



Quantitative Risk Analysis of IT Assets in Public Broadcasting: A Case Study at TVRI East Java

Lailatul Maulida

[The author informations are in the declarations section. This article is published by ETFLIN in Digital System and Computing, Volume 1, Issue 1, 2025, Page 6-12. DOI 10.58920/etflin000000 (pending update; Crossmark will be active once finalized)]

Received: 14 August 2025
Revised: 04 September 2025
Accepted: 20 October 2025
Published: 07 November 2025

Editor: Samsul Arifin

This article is licensed under a Creative Commons Attribution 4.0 International License. © The author(s) (2025).

Keywords: Quantitative risk analysis, IT asset management, Annual Loss Expectancy.

Abstract: Public institutions increasingly depend on IT assets to sustain essential operations, yet many still lack structured risk management frameworks. At TVRI East Java, the absence of a dedicated IT division underscores the need to evaluate asset vulnerabilities and threat exposures systematically. This study identifies and prioritizes critical IT assets and their associated risks using the Quantitative Risk Analysis (QRA) method. Data were gathered through interviews, document analysis, and expert validation. Thirteen IT assets were assessed against fifteen potential threats, and quantitative metrics such as Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE) were used to estimate financial impacts. The analysis showed that personal computers are the most critical assets, primarily threatened by computer viruses, while minor peripherals pose minimal risk. Expert verification confirmed that the findings reflect real operational conditions. However, the study's scope was limited by the reliance on a single expert for data validation, which may constrain the broader applicability of the findings. The results provide a structured basis for risk mitigation strategies and can guide similar institutions in strengthening IT asset management.

Introduction

Information technology (IT) assets serve as critical infrastructure in modern organizations, especially in public broadcasting institutions like TVRI East Java (1, 2). As organizations increasingly depend on IT systems for essential operations, such as TV broadcasting, these assets become vulnerable to various risks including data loss, malware attacks, and system failures (3, 4). These vulnerabilities threaten not only operational continuity but also financial stability. In Indonesia, IT risk management is mandated by law (5), yet many government institutions, including TVRI East Java, lack comprehensive risk documentation and structured asset protection strategies (6).

According to ISO/IEC 13335-1, risk analysis is essential to identify, measure, and map organizational vulnerabilities (7). The ISO/IEC 27005 framework, as seen in the study by Kurniawan & Salma (2025), provides formal guidelines in defining risks, probabilities, and consequences in the context of information security (8). The urgency is underscored by studies reporting substantial financial losses resulting from unmitigated IT risks, especially in public and broadcasting sectors (9). Despite existing qualitative and hybrid methods, quantitative approaches offer a more objective assessment by translating risks into measurable financial losses (10, 11). The Quantitative Risk Analysis (QRA) method, using metrics like Single Loss Expectancy (SLE) and Annualized Loss

Expectancy (ALE), facilitates evidence-based prioritization in asset maintenance and control (12). However, little has been done to incorporate IT assets in the context of Industry 5.0, characterized by interconnected systems, big data, and cyber-physical infrastructure, into risk models, especially in government-run media institutions.

This study aims to fill that gap by applying the QRA method to evaluate IT asset risks at TVRI East Java, identifying the assets and threats with the highest financial impact. A mixed-methods approach involving field interviews and document analysis was used to determine asset values and assess vulnerabilities. The results are expected to support data-driven asset prioritization and risk mitigation strategies, helping public institutions safeguard their digital infrastructure more effectively.

Methodology

Study Design and Rationale

This study employed a descriptive quantitative research design using the Quantitative Risk Analysis (QRA) method to assess the potential financial impact of IT asset risks at TVRI East Java. The rationale for choosing QRA lies in its capacity to convert identified threats into measurable monetary losses, providing a rational basis for asset prioritization and risk mitigation in public-sector broadcasting organizations. This methodological approach aligns with recent frameworks

such as ISO/IEC 27005:2022, which structure risk management through the quantification of asset exposure and probability of loss (13).

