure the survey effectively. The survey creation process involves setting up two primary components: Demographics and CSC Criteria. Each component comprises specific

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012

elements. For demographics, the administrator must include input fields such as sex, age, race, education, and work experience, as shown in Figure 3.

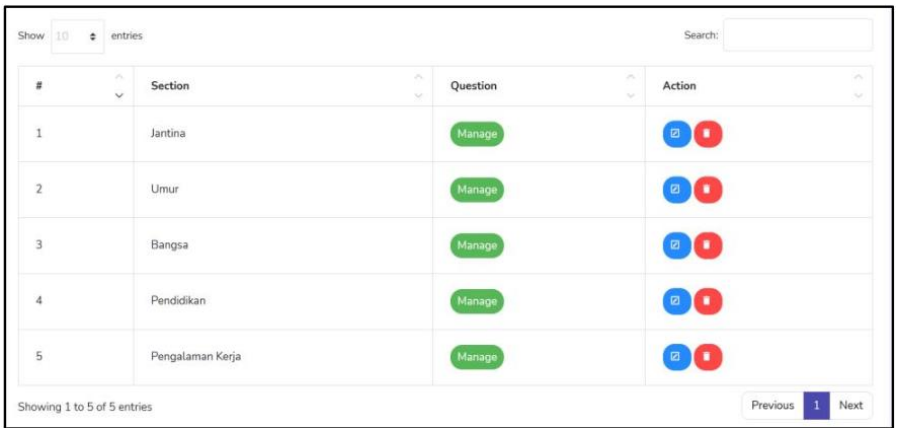


**Figure 3: Demographic Fields**

Regarding the CSC Criteria, the system incorporates the seven validated dimensions identified by Nasir et al. (2019) as foundational elements for assessing CSC. These dimensions include PCM, RM, SETA, TMC, MON, ISK and ISKS as shown in Figure 4. The system uses these criteria to evaluate an organization's CSC, with specific items and questions based on Nasir's study to measure each dimension effectively. An example of items used to measure ISP criteria is provided in Figure 5.

