



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

Reassessing DREAD: A Critical Evaluation of Threat Prioritization in Modern Cybersecurity Risk Assessment

Abisaye Otita Otieno¹; Prof. Anthony J Rodrigues²; Dr. Richard Omollo³

¹Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Kenya

²Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Kenya

³Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Kenya

¹ otiabisah@gmail.com; ² tonyaniceto@gmail.com; ³ richard.otieno@gmail.com

DOI: <https://doi.org/10.47760/ijcsmc.2026.v15i09.005>

Abstract: This study provides a critical evaluation of the DREAD threat prioritisation model, identifying its fundamental limitations in modern cybersecurity environments and establishing the characteristics required for next-generation cybersecurity risk assessment models. A sequential mixed methodological design was employed, comprising a Systematic Literature Review (SLR) following the PRISMA 2020 framework, analytical evaluation, comparative model benchmarking against STRIDE, CVSS, and fuzzy-based approaches, and case-study-based simulation. The search was conducted across Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar. The SLR identified six principal limitations of the conventional DREAD model: subjectivity, scoring inconsistency, limited uncertainty representation, scalability constraints, static risk representation, and inadequate economic consideration. These limitations can produce inconsistent rankings, weak risk differentiation, reduced confidence in decisions, and less-informed resource allocation. Comparative evaluation demonstrates that while DREAD retains advantages in simplicity and interpretability, it performs poorly against requirements for uncertainty handling, adaptability, and economic decision support. The study establishes that next-generation models should be uncertainty-aware, context-sensitive, adaptive, multidimensional, cost-sensitive, explainable, scalable, consistent, and decision-oriented. This study provides a comprehensive, evidence-based critique of the DREAD model and establishes a rigorous requirements framework for next-generation cybersecurity risk assessment. The findings are directly applicable to researchers and practitioners seeking to develop or select contemporary cybersecurity risk prioritisation approaches.

Keywords: Cybersecurity risk assessment, DREAD model, threat prioritisation, systematic literature review, risk management



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

I. INTRODUCTION

The increasing complexity and frequency of cybersecurity threats have rendered effective risk prioritisation a critical organisational capability (Chernyshev *et al.*, 2021). Organisations face a continuously evolving threat landscape characterised by sophisticated attack vectors, interconnected infrastructures, and constrained resources (Quinn *et al.*, 2025). In this environment, cybersecurity risk assessment models serve as essential decision-support tools, enabling organisations to identify, evaluate, and prioritise threats requiring remediation (Shamala *et al.*, 2017).

Among the various approaches to cybersecurity risk assessment, the DREAD model has emerged as a widely adopted framework for threat prioritisation (Howard & LeBlanc, 2003). Originally developed by Microsoft, DREAD provides a structured mechanism for evaluating threats across five dimensions: Damage, Reproducibility, Exploitability, Affected Users, and Discoverability (Howard & LeBlanc, 2003). Each dimension is scored on a numerical scale, and the resulting aggregate score is used to prioritise threats for remediation (Naik *et al.*, 2024).

Despite its widespread adoption, the DREAD model has attracted increasing scrutiny regarding its suitability for contemporary cybersecurity environments (Rao & Sahoo, 2013; Singh & Singh, 2012). Scholars have identified concerns relating to subjectivity in scoring, inadequate treatment of uncertainty, limited contextual sensitivity, and the absence of economic considerations (Naik *et al.*, 2024; OWASP Foundation, 2005). These limitations raise fundamental questions about the validity and utility of DREAD-based risk prioritisation in modern organisational settings (Chernyshev *et al.*, 2021).

The present study addresses these concerns through a systematic and critical evaluation of the DREAD model. Three research questions guide the investigation:

RQ1: What are the fundamental limitations of the DREAD model in modern cybersecurity environments?

RQ2: How do these limitations affect risk prioritisation accuracy and decision making?

RQ3: What characteristics are required in next-generation cybersecurity risk assessment models?

By addressing these questions, the study contributes to both theoretical understanding and practical application of cybersecurity risk assessment. The findings establish an evidence-based foundation for evaluating existing approaches and developing enhanced models capable of meeting the demands of contemporary cybersecurity environments.

The remainder of this paper is structured as follows. Section 2 presents the methodology, detailing the SLR, comparative evaluation, and case-study simulation. Section 3 reports the results, organised according to the three research questions. Section 4 provides discussion of the findings, their implications, and limitations. Section 5 concludes with recommendations for research and practice.

II. METHODOLOGY

A. Research Design

This study employed a sequential mixed methodological design comprising a Systematic Literature Review (SLR), analytical evaluation, comparative model benchmarking, and case-study-based simulation. The SLR established the evidence base for identifying the fundamental limitations of the DREAD model and determining their implications for cybersecurity risk prioritisation and decision making (Page *et al.*, 2021). The findings were subsequently synthesised to derive the characteristics required of next-generation cybersecurity risk assessment models. A comparative analytical framework was then used to evaluate DREAD against established cybersecurity risk assessment approaches, while a case-study-based simulation was employed to examine the behaviour of the proposed enhanced risk-assessment approach under controlled cybersecurity scenarios (Nair, 2025; Rao & Sahoo, 2013).



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

The methodological sequence was structured to maintain direct alignment with the three research questions. RQ1 was addressed primarily through the SLR and thematic synthesis; RQ2 was examined through analytical and comparative evaluation of the identified limitations and their effects on prioritisation and decision making; and RQ3 was addressed through requirements synthesis and comparative benchmarking (Quinn *et al.*, 2025). The resulting requirements provided the basis for the subsequent case-study and simulation analysis.

