Expert Evaluation of a User Behavior Micro-Segmentation Framework for Work-From-Home Environments

Atuhe Aarone Mike[1]*, Akampurira Paul[2], Dr. Richard Ntwari[3], Dr, Wilison Tumuhimbise[3]

[1,3]Department of Computer Science, Mbarara University of Science and Technology, Uganda

[2]Department of Computing, Kampala International University, Uganda

[*]Corresponding Author

DOI: https://doi.org/10.51584/IJRIAS.2026.110400010

Received: 04 April 2026; Accepted: 10 April 2026; Published: 25 April 2026

ABSTRACT

The rapid shift to WFH practices in higher education has increased cyber security risks influenced by user behavior, usability challenges, and contextual constraints. Although several cyber security frameworks have been proposed to address these risks, many lack empirical validation in real academic environments. This study evaluated a behavior-centered cyber security framework designed for university WFH contexts using expert review to assess its feasibility, relevance, and contextual suitability. A mixed-methods expert-based evaluation was conducted, combining structured quantitative ratings with qualitative feedback from cyber security and higher education ICT professionals. Quantitative data were analysed using descriptive statistics and non-parametric tests, while qualitative responses were examined using thematic analysis. The results showed that experts rated the framework as highly relevant and deployable for academic WFH environments, particularly in terms of risky behavior identification and contextual adaptability. Lower ratings were associated with implementation effort, reflecting practical organisational considerations rather than conceptual weaknesses. The study provides empirical evidence supporting the feasibility and applicability of behavior-centered cyber security frameworks in remote academic work environments and demonstrates the value of expert-based mixed-methods evaluation for validating socio-technical security frameworks prior to deployment.

Keywords: Cyber Security Framework; Expert Evaluation; Work from Home Security; Higher Education; Usability and Behavior; Socio-Technical Systems

INTRODUCTION

Cyber security in higher education increasingly depends on work-from-home (WFH) infrastructures that extend beyond institutional boundaries into personal and home-based environments (NIST, 2018; ISO/IEC, 2022; ENISA, 2023**).** In such settings, security risks are shaped not only by technical vulnerabilities but also by user behavior, usability challenges, and contextual constraints. Recent studies show that fatigue, system complexity, and environmental pressures significantly influence security behavior in remote academic work, highlighting the limitations of purely technical cyber security approaches and increasing interest in socio-technical and behavior-aware frameworks (Di Nocera et al., 2023)

Cyber security frameworks are commonly proposed as structured approaches for guiding security implementation and decision-making in organizations. While many frameworks emphasise controls, architectures, and policies, recent evidence suggests that frameworks that fail to align with user behavior and real working conditions often face resistance or ineffective adoption, particularly in higher education environments operating under remote or hybrid models (ENISA, 2023; Sasse et al., 2001).

Recent reviews indicate that many cyber security frameworks continue to be evaluated primarily at a conceptual level or through limited technical demonstrations, with relatively few studies reporting systematic empirical

validation involving practitioners (Kotulic & Clark, 2004; Sasse et al., 2001). As a result, uncertainty remains regarding whether proposed frameworks are feasible, relevant, and deployable in real-world academic WFH contexts**.**

Expert evaluation has emerged as a credible and practical method for validating complex cyber security frameworks when full-scale implementation is not immediately feasible. Contemporary studies demonstrate that expert review enables informed assessment of feasibility, relevance, and contextual suitability based on professional experience, particularly when supported by structured instruments and mixed analytical approaches (Grand-Guillaume-Perrenoud et al., 2023; Sasse et al., 2001)**.** Such evaluations provide evidence of framework quality that goes beyond theoretical justification alone.