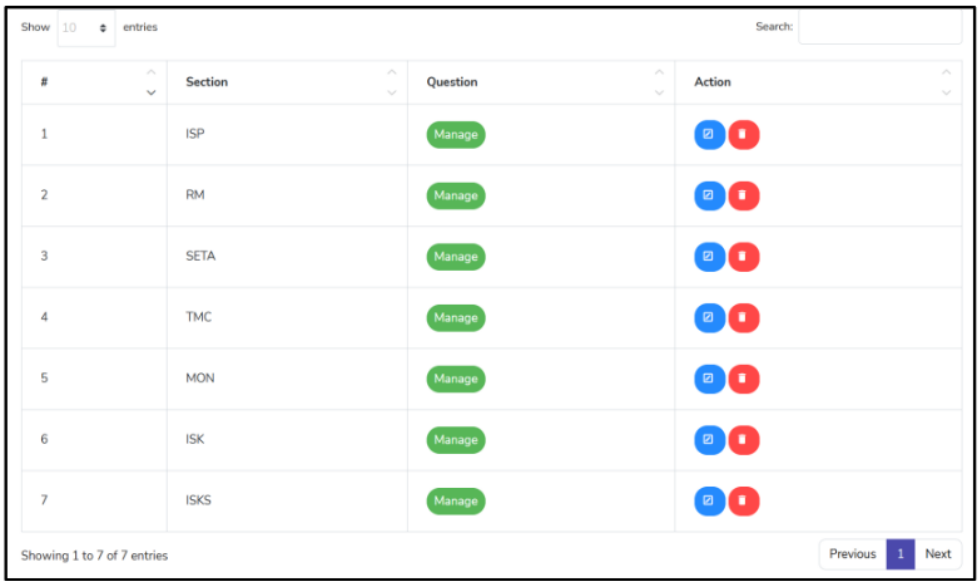


**Figure 4: Criteria of CSC**

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012

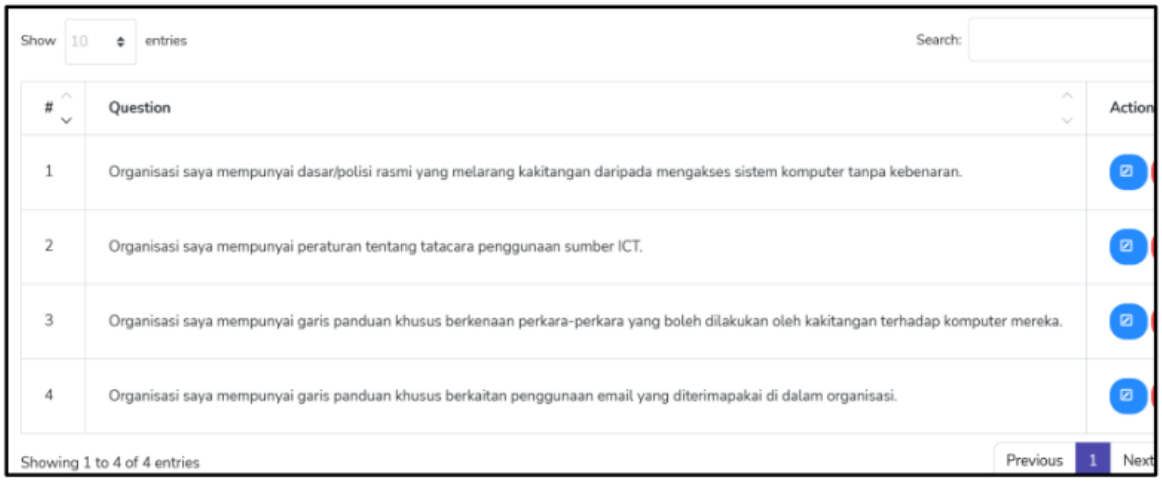


**Figure 5: Sample Items to Measure ISP Criteria**

After configuring the survey, it is distributed to participants, typically employees within an organization undergoing CSC evaluation. Participants complete the survey, and their responses are recorded and analyzed by the system. The system calculates the CSC criteria based on the collected data, generating comprehensive reports. These reports include detailed demographic profiles of respondents, as shown in Figure 6, and specific results for each CSC criterion. For instance, Figure 7 displays the current status of a company's ISP as "Moderate," indicating that some staff may not fully understand ISP policies. This insight enables management to take corrective actions to enhance policy comprehension and adherence. Finally, the system provides an overall CSC status report for the organization, as illustrated in Figure 8. These reports are critical for top management to assess their organization's security culture and implement necessary improvements.