Study Setting and Population

The research was conducted at TVRI East Java, a regional public broadcasting institution. The population includes all tangible IT assets owned and utilized by the organization between 2018 and 2020.

Data Collection and Materials

Data were collected through semi-structured interviews and document analysis. Interviews were conducted with the Head of Technical Production and Broadcasting to identify existing IT assets and associated threats. Supporting documents, such as procurement databases, asset inventory logs, and maintenance records, were used to obtain the quantity and monetary value of each asset.

Risk Assessment Procedures

The QRA method was implemented in seven continuous steps, beginning with defining the scope of evaluation, which was limited to tangible IT assets directly involved in TV production. Asset identification and valuation were performed based on procurement databases, ensuring price accuracy and categorization consistency. Subsequently, potential threats were identified using the Merrit risk taxonomy, encompassing 15 common threat vectors including power outage, virus infection, physical damage, and hardware theft. Each asset-threat pair was evaluated for exposure using an Exposure Factor (EF), derived from expert judgment and analysis of past incidents. Annual Rate of Occurrence (ARO) values were then estimated based on institutional risk records over a three-year period. These variables were used to calculate Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE), with formulas $SLE = \text{Asset Value} \times EF$ and $ALE = SLE \times ARO$. This calculation process reflects the standardized structure of quantitative risk assessment as outlined in ISO/IEC 27005:2022 and recent methodological studies emphasizing probability impact quantification in risk estimation (14). Results from the risk computation were further analyzed to determine the assets and threat types with the highest cumulative financial risk, which were then prioritized for mitigation.

Data Analysis

Descriptive statistical methods were used to analyze the computed ALE values. Risk matrices were constructed to rank both individual assets and threat categories. These rankings served as a decision-making tool to propose maintenance prioritization and investment recommendations in risk control strategies.

Results

Literature Review

The literature review served as the initial phase of this study, focusing on academic documents relevant to risk analysis using the Quantitative Risk Analysis (QRA) method and Information Technology (IT) assets within the context of Industry 5.0. Relevant sources included undergraduate theses and peer-reviewed journal articles. The selection of documents on IT assets was guided by two criteria: (1) publication years ranging from 2011 to 2020, and (2) the

presence of the keyword "information technology assets." Identified studies were examined to extract and classify various types of IT assets, which were then organized into tabular form to facilitate analysis and comparison.

The review yielded several documents discussing risk analysis using QRA and 27 journal articles specifically addressing IT assets in the Industry 4.0 era.

Defining the Scope

The first stage in the risk analysis process involved defining the scope of evaluation. This included three key components: identifying the assessment object (i.e., the location and number of IT assets to be analyzed), selecting the appropriate risk analysis method, and determining the specific areas requiring risk control. The IT assets under evaluation were classified into two categories: those relevant to the Industry 4.0 framework and those currently in use at TVRI East Java.

Object Selection

The selected research site was TVRI East Java, a regional public television station established on March 3, 1978, and located at Jl. Mayjend Sungkono No. 124, Surabaya. The institution was chosen due to its heavy reliance on information technology (IT) assets for its core business activity, television broadcasting. The scope of evaluation included both the quantity and operational distribution of IT assets across organizational units. TVRI's institutional structure comprises multiple divisions including programming, news, technical operations, and administration, all of which utilize IT infrastructure in varying capacities.

Data Collection

Data collection was conducted between March and September 2020 through two methods: interviews and document analysis. A semi-structured interview was held with Anasrul Yusak, M.Kom., Head of Broadcasting and Production Technology, who was selected based on his extensive experience in IT asset management within TVRI and prior service at Indonesia's Ministry of Communication and Information Technology. The interview provided key insights into TVRI's organizational vision and mission, historical IT asset risks, and inventory records from 2018 to 2020.

In addition, document analysis was carried out to strengthen the findings obtained through interviews. This included reviewing internal records such as equipment repair reports, which revealed several IT assets, such as personal computers, laptops, and servers, had undergone technical maintenance.