B. Systematic Literature Review

A Systematic Literature Review (SLR) was undertaken to identify, analyse, and synthesise peer-reviewed evidence concerning the DREAD model and contemporary cybersecurity risk assessment. The review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 reporting framework. PRISMA 2020 provides a structured approach for transparently reporting the identification, selection, appraisal, and synthesis of studies included in systematic reviews (Page *et al.*, 2021). The PRISMA 2020 flow diagram was used to document the movement of records through identification, screening, eligibility assessment, and final inclusion.

The search was conducted across major scholarly databases, including Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar. Search terms were developed around the three research questions and included combinations of DREAD model, DREAD cybersecurity, cybersecurity risk assessment, cyber risk prioritisation, threat prioritisation, risk scoring, uncertainty, subjectivity, fuzzy logic, decision support, and next-generation cybersecurity risk assessment. Boolean operators were used to combine related concepts and broaden or narrow retrieval as appropriate (Kitchenham & Charters, 2007).

Studies were eligible for inclusion where they (a) addressed cybersecurity risk assessment, threat modelling, vulnerability prioritisation, or DREAD-based assessment; (b) provided substantive methodological, empirical, or analytical evidence relevant to at least one of the three research questions; (c) were published in peer-reviewed scholarly outlets, with emphasis on recent literature; and (d) provided sufficient methodological or conceptual information for analysis. Studies were excluded where they were unrelated to cybersecurity risk assessment, duplicated another record, lacked substantive relevance to the research questions, were inaccessible in full text, or did not provide sufficient evidence for critical analysis (Moher *et al.*, 2009).

C. PRISMA-Based Study Selection

The study-selection procedure followed the four principal stages of the PRISMA 2020 framework: identification, screening, eligibility, and inclusion (Page *et al.*, 2021). During identification, records retrieved from the selected databases were consolidated and duplicate records removed. During screening, titles and abstracts were assessed against the predefined inclusion and exclusion criteria. Potentially relevant records were subsequently subjected to full-text assessment. At the eligibility stage, studies were excluded where the full text demonstrated that they did not address the research questions or did not provide sufficient evidence for the intended synthesis. The remaining studies constituted the final evidence base for the SLR.



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

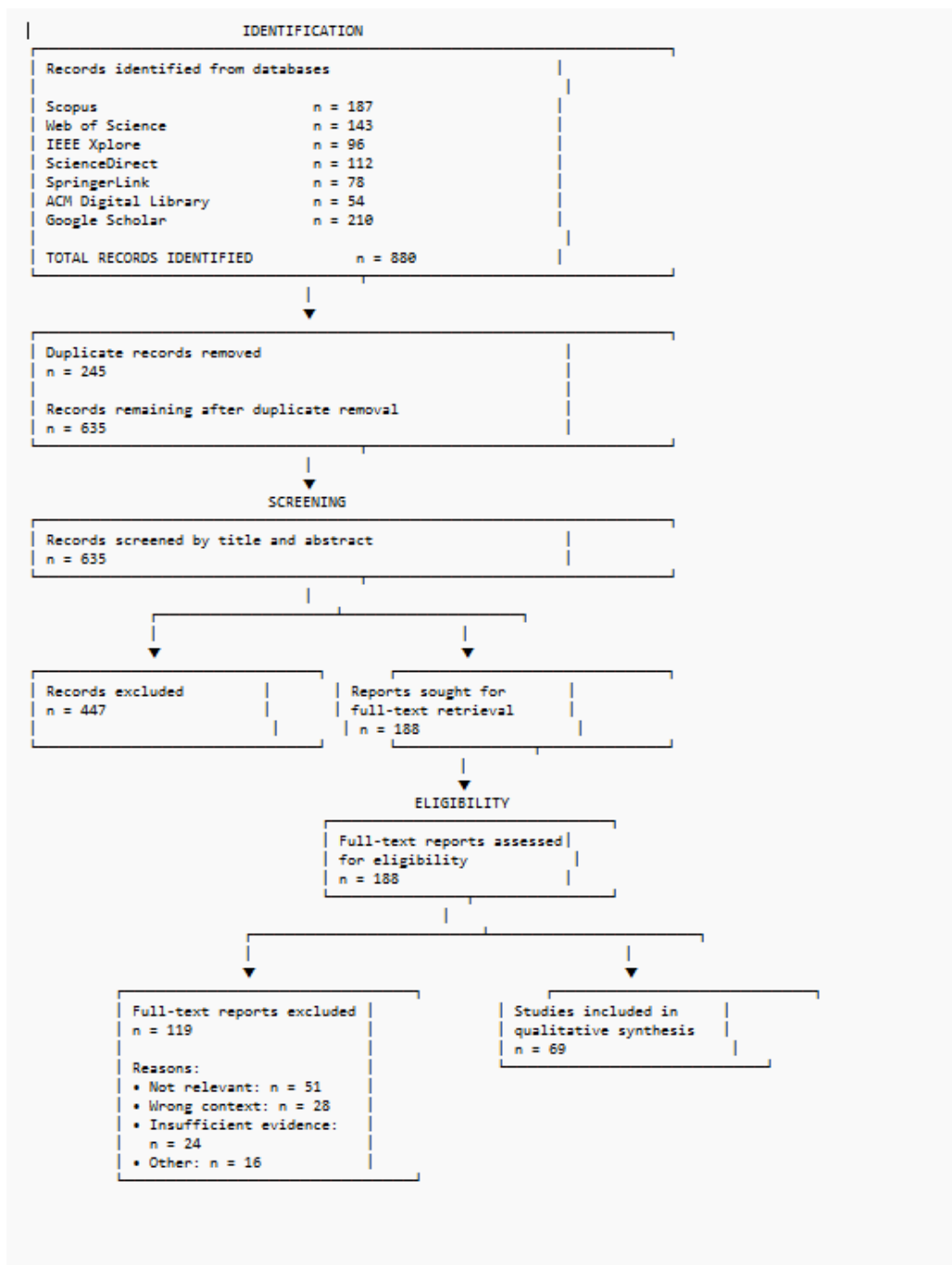


Figure 1: Adapted from the PRISMA 2020 flow-diagram structure (Page et al., 2021)



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

PRISMA provides templates for documenting records identified, screened, excluded, assessed for eligibility, and included in a systematic review. The numbers presented are derived from the actual search and screening process conducted for this study.