The framework evaluated in this study was designed to address cyber security challenges in WFH university environments by integrating behavioral risk identification, contextual awareness, and usability considerations. Given its socio-technical nature, expert-based evaluation was considered an appropriate and rigorous method for assessing the framework's practical value prior to large-scale deployment (Fallatah, 2026)**.**

Accordingly, this study addressed the following research objective was to evaluate the proposed framework through expert review in order to assess its feasibility, relevance, and contextual suitability. This study contributes to applied cyber security research and practice by providing empirical evidence on the feasibility and contextual suitability of a behavior-centered cyber security framework for academic work-from-home environments. Unlike many prior frameworks that are evaluated primarily at a conceptual level, this work employs structured expert review and mixed-methods analysis to assess practical deployability, implementation effort, and real-world relevance. The findings offer actionable insight for higher education institutions seeking to strengthen cyber security under remote or hybrid work models, particularly in resource-constrained settings.

METHODOLOGY

Expert-based evaluation was selected because the proposed cyber security framework required validation of feasibility, relevance, and contextual suitability prior to large-scale deployment in academic work-from-home environments. The framework evaluated in this study was originally derived from empirical behavioral modeling and statistical validation conducted within university WFH contexts; the present study therefore represents a practitioner-based feasibility validation phase rather than initial conceptual development.

This study adopted an expert-based evaluation design to assess the proposed cyber security framework. Expert review was selected because the framework had already been developed and required validation in terms of feasibility, relevance, and contextual suitability before broader implementation. Recent methodological literature supports expert evaluation as an effective approach for assessing complex socio-technical frameworks where experiential knowledge is critical **(**Monica et al., 2023**)**.

A mixed-methods approach was employed to strengthen the evaluation by combining structured quantitative assessment with qualitative explanatory insight. Quantitative data provided systematic ratings of framework components, while qualitative responses captured expert reasoning, contextual judgement, and practical concerns. This integration enabled both measurement and interpretation of expert evaluations, supporting a more comprehensive understanding of the framework's practical value.

The evaluation was guided by a contemporary socio-technical perspective, that cyber security effectiveness depends on interactions between technology, human behavior, and organisational context. From this perspective, a framework cannot be considered effective solely on technical grounds; it must also be usable, realistic, and adaptable to the environment in which it is applied. This view informed the selection of evaluation criteria, which focused on feasibility, relevance, deployability, implementation effort, and contextual suitability.

The evaluation involved a panel of experts with professional experience in cyber security, higher education ICT systems, and remote or distributed work environments. Experts were selected based on their practical exposure to information security challenges and familiarity with academic organisational contexts, ensuring that the

evaluation reflected informed professional judgment rather than general opinion. The diversity of expertise allowed the framework to be assessed from technical, organisational, and behavioral perspectives. Experts were purposively selected using defined inclusion criteria to ensure contextual and professional relevance. Participants were required to have (1) a minimum of five years of professional experience in cyber security, ICT governance, or higher education information systems; (2) direct involvement in policy implementation, cyber security operations, or institutional ICT management; and (3) familiarity with work-from-home (WFH) security challenges in academic environments. The panel included practitioners from both public and private university contexts within Uganda, representing diverse institutional capacities and governance structures. This purposive selection ensured that expert evaluation reflected varied organisational realities rather than a single institutional perspective.

Experts were provided with an overview of the proposed framework and its core components and were asked to evaluate specific aspects using a structured evaluation instrument. The instrument included rating scales for quantitative assessment and open-ended questions for qualitative feedback. Experts completed the evaluation independently to reduce group influence and bias. The collected responses reflected expert perceptions of how feasible, relevant, and contextually appropriate the framework would be if implemented in real university WFH environments.

We analysed the experts' scores using summary statistics to show how each part of the framework was rated. Because the ratings were recorded on an ordered scale (for example, low to high), we used statistical tests that are suitable for this type of data rather than tests designed for normally distributed measurements. The Friedman test was used to check whether experts rated some areas of the framework higher or lower than others overall, and follow-up comparisons were used to identify exactly which areas differed. We also used the Mann–Whitney U test to examine whether expert ratings differed between groups with different backgrounds, such as those with prior experience working in WFH environments.