IT Asset Identification and Classification

To determine the IT assets used at TVRI East Java, the researcher conducted direct field observations and semi-structured interviews with the Head of Broadcasting and Production Technology. The interview protocol was designed in accordance with the requirements of Quantitative Risk Analysis (QRA) and approved by institutional authorities following formal research permit procedures. Data collection took place in two interview sessions, supplemented by official inventory documents shared by the informant via WhatsApp.

From this inventory data, a total of 36 IT-related items were identified and classified according to the Industry 4.0

Table 1. Quantity of IT assessed in risk analysis.

IT Asset Category	Example Devices	Total Quantity
Computing Devices	PC, Server	30
Broadcasting Equipment	Studio Camera, Microphone	25
Networking Devices	Router, Switch	9
Supporting Peripherals	UPS, Monitor, Printer	12
Total Registered Assets		76

Table 2. IT asset valuation based on market price (Lazada).

No	IT Asset Type	Quantity	Total Price (IDR)
1	Smartphone	11	IDR 65,344,500
2	Telephone	1	IDR 165,000
3	Wi-Fi Router	4	IDR 928,000
4	Server	2	IDR 148,595,000
5	Personal Computer	36	IDR 361,009,100
6	CCTV	2	IDR 900,000
7	Camera	19	IDR 222,129,000
8	LCD Projector	1	IDR 5,000,000
9	Monitor	9	IDR 10,290,699
10	Laptop	19	IDR 93,583,465
11	Keyboard	3	IDR 360,000
12	Mouse	3	IDR 345,000
Total			IDR 908,649,764

Table 3. Risk occurrence rate (ARO) for IT threats.

No	Risk Description	ARO Value
1	Power loss	0.30
2	Communication loss	0.12
3	Data integrity loss	0.45
4	Accidental errors	0.15
5	Computer virus	0.80
6	Abuse of access privileges by employees	0.20
7	Natural disasters	0.00
8	Attempted unauthorized system access by outsiders	0.80
9	Theft or destruction of IT assets	0.10
10	Destruction of data	0.10
11	Abuse of access privileges by other authorized users	0.10
12	Successful unauthorized access by outsiders	0.10
13	Non-disaster-related downtime	0.15
14	Fire	0.20
15	Earthquake	0.20

framework. These assets were then reviewed to determine their relevance to the study's scope, which focused solely on tangible IT assets, those providing direct operational or economic benefits, such as hardware, servers, and computers. Based on this criterion, all 36 identified items

were categorized as tangible IT assets.

In parallel, a literature review was conducted to compile a list of IT assets commonly associated with the Industry 4.0 paradigm. This review, covering publications from 2011 to 2020, resulted in a list of 46 IT assets, which were subsequently categorized into 36 tangible and 10 intangible items. A comparison was then made between the Industry 4.0 asset list and the TVRI inventory to identify overlapping assets.

The result of this comparison showed that 12 Industry 4.0-aligned IT assets were present within the TVRI East Java environment. These 12 assets, including personal computers, servers, IoT devices, sensors, and audiovisual systems, served as the primary focus for the subsequent stages of risk analysis.

Asset Valuation

Following the identification of IT assets, the next step involved determining both the quantity and market value of each item. The number of assets was derived from a direct review of TVRI East Java's inventory records, which included specifications such as asset type, brand, and quantity. The summarized data are presented in **Table 1**. Price data were obtained using Lazada between June 9–11, 2020. The total valuation of IT assets is summarized in **Table 2**. Thus, the total market valuation of tangible IT assets at TVRI East Java amounted to IDR 908,649,764.

Risk and Threat Identification

This study adopted 15 categories of IT asset risks and threats as defined by J.W. Merritt. Following the classification of these risks, the Annualized Rate of Occurrence (ARO) was determined for each threat. ARO represents the likelihood, expressed as a percentage, that a specific risk will materialize within a one-year period.

The ARO values were obtained through a structured interview with Mr. Anasrul Yusak, M.Kom, a senior technical manager at TVRI East Java with extensive experience in IT infrastructure. The interview, conducted online via Zoom on June 23, 2020, involved assigning percentage likelihoods (1–100%) to each identified risk based on his professional judgment and experience.