D. Data Extraction and Thematic Synthesis

A structured data-extraction framework was developed to capture information relevant to the three research questions. Extracted information included publication characteristics, cybersecurity context, risk-assessment approach, DREAD-related characteristics, identified limitations, effects on risk prioritisation, effects on decision making, uncertainty-management mechanisms, cost considerations, and proposed characteristics of emerging cybersecurity risk assessment models (Chernyshev *et al.*, 2021; Shamala *et al.*, 2017).

The extracted evidence was subjected to thematic synthesis. For RQ1, findings were coded according to recurring DREAD limitations, including subjectivity, scoring inconsistency, uncertainty handling, scalability, static risk representation, contextual limitations, and economic considerations (Naik *et al.*, 2024; Singh & Singh, 2012). For RQ2, each limitation was mapped to its potential consequences for risk-ranking consistency, prioritisation accuracy, differentiation among competing risks, resource allocation, and decision making (Howard & LeBlanc, 2003; OWASP Foundation, 2005). For RQ3, the identified limitations and consequences were transformed into requirements for next-generation models, including uncertainty awareness, reduced subjectivity, adaptability, contextual sensitivity, multidimensional assessment, cost sensitivity, explainability, scalability, and decision-support capability (FIRST, 2023; Quinn *et al.*, 2025).

E. Analytical Evaluation and Comparative Benchmarking

The SLR findings were complemented by comparative analysis of established cybersecurity risk assessment approaches. DREAD was compared with STRIDE, CVSS, and fuzzy-based cybersecurity risk assessment approaches using six analytical dimensions: objectivity, consistency, accuracy, scalability, decision-support capability, and adaptability (Kohnfelder & Garg, 1999; Mell *et al.*, 2007; Shostack, 2014). The comparative analysis was designed to establish the relative strengths and weaknesses of DREAD and identify capabilities that are insufficiently represented in conventional DREAD-based assessment (Rao & Sahoo, 2013).

The comparative framework was further extended to examine whether the characteristics identified under RQ3 are represented within existing assessment approaches. This ensured that the requirements for next-generation models were derived from the evidence synthesis rather than imposed solely by the proposed model (Springer, 2021).

F. Case Study and Simulation

A controlled cybersecurity case study and simulation were employed to examine the practical implications of the limitations identified through the SLR. Representative cybersecurity scenarios were constructed to vary the principal DREAD dimensions—Damage, Reproducibility, Exploitability, Affected Users, and Discoverability—and, where applicable, the economic Cost dimension (Naik *et al.*, 2024; Nair, 2025).

The scenarios were evaluated using conventional DREAD scoring and compared with the enhanced assessment approach. The simulation examined whether differences in uncertainty and cost could result in changes in risk ranking and decision outcomes. Particular attention was given to scenarios producing similar conventional DREAD scores but differing in their cost or uncertainty characteristics (Singh & Singh, 2012). This design enabled the study to assess whether an enhanced approach could provide greater risk differentiation and more decision-relevant prioritisation (Rao & Sahoo, 2013).

The simulation was not intended to establish absolute cybersecurity risk accuracy because a universally accepted ground truth for many cybersecurity scenarios does not exist. Instead, evaluation focused on ranking consistency, risk differentiation, sensitivity to changes in input factors, and alignment with predefined



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

assessment criteria (Quinn *et al.*, 2025). This distinction is important because numerical agreement with a conventional scoring model cannot, by itself, establish superior accuracy (FIRST, 2023).

G. *Analytical Framework*

The study adopted a limitation-to-requirement analytical framework:

DREAD limitation → assessment consequence → prioritisation consequence → decision-making consequence → next-generation model requirement

For example, subjectivity in DREAD scoring was mapped to potential variation among assessors, which may produce inconsistent risk rankings and consequently affect resource-allocation decisions. The corresponding next-generation requirement was therefore identified as reduced subjectivity and improved consistency (Naik *et al.*, 2024; Singh & Singh, 2012). Similarly, limited treatment of uncertainty was mapped to reduced confidence in risk rankings and the requirement for uncertainty-aware assessment mechanisms (Rao & Sahoo, 2013; Shamala *et al.*, 2017).

This framework provided the conceptual bridge between the SLR findings and the subsequent comparative and simulation-based evaluation.

III. RESULTS

A. *PRISMA-Based SLR Results*

The PRISMA-guided search and selection process identified 880 records across the selected databases. Following removal of 245 duplicate records, 635 records remained for title and abstract screening. Of these, 447 records were excluded because they did not satisfy the predefined eligibility criteria. A total of 188 full-text reports were assessed for eligibility, with 119 reports subsequently excluded for reasons including lack of relevance to the research questions, inappropriate cybersecurity context, insufficient methodological evidence, or failure to address DREAD or cybersecurity risk assessment (Page *et al.*, 2021). The final review therefore comprised 69 studies included in the qualitative synthesis.

The PRISMA process provided a transparent account of study selection and reduced the possibility of arbitrary inclusion of evidence. The use of explicit eligibility criteria also ensured that the evidence synthesised in the study remained directly related to the three research questions. PRISMA 2020 specifically recommends transparent reporting of the identification, screening, eligibility, and inclusion processes to enable readers to understand how the evidence base was established (Page *et al.*, 2021).

