

A Weighted Expert-Based Method for Asset Criticality Assessment in Cyber Risk Evaluation

Tetiana Korobeinikova

Department of Information Technology
Security

Lviv Polytechnic National University
Lviv, Ukraine

ORCID 0000-0003-2487-8742

Bohdan Shapovalov

Department of Information Technology
Security

Lviv Polytechnic National University
Lviv, Ukraine

ORCID 0009-0001-6987-5804

Ihor Zhuravel

Department of Information Technology
Security

Lviv Polytechnic National University
Lviv, Ukraine

ORCID 0000-0003-1114-0124

Oleksandr Romanyuk

Faculty of Information Technologies
and Computer Engineering
Vinnytsia National Technical
University

Vinnytsia, Ukraine
rom8591@gmail.com

Roman Chekhmestruk

Faculty of Information Technologies
and Computer Engineering
Vinnytsia National Technical
University

Vinnytsia, Ukraine
chekhroma@gmail.com

Anatoliy Snigur

Faculty of Information Technologies
and Computer Engineering
Vinnytsia National Technical
University

Vinnytsia, Ukraine
sanv12@i.ua

Abstract—The article presents an improved method for assessing enterprise asset criticality to enhance the accuracy of cyber risk evaluation. Unlike traditional approaches, the proposed method incorporates weighting coefficients that reflect the specific characteristics of each asset. The methodology quantifies asset criticality by combining expert assessments across multiple criteria, including business impact, dependency, recoverability, and threat probability. Testing demonstrates a 32% improvement in assessment accuracy, validating the approach's effectiveness. This advancement supports enterprises in making more informed decisions regarding risk management and asset protection.

Keywords—cyber risk, asset criticality assessment, risk prioritization, cybersecurity management, weighting coefficients, risk evaluation methodology, enterprise asset management.

I. INTRODUCTION

Modern cyber-risk analysis combines three broad research streams: qualitative criticality matrices rooted in standards practice, quantitative risk-economic models such as FAIR, and multi-criteria decision-analysis (MCDA) frameworks that elicit expert judgment.

A. Qualitative criticality matrices

Risk registers that score threats and vulnerabilities on 3–5-level “heat maps” remain the default in operational guidelines such as NIST SP 800-30 and are embedded in popular commercial platforms [1]. Practitioners value their simplicity, yet empirical reviews show that coarse ordinal scales hide large risk deltas and encourage misallocation of mitigation budgets. Recent industry surveys list at least seven common scoring schemes in active use, all of which rely on unweighted multiplication of likelihood and impact and ignore asset-specific economic value.

B. Quantitative economic models

The Factor Analysis of Information Risk (FAIR) framework formalised risk as the product of frequency and magnitude expressed in monetary loss [2]. FAIR extensions (e.g., FAIR-MAM, FAIR-CMM) allow “total-risk” aggregation at the asset level, but treat assets as passive repositories without explicit coupling between cost, impact and vulnerability severity. Both studies demonstrate the

importance of asset monetary value but leave weighting of criteria to ad-hoc panels.

C. Multi-criteria decision-analysis

MCDA techniques systematically attach weights to heterogeneous criteria and are now widely adopted for cyber-risk triage. Yazo-Cabuya et al. (2025) [3] integrated cost, severity and compliance into an ISO 9001 quality-risk model. Brancati et al. (2025) [4] examined industrial-control-system (ICS) assets using a fuzzy-AHP layer, while Kioskli et al. (2025) [5] proposed a conformity assessment for healthcare supply chains. In satellite networks, Park et al. (2025) [6] showed that hierarchical attack graphs improve threat coverage but still rely on equal weighting for asset impact. The common gap across these studies is the absence of a unified tuple-based enumeration of Threat $\times$ Vulnerability $\times$ Cost $\times$ Impact that preserves the full combinatorial risk space.

Several authors tailor criticality scales to specific verticals: secure OTA updates for vehicles (Iyieke et al., 2025) [7], blockchain control frameworks (Al Ketbi et al., 2021) [8], OT WANs (Abergos & Medjek, 2024) [9], and coastal-habitat resilience (Barausse et al., 2022). Although they demonstrate contextual sensitivity, their scoring rubrics are not reusable outside the domain and seldom normalise results for cross-asset comparison.