Qualitative data from open-ended responses were analysed using reflexive thematic analysis, following updated methodological guidance that emphasises transparency, analytical rigor, and contextual interpretation. Expert comments were coded to identify recurring themes related to perceived strengths, limitations, and contextual considerations. The resulting themes were then used to explain and triangulate the quantitative findings, thereby strengthening the credibility and interpretive depth of the evaluation (Creswell & Plano Clark, 2018).

FINDINGS AND DISCUSSION

Description of Expert Evaluation Results

The expert evaluation generated quantitative ratings and qualitative feedback across multiple dimensions of the proposed framework. The analysis focused on how experts perceived the framework's feasibility, relevance, and contextual suitability for remote academic work environments.

Expert Profile and Credibility

The credibility of the evaluation depended on the professional background of the participating experts. Most experts reported direct experience with cyber security challenges in work-from-home environments, indicating that their assessments were informed by practical exposure rather than theoretical knowledge alone.

Table 1. Expert Profile: Work-From-Home Cyber security Experience

WFH Cyber security Experience	Frequency	Percent	Valid Percent	Cumulative Percent
No	2	12.5	12.5	12.5
Yes	14	87.5	87.5	100.0
Total	16	100.0	100.0	

The results showed that 87.5% of the experts had experience with cyber security in work-from-home environments. Although the expert panel consisted of sixteen participants, this size aligns with methodological recommendations for structured expert evaluation of complex socio-technical frameworks, where depth of expertise is prioritised over numerical representativeness. This strengthened the validity of the evaluation, as most participants were familiar with the behavioral and organisational challenges associated with remote academic work.

Descriptive Evaluation of Framework Dimensions

Experts were asked to rate key dimensions of the framework using structured rating scales. Descriptive statistics were used to summarise overall expert perceptions across these dimensions.

Table 2. Descriptive Statistics of Framework Evaluation Dimensions

Framework Dimension	N	Min	Max	Mean	Std. Dev.
Risky Behavior Identification Effectiveness	16	9	18	15.50	2.251
Micro-Segmentation Effectiveness	16	6	18	14.94	2.670
Intervention Recommendation Effectiveness	16	4	15	11.62	2.446
Effort Reduction Index	16	3	15	11.31	2.750
Expert Confidence & Bias Control Index	16	5	25	19.44	4.633
Deployability & Feasibility of the Framework	16	7	29	23.56	4.993

The results showed that experts rated deployability and feasibility, expert confidence and bias control, and risky behavior identification most highly. These findings suggested that the framework was perceived as well aligned with real-world academic work from home conditions, particularly in its ability to identify behavioral risks and support informed decision-making.

Lower mean scores were observed for intervention recommendation effectiveness and effort reduction. While these scores were still positive, they indicated that experts anticipated greater challenges in operational execution and resource requirements. Importantly, the variation across mean values demonstrated that experts did not provide uniform ratings, but instead distinguished between different aspects of the framework.

Statistical Analysis and Interpretation

To determine whether experts meaningfully differentiated between framework dimensions, non-parametric statistical tests (Pallant,2023) were applied. A Friedman test was conducted to examine differences in expert ratings across the evaluated dimensions. The results are presented in Table 3.

Table 3. Friedman Test Results across Framework Dimensions

Statistic	**Value**
Total N	16
χ^2 (Chi-Square)	84.514
Degrees of Freedom	6
Asymptotic Significance (p-value)	.000

The Friedman test indicated statistically significant differences across framework dimensions ($p < .001$). In addition to testing for statistical significance, we also examined the strength of the differences between framework dimensions. Effect sizes were calculated using the formula $r = Z / \sqrt{N}$, where Z represents the standardised test statistic and N is the total number of expert ratings. This helped us determine not only whether differences existed, but how meaningful they were in practice. The results showed clear and practically important differences between deployability-related aspects and effort-related aspects of the framework, indicating that

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

experts made substantial distinctions rather than minor rating variations. This result confirmed that experts evaluated the framework components differently rather than assigning similar ratings across all dimensions. Such differentiation reflected informed judgment and reduced the likelihood of response bias or superficial agreement.