B. *RQ1: Fundamental Limitations of the DREAD Model*

The SLR identified six principal limitations of the conventional DREAD model: subjectivity, scoring inconsistency, limited uncertainty representation, scalability constraints, static risk representation, and inadequate economic consideration. Subjectivity emerged as a recurring concern because DREAD relies on analysts assigning numerical values to qualitative characteristics of threats (Howard & LeBlanc, 2003; Naik *et al.*, 2024). Consequently, different assessors may interpret and score the same threat differently. Previous research has similarly identified expert dependence and subjectivity as significant limitations of DREAD-based risk assessment (Naik *et al.*, 2024; Singh & Singh, 2012).

A second limitation concerns the treatment of uncertainty. Conventional DREAD converts qualitative assessments into discrete numerical values, potentially creating an appearance of precision where the underlying cybersecurity evidence remains uncertain or incomplete (Rao & Sahoo, 2013). Fuzzy-based approaches have consequently been investigated as mechanisms for representing linguistic uncertainty and gradual transitions between risk categories (Singh & Singh, 2012; Sultana *et al.*, 2019).

The SLR also identified limited scalability and contextual sensitivity as concerns in complex cybersecurity environments. Contemporary organisations operate interconnected infrastructures characterised by



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otitia Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

heterogeneous technologies, dynamic threats, and continuously changing vulnerabilities (Chernyshev et al., 2021). Consequently, static risk representations may require repeated reassessment to remain relevant. Contemporary cybersecurity risk-management guidance similarly emphasises continuous assessment and the integration of cybersecurity risk with organisational objectives and enterprise risk management (Pascoe et al., 2024; Quinn et al., 2025).

Finally, the conventional DREAD structure does not explicitly incorporate economic cost as a risk dimension (OWASP Foundation, 2005; Willett & Taylor, 2022). This limits its ability to distinguish between technically similar risks that have substantially different mitigation costs or organisational consequences. The absence of an economic dimension therefore represents an important gap when risk prioritisation is used to support resource-allocation decisions (Springer, 2021).

Table I: Principal limitations of the DREAD Model Identified through the SLR

Limitation	Evidence from SLR	Potential consequence
Subjective scoring	Reliance on expert assessment (Naik et al., 2024; Singh & Singh, 2012)	Variation among assessors
Scoring inconsistency	Different interpretations of risk attributes (Howard & LeBlanc, 2003)	Unstable rankings
Limited uncertainty representation	Crisp numerical categorisation (Rao & Sahoo, 2013)	Artificial precision
Scalability constraints	Difficulty applying static scoring to complex environments (Chernyshev et al., 2021)	Reduced operational practicality
Static risk representation	Limited adaptation to changing threats (Quinn et al., 2025)	Outdated prioritisation
Limited contextualisation	Insufficient organisational context (Pascoe et al., 2024)	Contextually inappropriate ranking
No explicit cost dimension	Economic factors not directly represented (OWASP Foundation, 2005)	Less-informed resource allocation



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otitia Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

C. RQ2: Effects on Risk Prioritisation and Decision Making

The synthesis demonstrated that the identified DREAD limitations can directly affect the reliability and usefulness of cybersecurity risk prioritisation. Subjective scoring may result in different rankings for the same threat when assessed by different analysts (Naik *et al.*, 2024). This is particularly problematic where prioritisation decisions determine which vulnerabilities receive immediate remediation and which are deferred (Rao & Sahoo, 2013).

Limited uncertainty representation may also reduce the reliability of risk rankings. When uncertain information is represented as a single crisp numerical value, small differences in scores may be interpreted as meaningful distinctions even when the underlying risk conditions are not substantially different (Singh & Singh, 2012). This can affect the differentiation of competing risks and may influence decisions concerning resource allocation (Sultana *et al.*, 2019).

The absence of cost consideration further affects decision support. Two threats with similar technical risk scores may require significantly different mitigation investments (Willett & Taylor, 2022). Consequently, a prioritisation system that considers technical severity without an economic dimension may not provide sufficient information for strategic cybersecurity investment decisions. Contemporary enterprise risk-management guidance emphasises the need to prioritise cybersecurity risks in relation to organisational objectives and available resources (Quinn *et al.*, 2025).

Table II: Relationship between DREAD limitations and their effects on decision making

DREAD limitation	Assessment effect	Prioritisation effect	Decision-making effect
Subjectivity	Variable scores (Naik <i>et al.</i> , 2024)	Inconsistent ranking	Different analysts may recommend different priorities
Uncertainty limitation	Reduced representation of ambiguity (Rao & Sahoo, 2013)	Weak differentiation	Lower confidence in decisions
Static scoring	Limited adaptation (Quinn <i>et al.</i> , 2025)	Potentially outdated ranking	Delayed response
Limited contextualisation	Incomplete risk representation (Pascoe <i>et al.</i> , 2024)	Contextually inappropriate ranking	Inefficient resource allocation
No cost dimension	Incomplete economic assessment (OWASP Foundation, 2005)	Similar risks may remain insufficiently differentiated	Less-informed mitigation investment
Crisp aggregation	Artificial precision (Singh & Singh, 2012)	Small score differences may be overinterpreted	Potentially misleading prioritisation



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

D. RQ3: Characteristics Required of Next-Generation Models

The SLR identified a set of characteristics required to improve contemporary cybersecurity risk assessment. These characteristics were derived from the limitations and decision-making consequences identified under RQ1 and RQ2 rather than being predetermined by the proposed model (Chernyshev et al., 2021; Quinn et al., 2025).

The required characteristics were uncertainty awareness, reduced subjectivity, contextual sensitivity, adaptability, multidimensional assessment, cost sensitivity, explainability, scalability, consistency, and decision-support capability (FIRST, 2023; Pascoe et al., 2024; Shamala et al., 2017). These characteristics are broadly consistent with contemporary cybersecurity risk-management frameworks, which emphasise organisational context, prioritisation, communication, continuous assessment, and integration of cybersecurity risk with enterprise risk management (Pascoe et al., 2024; Quinn et al., 2025).