The results show that the highest risk occurrences were associated with computer virus and attempted unauthorized system access by outsiders, each with an ARO of 0.80 (**Table 3**). Conversely, natural disasters were considered the least likely, with an ARO of 0.00.

Determining the Exposure Factor (EF)

Exposure Factor (EF) represents the percentage of asset loss resulting from specific threats or risks and is essential for quantitative risk analysis. In this study, EF values were obtained through a structured expert interview with Mr. Anasrul Yusak, M.Kom, who also participated in prior stages of the risk assessment process.

During the interview, which was conducted online via Zoom on June 23, 2020, the expert was asked to estimate the potential loss percentage for each of the 12 previously identified IT assets across 15 defined risk categories. Each percentage was then converted into decimal values to facilitate further calculation in the quantitative risk modeling.

The resulting EF values serve as critical input parameters for calculating Single Loss Expectancy (SLE) and Annual Loss Expectancy (ALE) in subsequent steps.

The resulting Exposure Factor values for each IT asset

against the fifteen identified threats were obtained through expert interviews and converted into decimal form to facilitate calculation.

The complete matrix of Exposure Factor (EF) values for all asset-threat combinations is provided in the appendix.

Based on the Exposure Factor (EF) data, two threat categories, natural disasters and earthquakes, were assigned an EF value of 0, indicating no anticipated impact on IT assets. The highest EF value was recorded for two asset types: personal computers and laptops, both under the computer virus threat category, with an EF score of 0.8. This suggests that malware attacks are considered to pose the greatest potential loss to critical operational devices at TVRI East Java.

Group Evaluation

As previously noted, TVRI East Java lacks a dedicated IT division. Consequently, all IT asset management and control are handled by Mr. Anasrul Yusak, M.Kom, Head of Technical Production and Broadcasting. Thus, the group evaluation was conducted solely with his involvement.

The evaluation was conducted virtually via Zoom on Friday, September 4, 2020, at 15:00 WIB. In the first discussion on threats, the researcher reviewed the 15 identified threat categories and the previously assigned Annualized Rate of Occurrence (ARO) values. The expert validated both the threat list and the ARO values.

In the second discussion on Exposure Factor (EF), the researcher re-explained the impact percentages, which the expert confirmed as consistent with real-world conditions at TVRI. In the third review, the IT assets were validated based on their alignment with Industry 4.0 and their presence at TVRI East Java. The pricing of these assets was also reviewed, with the researcher explaining that market prices were obtained via the Lazada platform, using online market data to reflect realistic asset values.

The expert provided critical feedback regarding two asset categories, Wi-Fi and CCTV, whose quantities were outdated in the inventory. Following this input, the number of Wi-Fi units was revised from 4 to 23, and CCTV units from 2 to 20.

Calculation

The calculation phase involved three systematic steps. First, a spreadsheet matrix was constructed by inputting the monetary values of IT assets along the vertical axis, derived from validated market prices. Second, 15 threat categories were listed along the horizontal axis, each assigned an Annual Rate of Occurrence (ARO) based on expert judgment. Third, Exposure Factor (EF) values were inserted into the intersecting cells between each asset and threat, reflecting the estimated percentage of loss if a threat were to occur. All input values used in the matrix were compiled and verified during the data collection and validation process.

This matrix structure allowed for the integration of asset value, annualized threat probability, and potential impact severity into a single view. Notably, two threats, *natural disasters* and *earthquakes*, had an EF value of zero, indicating no expected loss for any IT asset categories.

To support the quantitative risk analysis, a detailed matrix was compiled by combining asset values, annualized rate of occurrence (ARO), and exposure factor (EF) for each identified threat and asset. This matrix forms the basis for calculating Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE), and is presented in the appendix.

Based on the exposure factor matrix presented in the

$$SLE = \text{Asset Value} \times EF$$

Equation 1 | *SLE* (Single Loss Expectancy) is the estimated financial loss for a single incident involving a specific threat to an IT asset. *EF* = exposure factor.

$$ALE = SLE \times ARO$$

Equation 2 | *ALE* = Annual Loss Expectancy. *ARO* (Annualized Rate of Occurrence) is the estimated frequency or probability of that threat occurring within one year.

appendix, the values for earthquake and natural disaster risks are zero, indicating no measurable impact on IT assets. The highest exposure factors were associated with the risk of computer virus, particularly affecting personal computers and laptops.