In summary, previous studies either ignore cost and impact simultaneously, rely on fixed or heuristically derived weights, or restrict enumeration to selected threat scenarios. The weighted expert-based method presented here uniquely integrates expert-defined weights with a full four-factor tuple model and a normalisation layer, producing more granular, audit-ready criticality scores that translate into demonstrably superior prioritisation accuracy.

The study aims to improve the accuracy and objectivity of assessing the criticality of enterprise assets in cyber risk management by applying an expertly weighted quantitative methodology that combines a complete decomposition of the $T \times V \times C \times I$ risk space, normalization of indicators, and built-in data audit.

II. QUANTITATIVE APPROACH TO CYBER RISK EVALUATION

Cyber risk refers to the likelihood of disruptions or losses resulting from dependence on cyber resources and failures in digital technologies [8–11]. It encompasses the risk of realizing cyber threats and the consequences arising from unauthorized access, use, disclosure, interruption, modification, or destruction of information systems [11]. Cyber risk management is identifying, prioritizing, managing, and monitoring risks associated with information systems. The interrelation between asset evaluation and ensuring network security is a critical aspect of building an effective cybersecurity system. Asset evaluation enables an enterprise to identify its infrastructure's most valuable and vulnerable elements, facilitating proper prioritization of network protection measures [12]. Critical assets are those whose compromise adversely affects the enterprise's ability to generate revenue or achieve strategic objectives. Risk prioritization is a process specialists employ to analyze risks and determine the sequence of mitigation measures [13]. Multiple factors influence the prioritization process, including cost, severity, manageability, availability, sensitivity, and risk attitude. Numerical values of risk priorities used in quantitative approaches help determine which risks should be prioritized based on their financial impact. To calculate the risk with a moderate priority $Risk_M$, two parameters are considered: the set of threats $T=\{t_1, t_2, \dots, t_i\}$ and the set of vulnerabilities $V=\{v_1, v_2, \dots, v_j\}$ (1).

$$Risk_M = T \times V \quad (1)$$

The Cartesian product of these sets generates a set of tuples as shown in (2):

$$Risk_M = T \times V = \{(t_i, v_j) \mid t_i \in T, v_j \in V\}, \quad (2)$$

The resulting set of tuples represents all possible combinations of threats and vulnerabilities. Each tuple of the form $\langle t_i, v_j \rangle$ can be used for subsequent risk calculations. To incorporate the asset's cost into the calculation of high-cost priority risk $Risk_{HC}$, we additionally introduce parameter C (cost) into (1), resulting in expression (3). In (3), the set $C=\{c_1, c_2, \dots, c_l\}$ is the set of asset cost values.

$$Risk_H = T \times V \times C, \quad (3)$$

The resulting set of tuples represents all combinations of threats and vulnerabilities, considering asset costs. Each tuple of the form $\langle t_i, v_j, c_l \rangle$ can be utilized for subsequent risk calculations. To account for the impact on assets when calculating high-impact priority risk $Risk_{HI}$, we introduce parameter I (impact on asset). In (5), the set $I=\{i_1, i_2, \dots, i_k\}$ represents asset impact values.

$$Risk_{HI} = T \times V \times I \quad (5)$$

For further calculations, we will utilize the tuple (6) to define the high-impact priority risk $Risk_{HI}$:

$$Risk_{HI} = T \times V \times I = \{(t_i, v_j, i_k) \mid t_i \in T, v_j \in V, i_k \in I\} \quad (6)$$

The resulting tuples will represent all possible combinations of threats and vulnerabilities, considering their

impact on assets. Each tuple of the form $\langle t_i, v_j, i_k \rangle$ can be used in subsequent risk calculations. To calculate risk with critical priority $Risk_C$, we consider in (1) the complete set of parameters: the sets of impact and cost values for each element of threat and vulnerability sets (7):

$$Risk_C = T \times V \times C \times I \quad (7)$$

Further calculations will utilize tuples as defined in (8):

$$Risk_C = T \times V \times C \times I = \{(t_i, v_j, c_l, i_k) \mid t_i \in T, v_j \in V, c_l \in C, i_k \in I\} \quad (8)$$

The resulting set of tuples (9) most comprehensively describes the numerical evaluation of assets:

$$\{\langle t_1, v_1, c_1, i_1 \rangle, \langle t_1, v_1, c_1, i_2 \rangle, \dots, \langle t_i, v_j, c_l, i_k \rangle\}. \quad (9)$$