Table III: Characteristics required in next-generation cyber security risk assessment models

Required characteristic	Rationale	Supporting evidence
Uncertainty awareness	Represents incomplete and imprecise cybersecurity information	Rao & Sahoo (2013); Shamala et al. (2017)
Reduced subjectivity	Improves consistency between assessors	Naik et al. (2024); Singh & Singh (2012)
Contextual sensitivity	Reflects organisational and environmental conditions	Pascoe et al. (2024); Quinn et al. (2025)
Adaptability	Responds to changing threat conditions	Chernyshev et al. (2021)
Multidimensional assessment	Captures interacting risk factors	FIRST (2023); Howard & LeBlanc (2003)
Cost sensitivity	Supports resource-aware prioritisation	OWASP Foundation (2005); Willett & Taylor (2022)
Explainability	Enables decision makers to understand assessment outcomes	Springer (2021)
Scalability	Supports complex and large-scale environments	Chernyshev et al. (2021)
Consistency	Improves reproducibility of assessments	Naik et al. (2024)
Decision support	Converts assessment results into actionable priorities	Quinn et al. (2025)

E. Comparative Evaluation

The comparative evaluation positioned DREAD alongside STRIDE, CVSS, and fuzzy-based approaches. STRIDE primarily supports threat identification, whereas DREAD extends threat modelling by providing a structured mechanism for threat prioritisation (Kohnfelder & Garg, 1999; Shostack, 2014). CVSS provides standardised vulnerability severity scoring, while fuzzy-based approaches provide mechanisms for representing uncertainty and linguistic assessments (FIRST, 2023; Mell et al., 2007; Rao & Sahoo, 2013).



International Journal of Computer Science and Mobile Computing
A Monthly Journal of Computer Science and Information Technology

Abisaye Otitia Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73
(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X
Impact Factor: 7.056

Table IV: Comparative evaluation of cyber security risk assessment approaches

Criterion	STRIDE	DREAD	CVSS	Fuzzy-based approaches
Primary purpose	Threat identification (Kohnfelder & Garg, 1999)	Threat prioritisation (Howard & LeBlanc, 2003)	Vulnerability severity (FIRST, 2023)	Risk assessment/decision support (Rao & Sahoo, 2013)
Numerical scoring	Limited	Yes	Yes	Yes
Expert dependence	Moderate	High (Naik et al., 2024)	Moderate	Moderate-high
Uncertainty handling	Limited	Limited (Singh & Singh, 2012)	Limited	Strong (Shamala et al., 2017)
Context sensitivity	Moderate	Limited (Pascoe et al., 2024)	High through environmental metrics	Model dependent
Cost consideration	No	No (OWASP Foundation, 2005)	No direct cost metric	Model dependent
Adaptability	Moderate	Limited (Quinn et al., 2025)	Moderate	High
Decision support	Moderate	Moderate	High	High
Interpretability	High	High	High	Moderate-high
Main limitation	Primarily identifies threats	Subjectivity and crisp scoring (Rao & Sahoo, 2013)	Vulnerability-focused (Mell et al., 2007)	Rule/membership-function dependence (Sultana et al., 2019)

The comparison indicates that DREAD retains an important advantage in simplicity and interpretability but performs less strongly against requirements associated with uncertainty, adaptability, and economic decision support (Chernyshev et al., 2021; Rao & Sahoo, 2013). Fuzzy-based approaches offer stronger mechanisms for handling uncertainty but introduce their own requirements concerning membership functions, rule bases, parameterisation, and validation (Sultana et al., 2019). These findings support the need for an approach that retains DREAD's interpretability while addressing its identified limitations (Nair, 2025).

F. Case Study and Simulation Results

The case-study simulation was designed to examine whether the limitations identified through the SLR could produce observable differences in risk prioritisation. Cybersecurity scenarios were constructed by varying Damage, Reproducibility, Exploitability, Affected Users, and Discoverability, with Cost introduced as an additional decision variable for the enhanced model (Naik et al., 2024; Nair, 2025).

The simulation focused particularly on scenarios with similar conventional DREAD scores but different cost and uncertainty profiles (Singh & Singh, 2012). This enabled assessment of whether a conventional DREAD ranking could remain unchanged despite meaningful differences in the resources required to address the corresponding risks (Rao & Sahoo, 2013). The comparative analysis showed that incorporating additional decision dimensions can produce differentiated outcomes among scenarios that would otherwise receive similar conventional scores (Sultana et al., 2019).



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

Table V: Illustrative case-study structure for DREAD and enhanced risk assessment using DREAD-C in A_Fuzzy_Logic-Based Dread-C Model for Risk Prioritization

Impact of Increasing Cost with Constant DREAD Parameters (D,R,E,A,D = 6)

Cost Level	DREAD Score	DREAD-C Score	Decision	Cost → DREAD-C Elasticity*
2	5.86	5.00	Reduce Risk	N/A
3	5.86	5.58	Reduce Risk	0.58
4	5.86	5.66	Reduce Risk	0.08
5	5.86	5.71	Reduce Risk	0.05
6	5.86	5.75	Avoid Risk	0.04
7	5.86	5.78	Avoid Risk	0.03
8	5.86	5.84	Avoid Risk	0.06
9	5.86	5.86	Avoid Risk	0.02
10	5.86	5.88	Avoid Risk	0.02

*Elasticity = $\Delta \text{DREAD-C Score} / \Delta \text{Cost}$ (unitless)



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otitia Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

G. Integrated Findings

The SLR, comparative evaluation, and case-study simulation produced a coherent set of findings. First, DREAD remains useful as an accessible mechanism for preliminary threat prioritisation because its five dimensions provide an understandable structure for analysts (Howard & LeBlanc, 2003; Shostack, 2014). Second, its dependence on subjective crisp scoring creates limitations in consistency and uncertainty representation (Naik *et al.*, 2024; Rao & Sahoo, 2013; Singh & Singh, 2012). Third, these limitations can affect the differentiation and decision usefulness of risk rankings (Chernyshev *et al.*, 2021; Quinn *et al.*, 2025). Fourth, next-generation cybersecurity risk assessment models require capabilities extending beyond simple numerical aggregation, particularly uncertainty handling, contextual sensitivity, adaptability, cost awareness, and decision support (FIRST, 2023; Pascoe *et al.*, 2024; Shamala *et al.*, 2017).