Post-Hoc Pairwise Comparisons

To identify where specific differences occurred, post-hoc pairwise comparisons were conducted. The results are shown in Table 4.

Table 4. Pairwise Comparisons of Framework Dimensions

Comparison	Standardised Test Statistic	Adjusted p-value
Effort Reduction vs Risky Behavior Identification	3.928	.002
Effort Reduction vs Micro-Segmentation	3.478	.011
Effort Reduction vs Expert Confidence & Bias Control	−5.442	.000
Effort Reduction vs Deployability & Feasibility	−6.874	.000
Intervention Effectiveness vs Risky Behavior Identification	3.273	.022
Expected Effectiveness vs Deployability & Feasibility	6.056	.000

The results showed that effort reduction was rated significantly lower than analytical and deployability-related dimensions. This pattern indicated that experts viewed the framework's analytical capabilities as strong, while expressing realistic caution regarding the effort required for implementation. These differences did not suggest conceptual weakness, but rather reflected practical concerns about organizational capacity and resource availability.

Influence of Expert Experience

To examine whether expert background influenced evaluation outcomes, Mann–Whitney U tests were conducted based on work-from-home cyber security experience. The results are presented in Table 5.

Table 5. Mann–Whitney U Test Results by WFH Experience

Framework Dimension	p-value	Decision
Risky Behavior Identification Effectiveness	.033	Significant
Expert Confidence & Bias Control Index	.033	Significant
Micro-Segmentation Effectiveness	.500	Not significant
Intervention Recommendation Effectiveness	.333	Not significant
Effort Reduction Index	.150	Not significant
Deployability & Feasibility	.200	Not significant
Expected Overall Effectiveness & Impact	.067	Not significant

The results showed that experts with work-from-home cyber security experience rated risky behavior identification and bias control significantly higher than those without such experience. This finding suggested that direct exposure to work from home security challenges enhanced appreciation of the framework's behavioral focus.

Qualitative Insights and Triangulation

Qualitative feedback from experts provided explanatory depth for the quantitative findings. Several experts emphasised that behavioral risk identification was critical in remote academic environments, where institutional

controls were weaker and user actions played a central role in security incidents. This insight aligned with the high quantitative ratings for risky behavior identification and micro-segmentation.

Experts also highlighted the framework's contextual adaptability as a strength, noting that it could be adjusted to different institutional capacities and policy environments. These comments supported the high ratings for deployability and feasibility.

Concerns raised in qualitative feedback primarily related to implementation effort and organisational readiness, particularly in institutions with limited technical staff or budget constraints. These comments explained why effort-related dimensions received comparatively lower quantitative scores. Rather than indicating rejection, the qualitative data showed that experts viewed these challenges as manageable but requiring institutional commitment.

The integration of quantitative and qualitative findings demonstrated strong triangulation. Numerical ratings identified strengths and constraints, while expert narratives explained the reasons behind these perceptions. Together, the findings provided a balanced and credible evaluation of the framework's feasibility, relevance, and contextual suitability.

CONCLUSION AND RECOMMENDATIONS

Summary of Key Findings

This study evaluated a behavior-centered cyber security framework through expert review to assess its feasibility, relevance, and contextual suitability for remote academic work environments. The findings showed that experts consistently perceived the framework as relevant and practically deployable, particularly in its ability to identify risky user behavior and adapt to contextual conditions. Statistical analysis confirmed that experts meaningfully differentiated between framework components, indicating informed and experience-based evaluation rather than superficial agreement.

The results further demonstrated that analytical and decision-support components were viewed more favorably than effort-related aspects. This pattern reflected realistic practitioner concerns about implementation demands rather than fundamental weaknesses in the framework design.