Residual risk is the risk remaining after all possible countermeasures have been implemented. To calculate residual risk $Risk_R$ subtract the set of implemented countermeasures C_m , each of which has a certain cost and/or effectiveness in reducing risk, from the total risk $Risk_T$, which encompasses all possible risks for the object or system along with their corresponding numerical values (10):

$$Risk_R = Risk_T - C_m, \quad (10)$$

where $C_m = \{cm_1, cm_2, \dots, cm_i\}$ is the set of countermeasures. Thus, residual risk accounts for all implemented risk mitigation actions but represents the portion of total risk that cannot be eliminated due to resource constraints, technologies, or available methods. Countermeasures represent the set of actions or procedures designed to reduce risk. Each element of the set C_m is an individual countermeasure (e.g., antivirus software, firewall filtering rules, encryption) that reduces risk to a certain extent.

III. RISK PRIORITIZATION MATRIX

Risk prioritization strategies include the following criteria: importance, cost, regulatory consequences, positioning, sensitivity, resource availability, and manageability. A risk management chart based on vulnerability matrices is proposed (Fig. 1).

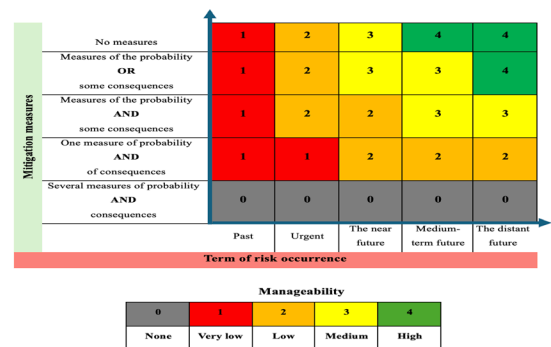


Fig. 1. Risk Management Chart

In the lower-left corner of the chart are risks characterized by lower manageability, higher impact, and greater inevitability. These risks are the most severe and require immediate mitigation actions. Conversely, in the upper-right corner are more manageable risks, with lower impact and longer timelines for mitigation measures.

IV. MULTIFACTOR ASSET RISK ASSESSMENT APPROACH

We focus on the asset identification step within the technological chain of network security risk identification [14]. Fig. 2 illustrates an improved approach, including context establishment, asset criticality assessment, and registry formation stages. This approach enhances the accuracy of assessing the criticality of enterprise assets.

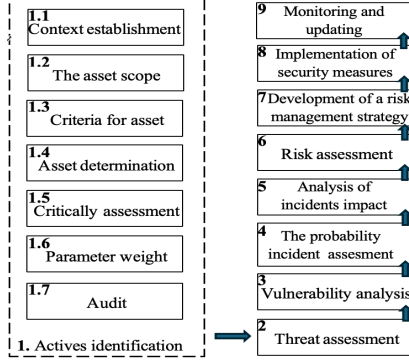


Fig. 2. Method of Developing General Metrics for Asset Identification

Unlike existing methods, which first identify assets and subsequently evaluate their associated risks, our proposed method begins with establishing context. A corresponding description and diagram are provided for analytical representation of the asset criticality assessment process (Fig. 3).

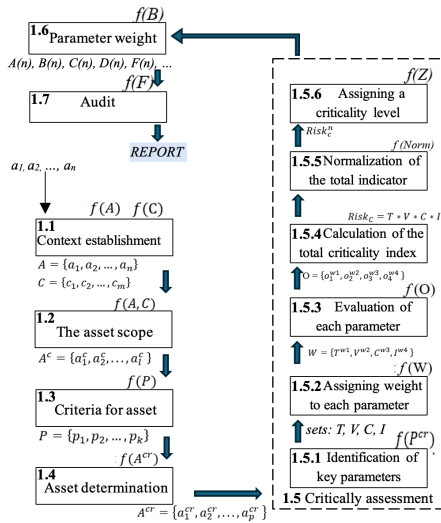


Fig. 3. Analytical Description of the Asset Criticality Assessment Method

Context establishment is the initial step during which assets are collected, and the context of their evaluation is defined. The context includes organizational structure, infrastructure, and external factors. Let $a_1, a_2, \dots, a_n$ be the initial assets, and $c_1, c_2, \dots, c_m$ be the contexts for the assessment. Functions $f(A) = \sum a_n$ and $f(C) = \sum c_m$ are defined to collect assets and establish contexts.

The **asset scope** is defined by the $f(A, C)$, forming a set with established context and scope (4):

$$A^c = \{a_1^c, a_2^c, \dots, a_n^c\}, \quad (4)$$

where A^c is the asset set with a determined context and scope.