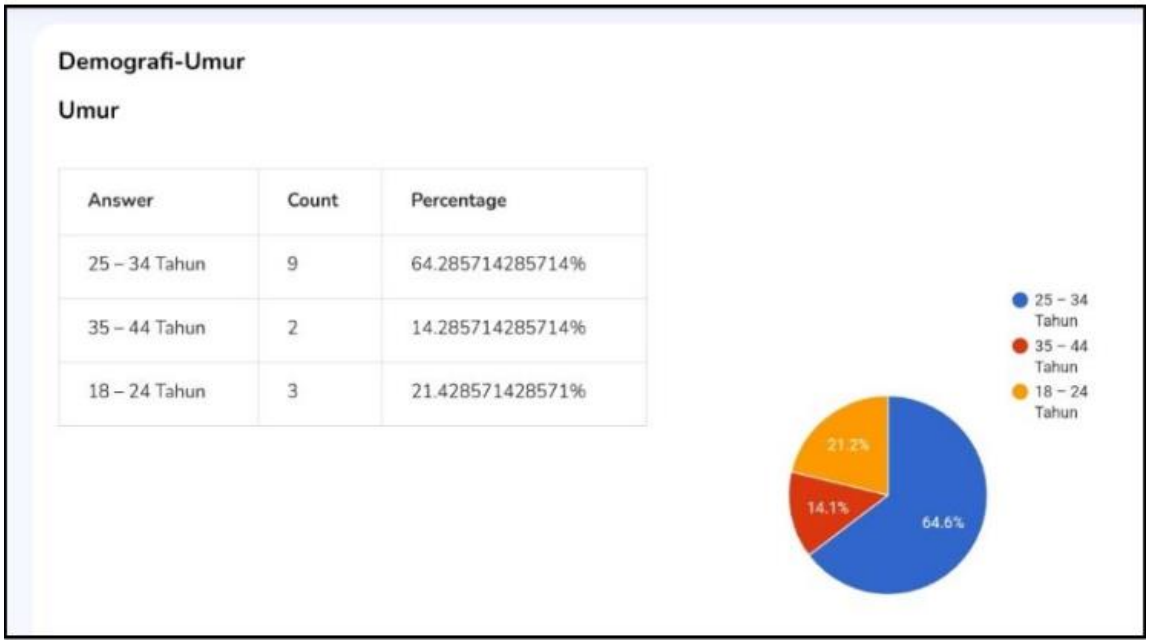


**Figure 6: Age of Respondents**

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012


**Figure 7: Status of ISP**


**Figure 8: Status of Overall CSC**

## Discussion

The Cyber Security Culture (CSC) assessment system, developed and deployed successfully, leverages (Nasir et al., 2019) seven dimensions as a framework to evaluate an organization's cybersecurity culture. The system, accessible via mobile phones and computers, incorporates a user-friendly web-based platform using HTML for the interface, PHP for backend processing, and MySQL for data management. The CSC audit system's deployment underscores its practical applicability in real-world settings. The use of a web-based platform enhances accessibility and usability. This system, by providing a holistic evaluation based on validated dimensions, offers a more comprehensive assessment compared to existing models.

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012

For instance, Alhogail (2015) developed a model focusing on employee behavior and awareness, but our system extends this by incorporating procedural and managerial aspects, thus providing a thorough evaluation of CSC. This comprehensive approach ensures that all facets of cybersecurity culture are assessed, offering a more robust framework for organizations to improve their security practices. Comparing our system to the Cybersecurity Audit Model (CSAM) proposed by Sabillon et al. (2017), which focuses on converging IT and InfoSec audits to address evolving cyber threats, our system similarly adapts to contemporary challenges by integrating validated dimensions and leveraging advanced web technologies. The iterative design and real-world application of our system ensure its effectiveness and reliability, consistent with the principles of design science research highlighted by Hevner et al. (2004).

Additionally, the system's capability to store and analyze data using MySQL facilitates efficient data management and supports decision-making processes. This aligns with the observations of (Siponen & Vance, 2010), who noted that robust technological infrastructure enhances the effectiveness of security measures. The comprehensive evaluation provided by our system, covering all seven dimensions, offers a detailed assessment that helps organizations identify and address vulnerabilities, thereby strengthening their overall cybersecurity posture.

The ethnographic study by Greig et al. (2015) revealed that even organizations with seemingly good practices could have poor security culture at the ground level. This underscores the importance of regular, detailed assessments like those facilitated by our CSC system. Similarly, the framework developed by Da Veiga & Eloff (2010) highlights the need for cultivating a security-aware culture, which our system supports by providing actionable insights based on a comprehensive set of criteria. In conclusion, the CSC assessment system stands out as a valuable tool for organizations aiming to enhance their CSC. By providing detailed evaluations and actionable recommendations, the system aids in fostering a culture of vigilance and compliance, ultimately leading to strengthened security practices and reduced vulnerability to cyber threats.

**Limitation and Future Works**

Despite the promising development and initial validation of the Cyber Security Culture (CSC) assessment system, several limitations must be acknowledged. One significant limitation is the presentation of results. Although the current format provides a detailed account of the CSC assessment, it may not effectively convey critical insights to management for quick identification of areas needing improvement. Future iterations should focus on employing more visual representations, such as spider-web diagrams, to enhance readability and allow management to more easily discern which criteria require further attention. Additionally, the study's scope was limited to a controlled environment, and the system's effectiveness across diverse organizational settings with varying levels of cybersecurity maturity has not been thoroughly tested. The reliance on self-reported data may introduce social desirability bias, which can affect the accuracy of the results.