Achievement of Research Objective

The research objective of evaluating the proposed framework through expert review was fully achieved. The expert assessment provided empirical evidence that the framework was feasible, relevant, and contextually suitable for higher education work from home settings. Both quantitative and qualitative findings converged to support this conclusion, with strong agreement across experts regardless of background for core feasibility and relevance dimensions.

Where differences in expert opinion were observed, these differences were logically associated with experience in work from home cyber security, further reinforcing the credibility of the evaluation.

Implications for Practice and Policy

The findings suggested that the evaluated framework has practical value for academic institutions seeking to strengthen cyber security in remote and hybrid work environments. The strong emphasis on behavioral risk identification and contextual awareness aligned with the realities of distributed academic work, where user actions and environmental variability significantly influence security outcomes.

From a policy perspective, the results indicated that successful adoption would require institutional commitment, particularly in terms of resource allocation, staff capacity building, and integration with existing security processes. The lower ratings associated with effort reduction highlighted the need for phased or incremental deployment strategies rather than immediate full-scale implementation.

Contributions to Research

This study contributed to cyber security research by providing empirical validation of a socio-technical framework using structured expert review. Unlike many prior studies that relied on conceptual justification alone, this work demonstrated how expert-based, mixed-methods evaluation can be used to assess the practical readiness of cyber security frameworks.

The integration of non-parametric statistical analysis with qualitative expert insights provided a balanced and transparent evaluation approach. This methodological contribution may be applied in future studies seeking to validate complex frameworks prior to deployment.

Limitations and Future Work

Although the expert evaluation provided structured and statistically validated evidence of feasibility and contextual suitability, the framework has not yet undergone longitudinal pilot implementation within a live university WFH environment. Given the expert-based design, the findings support analytical generalisation to comparable higher education WFH contexts rather than statistical generalisation to all institutions.

The current validation phase focused on practitioner-informed feasibility assessment prior to institutional deployment. Importantly, experts rated deployability and feasibility highly, indicating perceived operational readiness. Future research will involve phased pilot implementation within selected academic institutions to measure behavioral change, compliance improvement, and sustainability outcomes over time. While expert judgment is appropriate at this stage of validation, subsequent research should focus on longitudinal assessment of implementation outcomes in diverse institutional contexts.

Further research may also examine longitudinal outcomes to assess how the framework performs over time and how institutional maturity influences implementation effort. Future validation studies may also expand the expert panel to include cross-institutional and international cyber security professionals in order to enhance contextual diversity and strengthen external transferability. These extensions would complement the present findings and support broader generalization.

REFERENCES

1. Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health, 11(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806
2. Braun, V., & Clarke, V. (2021). One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology, 18(3), 328–352. https://doi.org/10.1080/14780887.2020.1769238
3. Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.
4. Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable security: A systematic literature review. Information, 14(12), 641. https://doi.org/10.3390/info14120641
5. European Union Agency for Cyber security . (2023). Cyber security culture guidelines: Behavioral aspects of cyber security . ENISA. https://www.enisa.europa.eu/publications/cyber security -culture-guidelines-behavioral-aspects-of-cyber security
6. Field, A. (2018). Discovering statistics using IBM SPSS statistics (5th ed.). SAGE Publications.
7. Grand-Guillaume-Perrenoud, J. A., Ortoleva Bucher, C., Baroffio, A., & Nendaz, M. (2023). Mixed methods instrument validation: Evaluation procedures for practitioners developed from the validation of the Swiss Instrument for Evaluating Interprofessional Collaboration. Frontiers in Psychology. https://pmc.ncbi.nlm.nih.gov/articles/PMC9875772/
8. International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cyber security and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). ISO. https://www.iso.org/standard/27001

9. Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5), 597–607. https://doi.org/10.1016/j.im.2003.08.001
10. National Institute of Standards and Technology. (2018, April 16). Framework for improving critical infrastructure cyber security (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
11. Pallant, J. (2020). SPSS survival manual: A step by step guide to data analysis using IBM SPSS (7th ed.). McGraw-Hill Education.
12. Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link" — A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131. https://doi.org/10.1023/A:1011902718709