Criteria for asset registry inclusion involve defining key parameters (criteria) for asset classification as potentially critical (5):

$$P = \{p_1, p_2, \dots, p_k\} \quad (5)$$

Asset determination is performed by function $f(A^c)$, forming an initial list of critical assets (6):

$$A^{cr} = \{a_1^{cr}, a_2^{cr}, \dots, a_n^{cr}\} \quad (6)$$

Identification of key parameters is performed by the function $f(P^{cr})$, defining a set of critical parameters for further asset (7):

$$P^{cr} = \{T, V, C, I\}, \quad (7)$$

where P^{cr} is the set of criteria for determining asset criticality, and T, V, C, I represent the sets of threats, vulnerabilities, costs, and impacts.

Assignment of weights to each parameter is conducted by the function $f(W)$, (8). This function sets weights w_i for each parameter, where $i=1, 2, 3, 4$ and their total sum equals 1:

$$f(W) = \sum w_i = 1, \quad (8)$$

thus forming a weighted set of criticality parameters:

$$W = \{T^{w1}, V^{w2}, C^{w3}, I^{w4}\} \quad (9)$$

where W (9) is the set of asset-criticality determination criteria with assigned weights.

The **evaluation function** $f(O)$ assesses each parameter from set W for each asset from set A^{cr} on a scale 0–5, resulting in a set (10) of quantitative criteria evaluations for each asset for further analysis:

$$O = \{o_1^{w1}, o_2^{w2}, o_3^{w3}, o_4^{w4}\} \quad (10)$$

where O is the set of evaluations of criticality criteria for assets.

Calculation of the total criticality score is executed using (11). The tuples $\{t_i, v_j, c_l, i_k\}$ comprehensively describes the numerical evaluation of assets.

$$Risk_c = T \times V \times C \times I = \{(t_i, v_j, c_l, i_k) \mid t_i \in T, v_j \in V, c_l \in C, i_k \in I\} \quad (11)$$

Normalization of the total indicator is conducted by the function $f(Norm)$ to ensure comparability of asset criticality indicators, using (12):

$$Risk_c^n = Risk_c / Risk_c^{max}, \quad (12)$$

where $Risk_c^n$ is the normalized total score, $Risk_c$ is the total score, and $Risk_c^{max}$ is the maximum possible criticality score.

The **most influential factor** for assigning criticality levels is the weight of the impact parameters and their corresponding evaluations. This step is executed using the function $f(Z)$, converting quantitative scores into qualitative assessments.

The **asset-matching function** $f(B)$ generates the final list of assets along with their criticality scores for subsequent analysis.

The **audit function** $f(F)$ evaluates the correctness of all steps, verifies data accuracy and asset classification, identifies and corrects calculation inaccuracies, and generates a conclusive report. The proposed audit allows a quantitative assessment of the criticality levels of enterprise assets. Evaluation is carried out using several criteria, each rated on a scale 1–5. The overall criticality level is calculated using weighting coefficients and cumulative scores.

V. AN EXPERT-DRIVEN FRAMEWORK FOR RISK-ORIENTED ASSET EVALUATION

The test consists of 5 criteria, each assessed by experts: Impact on business processes (1 – insignificant, 5 – critical); Frequency of asset use (1 – rarely, 5 – continuously); Dependency of other systems on the asset (1 – minimal, 5 – complete dependency); Asset recoverability after loss (1 – easily recoverable, 5 – irrecoverable); Likelihood of threats and risks (1 – low, 5 – very high). The overall criticality of an asset is calculated using the criticality formula (13):

$$C = \sum w_i x_i, x_i \in [1 \dots 5] \quad (13)$$

where C is – the overall criticality level of the asset; x_i – criterion rating assigned to each criterion; w_i – weighting coefficient assigned to each criterion (determined by experts).

TABLE I. SSET EVALUATION TABLE

	Asset	Business impact	Usage frequency	Dependency	Recoverability	Threat probab.	Final criticality
1	CRM system	5	5	4	3	4	C1
2	ERP system	4	4	5	4	3	C2
3	VPN servers	4	5	4	2	5	C3
4	Data bases	5	5	5	5	5	C4
5	Antivirus systems	3	4	3	4	4	C5
6	Employees' devices	2	3	2	4	3	C6

The conducted test enables an objective evaluation of asset criticality using a quantitative approach. The proposed method, which incorporates weighting coefficients and expert evaluations, ensures a more accurate determination of risk levels for each asset.