The second calculation step involved generating a new spreadsheet, where each cell represents the Single Loss Expectancy (SLE), calculated as the product of the asset value and its corresponding Exposure Factor (EF). *SLE* quantifies the monetary loss expected from a single security incident, using **Equation 1**.

According to the Single Loss Expectancy (SLE) results presented in the appendix, the threat categories of "earthquake" and "natural disaster" yielded no calculated losses, indicating no financial impact on the identified IT assets. The lowest SLE values were recorded for keyboard and mouse assets, each affected by only three types of threats. Conversely, the highest SLE was observed in personal computers (PCs) under the "computer virus" threat, amounting to IDR 288,807,280.

The third step in the risk assessment process involved calculating the Annual Loss Expectancy (ALE) by multiplying each SLE value by its corresponding Annualized Rate of Occurrence (ARO). *ALE* represents the expected annual monetary loss due to specific security threats impacting each IT asset. The formula applied is **Equation 2**. As detailed in the appendix containing ALE results, several threats pose substantial financial losses, with the highest ALE recorded for personal computers due to computer virus attacks (IDR 231,045,824).

Discussion

Risk Analysis

The final stage of the Quantitative Risk Analysis (QRA) involves evaluating and prioritizing which aspects of IT assets require immediate control. Two analytical approaches were employed: Analysis Across Asset and Analysis Across Risk (15).

The findings from both the Analysis Across Asset and Analysis Across Risk methods provide a clear basis for prioritizing IT security measures. The high financial loss associated with personal computers (IDR 393,860,928) underscores their central role in organizational operations and their susceptibility to high-impact threats. This aligns with previous studies such as Bilgin M. et al. (2024), which identified physical loss as primary loss contributors in IT risk assessments due to their critical data storage and processing functions (16). Conversely, the minimal loss potential associated with mice (IDR 7,762) reflects their low replacement cost and limited operational disruption, supporting the notion that resource allocation should be proportional to asset value and criticality.

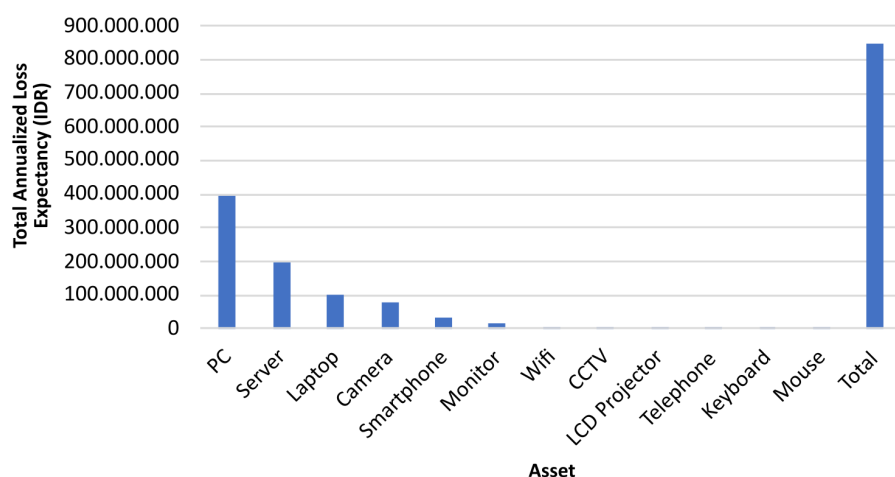


Figure 1. Comparison of total Annualized Loss Expectancy (ALE) per IT asset.