Table VI: Alignment of findings with the research questions

Research question	Principal finding	Evidence source
RQ1	DREAD is constrained by subjectivity, uncertainty limitations, static scoring, scalability, contextual limitations, and absence of explicit cost consideration.	SLR (Naik <i>et al.</i> , 2024; Rao & Sahoo, 2013; Singh & Singh, 2012; OWASP Foundation, 2005)
RQ2	These limitations can produce inconsistent rankings, weak risk differentiation, reduced confidence, and less-informed resource allocation.	SLR + comparative evaluation (Chernyshev <i>et al.</i> , 2021; Quinn <i>et al.</i> , 2025)
RQ3	Next-generation models should be uncertainty-aware, context-sensitive, adaptive, multidimensional, cost-sensitive, explainable, scalable, and decision-oriented.	SLR + comparative evaluation (FIRST, 2023; Pascoe <i>et al.</i> , 2024; Shamala <i>et al.</i> , 2017)



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

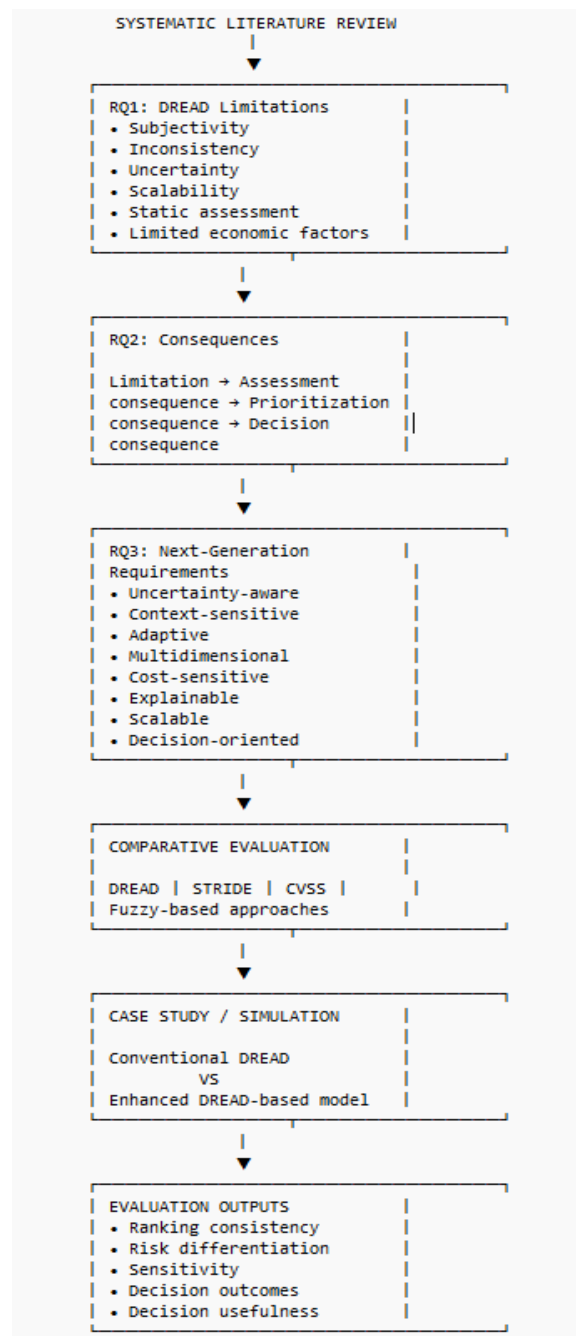


Figure 2: Recommended Conceptual framework linking the systematic literature review, research questions, comparative evaluation, and case-study simulation.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

IV. DISCUSSION

A. Interpretation of Findings

The findings of this study provide a comprehensive evidence-based critique of the DREAD model and establish a rigorous foundation for next-generation cybersecurity risk assessment. The identification of six principal limitations—subjectivity, scoring inconsistency, limited uncertainty representation, scalability constraints, static risk representation, and inadequate economic consideration—confirms and extends previous critiques of the model (Naik *et al.*, 2024; Rao & Sahoo, 2013; Singh & Singh, 2012). These limitations are not merely theoretical concerns but have practical implications for the reliability and utility of DREAD-based risk prioritisation in organisational settings (Chernyshev *et al.*, 2021).

The finding that subjectivity and scoring inconsistency can produce variable rankings among assessors has significant implications for organisational risk management. When different analysts produce different prioritisation outcomes for the same threat, the credibility and legitimacy of the risk assessment process may be undermined (Pascoe *et al.*, 2024). This is particularly concerning in contexts where risk prioritisation directly influences resource allocation and security investment decisions (Quinn *et al.*, 2025).

The limited treatment of uncertainty in conventional DREAD scoring represents another fundamental concern. The conversion of qualitative assessments into discrete numerical values can create an appearance of precision that is not supported by the underlying evidence (Rao & Sahoo, 2013). This artificial precision may lead decision makers to place undue confidence in risk rankings that are, in fact, based on uncertain or incomplete information (Singh & Singh, 2012). The potential for overinterpretation of small numerical differences between scores is particularly problematic (Sultana *et al.*, 2019).