Future work should aim to implement the system in a broader range of organizations to evaluate its generalizability and efficacy in different contexts. Incorporating more objective measures, such as direct observations or system logs, in future studies could validate the self-reported data. Additionally, while the current system addresses the seven dimensions identified by Nasir et al. (2019), future enhancements should consider integrating additional dimensions or emerging threats to provide a more comprehensive assessment of an organization's cybersecurity culture. Another key area for improvement lies in enhancing data visualization.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012

While the current system uses graph-based outputs, future iterations could explore the inclusion of more sophisticated visual tools, such as spider-web diagrams (radar charts), to further enhance the interpretability of results. Continuous adaptation and refinement of the system in response to the evolving cyber threat landscape will be crucial for maintaining its relevance and effectiveness in fostering a robust cybersecurity culture within organizations.

## Conclusion

The development of the CSCA system marks a significant advancement in assessing and enhancing organizational cybersecurity practices. By adopting the seven dimensions identified in Nasir et al. (2019), the study ensures a robust framework for evaluating CSC. The web-based platform, designed with HTML for the user interface, PHP for backend processing, and MySQL for data storage and retrieval, offers an accessible and user-friendly tool for organizations. Results show the system effectively identifies strengths and areas for improvement in cyber security culture. Comparing our findings with existing literature highlights the unique contributions and advantages of our system. Despite limitations in result presentation and validation scope, future enhancements could include more intuitive formats like spider-web diagrams and broader validation across diverse contexts. This study provides a validated, user-friendly tool for assessing and improving CSC, fostering vigilance and resilience to defend against cyber threats.

## Acknowledgement

This project is wholly funded by the UC TATI Short Term Grant (STG) 9001-2405, which helps to make the research practical and efficient.

## References

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers and Security*, https://doi.org/10.1016/j.cose.2009.12.005

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*(August 2015) 567–575. https://doi.org/10.1016/j.chb.2015.03.054

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers and Security*, *39*(PART B) 396–405. https://doi.org/10.1016/j.cose.2013.09.004

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, *29*(2) 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Dugo, T. M. (2007). *The Insider Threat to Organisational Information Security: A Structural Model and Empirical Test*. Auburn University.

Greig, A., Renaud, K., & Flowerday, S. (2015). *An Ethnographic Study to Assess the Enactment of Information Security Culture in a Retail Store*. 61–66.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/25148625

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 185-196
DOI: 10.35631/JISTM.1039012
Karlsson, F., & Hedström, K. (2014). *End User Development and Information Security Culture* (pp. 246–257). Springer International Publishing. https://doi.org/10.1007/978-3-319-07620-1_22

Nævestad, T. O., Frislid Meyer, S., & Hovland Honerud, J. (2018). Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security. *Safety and Reliability - Safe Societies in a Changing World - Proceedings of the 28th International European Safety and Reliability Conference, ESREL 2018*, 3021–3030. https://doi.org/10.1201/9781351174664-379

Nasir, A., Abdullah Arshah, R., & Ab Hamid, M. R. (2019). A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions. *Information Security Journal*, *28*(3), 55–80. https://doi.org/10.1080/19393555.2019.1643956

Niekerk, J. Van, & Solms, R. Von. (2006). Understanding Information Security Culture: A Conceptual Framework. *Proceedings of ISSA 2006*, 1–10.

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, *59*, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). *Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017*. https://doi.org/10.1109/INCISCOS.2017.20

Schein, E. H. (1992). Organizational culture and leadership. In *SF JosseyBass Senge P* (Vol. 7, Issue 2).

Schlienger, T., & Teufel, S. (2005). Tool supported management of information security culture. *IFIP Advances in Information and Communication Technology*, 65–77.

Schlienger, Thomas, & Teufel, S. (2003). Information security culture: from analysis to change. *South African Computer Journal*, *31*, 46–52.

Shkarlet, S., Lytvynov, V., Dorosh, M., Trunova, E., & Voitsekhovska, M. (2020). The model of information security culture level estimation of organization. *Advances in Intelligent Systems and Computing*. https://doi.org/10.1007/978-3-030-25741-5_25

Siponen, M., & Vance, A. (2010). Neutralizaiton: New Insights into the Problem of Employee Information Systems Security. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/Article

Tolah, A., Furnell, S. M, & Papadaki, M. (2017). A Comprehensive Framework for Cultivating and Assessing Information Security Culture. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, *Haisa*, 52–64.