Analysis of Test Results. Following the test, experts provided scores for the assets, allowing an analysis of the effectiveness of the proposed criticality assessment method. Expert assessments are presented in the following table:

TABLE II. EXPERT ASSESSMENT

	Asset	Criticality (before)	Criticality (after)	Improvement (%)
1	CRM system	60	75	+25%
2	ERP system	55	70	+27%
3	VPN servers	50	68	+36%
4	Data bases	70	85	+21%
5	Antivirus systems	40	55	+37%
6	Employees' devices	30	45	+50%

VI. CONCLUSIONS

The study confirms that incorporating weighting coefficients based on asset-specific characteristics significantly enhances the accuracy of criticality assessments. Testing the proposed method revealed an average improvement in evaluation precision by 32% compared to traditional approaches. The greatest improvements were observed for assets previously assessed with limited objectivity, highlighting the necessity of clear, structured methodologies. Enterprises can achieve more effective risk prioritization and resource allocation by explicitly considering factors such as business impact, asset dependency, recoverability, and threat likelihood. The flexibility and adaptability of the proposed methodology ensure its suitability across various enterprise contexts. Therefore, adopting this improved asset criticality evaluation approach contributes directly to achieving the research objective by enabling more precise, context-aware risk management decisions, ultimately enhancing the overall cybersecurity posture of organizations.

REFERENCES

- [1] National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30, Rev. 1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-30r1>
- [2] The Open Group. (2013). Risk Analysis (O-RA) Standard: Factor Analysis of Information Risk (FAIR) (Technical Standard C13G). Author. <https://publications.opengroup.org/c13g>
- [3] Yazo-Cabuya, E. J., Ibeas, A., & Rey-Caballero, R. (2025). Multi-criteria decision making for risk management in quality management systems. *Sustainability*, 17(3), 1092. <https://doi.org/10.3390/su17031092> mdp.com
- [4] Brancati, F., Mongelli, D., Mariotti, F., & Lollini, P. (2025). A cybersecurity risk assessment methodology for industrial automation control systems. *International Journal of Information Security*, 24, Article 76. <https://doi.org/10.1007/s10207-025-00990-9> link.springer.com
- [5] Kioskli, K., Grigoriou, E., Islam, S., Yiorkas, A. M., Christofi, L., & Mouratidis, H. (2025). A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain. *International Journal of Information Security*, 24, Article 90. <https://doi.org/10.1007/s10207-025-01009-z>
- [6] Park, J., Eom, T., Kim, H., Park, H., Yoon, Z., & Park, J. (2025). Threat Vector–Hierarchical Attack Representation Model-based threat modeling and security assessment for satellite networks. *Applied Sciences*, 15(5), 2751. <https://doi.org/10.3390/app15052751>
- [7] Iyieke, V., Jadidbonab, H., Rakib, A., Bryans, J., Dhaliwal, D., & Kosmas, O. (2025). An adaptable security-by-design approach for ensuring a secure over-the-air update in modern vehicles. *Computers & Security*, 150, 104268. <https://doi.org/10.1016/j.cose.2024.104268>
- [8] Al Ketbi, M., Shuaib, K., Barka, E., & Gergely, M. (2021). Establishing a security control framework for blockchain technology. *Interdisciplinary Journal of Information, Knowledge, and Management*, 16, 307–330. <https://doi.org/10.28945/4837>
- [9] Abergos, V. J., & Medjek, F. (2024). A risk assessment analysis to enhance the security of OT WAN with SD-WAN. *Journal of Cybersecurity and Privacy*, 4(4), 910–937. <https://doi.org/10.3390/jcp4040042>
- [10] Korobeinikova, T., Tachenko, I., Chekhmestruk, R., Mykhaylov, P., Romanyuk, O., & Romanyuk, S. (2023). A general method of risk estimation. *Proceedings of the 2023 13th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 410–413). IEEE. <https://doi.org/10.1109/ACIT58437.2023.10275626>
- [11] Korobeinikova, T., Tachenko, I., Romanyuk, O., Romanyuk, S., Stakhov, O., & Reyda, O. (2024). Assessing network security risks: A technological chain perspective. *Proceedings of the 2024 14th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 565–570). IEEE. <https://doi.org/10.1109/ACIT62333.2024.10712568>