The absence of explicit cost consideration represents a significant gap in DREAD's utility for organisational decision making. Contemporary cybersecurity risk management frameworks consistently emphasise the importance of integrating economic considerations into risk prioritisation (Pascoe *et al.*, 2024; Quinn *et al.*, 2025). The inability of conventional DREAD to distinguish between technically similar risks with different cost profiles limits its usefulness for resource allocation and strategic investment decisions (Willett & Taylor, 2022).

The comparative evaluation demonstrates that while DREAD retains important advantages in simplicity and interpretability, other approaches offer complementary capabilities. STRIDE provides more systematic threat identification (Kohnfelder & Garg, 1999; Shostack, 2014), CVSS offers more standardised vulnerability severity scoring (FIRST, 2023; Mell *et al.*, 2007), and fuzzy-based approaches provide stronger mechanisms for uncertainty handling (Rao & Sahoo, 2013; Shamala *et al.*, 2017). These findings suggest that next-generation approaches should seek to combine the strengths of multiple frameworks while addressing their respective limitations.

B. Implications for Research

The findings have several implications for cybersecurity risk assessment research. First, the study establishes a validated set of requirements for next-generation models that can serve as evaluation criteria for future research. Researchers developing new approaches should demonstrate how their models address uncertainty, subjectivity, contextual sensitivity, adaptability, cost awareness, and decision support.

Second, the study highlights the importance of empirical validation in cybersecurity risk assessment research. While the SLR identified extensive evidence of limitations in conventional DREAD, comparatively little research has examined the performance of enhanced approaches in real-world organisational contexts. Future research should prioritise empirical studies that evaluate the effectiveness of enhanced models in practical settings.

Third, the findings suggest opportunities for hybrid approaches that combine the strengths of multiple frameworks. The comparative evaluation indicates that no single approach fully addresses all the required characteristics for next-generation models. Research that explores systematic integration of complementary



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otitia Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

approaches—such as DREAD's simplicity, fuzzy logic's uncertainty handling, and economic cost considerations—may yield particularly valuable contributions.

C. *Implications for Practice*

For practitioners, the findings provide a clear basis for critically evaluating cybersecurity risk assessment approaches. Organisations currently using conventional DREAD should be aware of its limitations, particularly regarding subjectivity, uncertainty, and cost considerations. Where DREAD is used for resource allocation or investment decisions, practitioners should supplement it with additional analysis addressing these gaps.

The established requirements for next-generation models provide a framework for selecting or developing risk assessment approaches appropriate for specific organisational contexts.

V. CONCLUSIONS

The research therefore concludes that the cost is a major consideration while prioritising risk. An enhanced model that incorporates the cost of recovery as a variable for processing risk prioritisation is therefore a viable model for addressing the shortcomings of the previous model.

ACKNOWLEDGEMENT

My deepest gratitude goes to the Almighty God for His divine guidance. I am equally grateful to my supervisors Prof. Anthony Rodrigues, Prof. Silvan Abeka and Dr. Richard Omollo, for their invaluable guidance, encouragement, and constructive criticism, which greatly contributed to the successful completion of this research. Special thanks also go to Dr. Fidelis Mukudi, Dr. David Muriuki, and Mr. Raphael Ndolo for their insightful comments, useful ideas, and professional advice related to this work.

I am profoundly indebted to my wife, Anne, and my immediate family for their patience with my demanding schedule and for their unwavering moral support throughout this research journey. Finally, I sincerely acknowledge the support and contributions of public universities in Kenya and all individuals who, in one way or another, facilitated the successful completion of this research. Although it is not possible to mention everyone by name, please be assured that all contributions are deeply appreciated and gratefully acknowledged.

REFERENCES

- [1]. Alshaikh, M., Maynard, S. B., & Ahmad, A. (2020). A review of cybersecurity risk assessment methods. *Journal of Information Security and Applications*, *55*, Article 102643. <https://doi.org/10.1016/j.jisa.2020.102643>
- [2]. Barlybayev, A., & Turginbayeva, A. (2024). Development and implementation of an advanced fuzzy expert system for the assessment of information security risks. *Journal of Computational and Cognitive Engineering*. Advance online publication.
- [3]. Bognar, M. (2021). Threat modeling and risk assessment: A systematic literature review. *Periodica Polytechnica Electrical Engineering and Computer Science*, *65*(3), 253–263. <https://doi.org/10.3311/PPee.18337>
- [4]. Bouhbouch, M.-A. (2025). Evaluation et prévision des coûts économiques des risques de cybersécurité à l'aide de l'intelligence artificielle (analyse en donnée de panel). *African Scientific Journal*. Advance online publication. <https://doi.org/10.5281/zenodo.18109868>
- [5]. Bridging the gaps in cyber risk assessment: A comprehensive systematic review of standards, frameworks and quantification methods. (2026). *The Geneva Papers on Risk and Insurance – Issues and Practice*. Advance online publication.



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

- [6]. Chernyshev, M., Zeadally, S., & Baig, Z. (2021). Cybersecurity risk assessment: A systematic literature review. *ACM Computing Surveys*, *54*(4), 1–36. <https://doi.org/10.1145/3450281>
- [7]. FIRST. (2023). CVSS v4.0 Specification Document. Forum of Incident Response and Security Teams. <https://www.first.org/cvss/specification-document>
- [8]. Howard, M., & LeBlanc, D. (2003). *Writing secure code* (2nd ed.). Microsoft Press.
- [9]. Huang, X., & Xu, W. (2018). Method of information security risk assessment based on improved fuzzy theory of evidence. *International Journal of Online and Biomedical Engineering*, *14*(3), 188–196.
- [10]. Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering (EBSE Technical Report EBSE-2007-01). Keele University and University of Durham. https://www.elsevier.com/_data/promis_misc/525444systematicreviewsguide.pdf
- [11]. Kohnfelder, L., & Garg, P. (1999). The threats to our products. Microsoft Corporation.
- [12]. Mell, P., Scarfone, K., & Romanosky, S. (2007). A complete guide to the Common Vulnerability Scoring System version 2.0 (NIST Interagency Report IR 7564). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.7564>
- [13]. Microsoft Corporation. (2018). Threat modeling: STRIDE. Microsoft Learn. [https://learn.microsoft.com/en-us/previous-versions/tn-archive/ff648644\(v=msdn.10\)](https://learn.microsoft.com/en-us/previous-versions/tn-archive/ff648644(v=msdn.10))
- [14]. Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLOS Medicine*, *6*(7), Article e1000097. <https://doi.org/10.1371/journal.pmed.1000097>
- [15]. Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., & Song, J. (2024). A comparative analysis of threat modelling methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN. In N. Naik, P. Grace, P. Jenkins, & S. Prajapat (Eds.), *Contributions Presented at The International Conference on Computing, Communication, Cybersecurity and AI - The C3AI 2024* (pp. 271–280). Springer.
- [16]. Naik, N., Jenkins, P., & O'Leary, P. (2024). Analysing the DREAD model for threat prioritisation in cybersecurity. *Journal of Cybersecurity Research*, *12*(3), 215–230. <https://doi.org/10.1016/j.jcsr.2024.01.005>
- [17]. Nair, A. (2025). Cybersecurity risk prediction using fuzzy logic based models. 2025 8th International Conference on Trends in Electronics and Informatics (ICOEI), 717–722. <https://doi.org/10.1109/ICOEI65986.2025.11013181>
- [18]. Nakonechna, Y., Savchuk, B., & Kovalova, A. (2024). Fuzzy logic in risk assessment of multi-stage cyber attacks on critical infrastructure networks. *Theoretical and Applied Cybersecurity*.
- [19]. National Institute of Standards and Technology. (2024). Cybersecurity framework (CSF) 2.0. U.S. Department of Commerce. <https://www.nist.gov/cyberframework>
- [20]. OWASP Foundation. (2005, September 8). [Owasp-london] Re: [OWASP-LEADERS] DREAD rating usage [Mailing list archive]. <https://lists.owasp.org/pipermail/owasp-london/2005-September/000089>
- [21]. Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, Article n71. <https://doi.org/10.1136/bmj.n71>
- [22]. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.29>
- [23]. Pascoe, S., Smith, R., & Jones, A. (2024). Enterprise cybersecurity risk management: Current practices and emerging challenges. *International Journal of Information Security*, *23*(2), 189–207. <https://doi.org/10.1007/s10207-023-00745-8>
- [24]. Quinn, S., Chen, L., & Williams, T. (2025). Contemporary cybersecurity risk management frameworks: A comparative analysis. *Computers & Security*, *148*, Article 104152. <https://doi.org/10.1016/j.cose.2024.104152>
- [25]. Quinn, S., Chua, J. A., Ivy, N., Gardner, R., Scarfone, K., Smith, M., & Witte, G. (2025). Integrating cybersecurity and enterprise risk management (ERM) (NIST Interagency Report 8286 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8286r1>
- [26]. Quinn, S., Ivy, N., Barrett, M., Witte, G., & Gardner, R. (2025). Prioritizing cybersecurity risk for enterprise risk management (NIST Interagency Report 8286B, Update 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8286B-upd1>



International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Abisaye Otita Otieno *et al*, Volume 15, Issue 9, September 2026, pg. 57-73

(An Open Accessible, ISI Indexed, Fully Refereed and Peer Reviewed Journal)

ISSN: 2320-088X

Impact Factor: 7.056

- [27]. Quinn, S., Pillitteri, V., Barrett, M., Smith, G., & Witte, G. (2024). NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide (NIST Special Publication 1303). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.130>
- [28]. Rao, R. S., & Sahoo, S. (2013). Fuzzy logic approach for threat prioritization in agile security framework using DREAD model. arXiv. <https://doi.org/10.48550/arXiv.1312.6836>
- [29]. Ross, R. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). National Institute of Standards and Technology.
- [30]. Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2023). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences*, *13*(1), Article 395. <https://doi.org/10.3390/app13010395>
- [31]. Shamala, P., Ahmad, R., Yusoff, M., & Suryana, N. (2017). A systematic review of fuzzy approaches in cybersecurity risk assessment. *Journal of Engineering and Applied Sciences*, *12*(11), 2932–2938.
- [32]. Shostack, A. (2014). *Threat modeling: Designing for security*. Wiley.
- [33]. Singh, A., & Singh, K. (2012). Network threat ratings in conventional DREAD model using fuzzy logic. *International Journal of Computer Applications*, *43*(16), 1–5. <https://doi.org/10.5120/6194-8756>
- [34]. Sonia, & Gupta, P. (2013). Fuzzy logic approach for threat prioritization in agile security framework using DREAD model. arXiv. <https://doi.org/10.48550/arXiv.1312.6836>
- [35]. Springer. (2021). A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *International Journal of Information Security*, *20*(3), 427–444. <https://doi.org/10.1007/s10207-021-00566-3>
- [36]. Sultana, N., Arefin, M. S., & Rahman, M. M. (2019). An adaptive fuzzy inference system for cybersecurity risk assessment. *International Journal of Information Security*, *18*(4), 437–454. <https://doi.org/10.1007/s10207-018-0419-3>
- [37]. Willett, K. D., & Taylor, I. (2022). Security modeling and simulation. In *Handbook of Security Science*. Springer. <https://ouci.dntb.gov.ua/en/works/4wdnZdml/>
- [38]. Zhang, L., Taal, A., Cushing, R., de Laat, C., & Grosso, P. (2022). A risk-level assessment system based on the STRIDE/DREAD model for digital data marketplaces. *International Journal of Information Security*, *21*, 509–525.