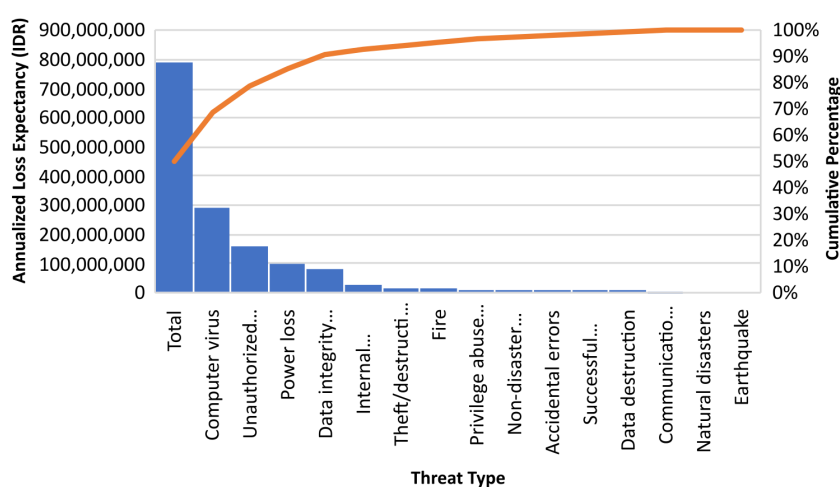


Figure 2. Annualized Loss Expectancy (ALE) distribution by threat type.

These quantitative outcomes indicate that the concentration of losses in computing devices particularly personal computers and servers reflects the institution's dependence on digital workflows and networked broadcasting systems. This implies that the most critical vulnerabilities are not merely a function of asset value but of their operational centrality. Instead of viewing the results as isolated numbers, this pattern reveals that digital production continuity at TVRI East Java is particularly sensitive to endpoint device failures and cyber threats.

To improve the clarity of **Figure 1** presents a graphical representation of the total Annualized Loss Expectancy (ALE) across IT assets. This visualization demonstrates that personal computers and servers constitute the primary contributors to the institution's overall financial risk exposure, reaffirming their designation as operationally critical assets within the organizational infrastructure.

A comparative interpretation of this ranking suggests that high-value computing assets act as both the operational and financial backbone of the organization. Prioritizing protection for these devices would therefore yield the greatest reduction in potential loss. This interpretation aligns with Bilgin et al. (2024), who emphasize that IT risk management should focus on devices responsible for data storage and processing, as they represent the most

significant points of organizational exposure (16).

In the risk-oriented analysis, the computer virus emerged as the most financially damaging threat (IDR 294,961,866), surpassing hardware failures, human error, or other environmental factors. This is consistent with Alawida M. et al. (2022), who reported that malware and virus-related incidents account for a significant portion of total IT-related financial losses (17). The results of this study are in line with the ISO/IEC 27005-based risk evaluation as demonstrated in the AMS audit (2024), and reinforce that formal methodological practices (such as ISO standards and QRA maturity models) are important for accuracy and credibility (18). The absence of recorded losses from natural disasters and earthquakes may be attributed to either low exposure probability within the study's geographical context or effective existing disaster-preparedness measures.

As illustrated in **Figure 2**, threats associated with computer viruses and unauthorized system access overwhelmingly dominate the overall risk landscape, accounting for the largest proportion of annualized financial losses. The visualization provides a comprehensive depiction of risk concentration across various threat categories, thereby facilitating data-driven prioritization and evidence-based decision-making in IT risk management.

Visualizing these results through **Figures 1** and **2**

provides a clearer understanding of how loss concentration is distributed across both assets and threat categories, supporting more data-driven decision-making in IT security planning.

From an analytical standpoint, these results confirm that technological risks especially malware and unauthorized system access dominate over environmental or accidental risks in shaping the institution's overall risk posture. This observation mirrors findings by Alawida et al. (2022), who also identified cyber-originated threats as primary financial drivers in public and media-sector IT environments (17). Hence, strengthening network defense mechanisms and adopting continuous monitoring tools should become central strategies in TVRI's risk mitigation framework.

Beyond measurable financial implications, these risks also carry significant non-financial consequences. Service interruptions caused by malware infections or system downtime could disrupt broadcasting continuity, directly impacting TVRI's credibility and audience trust. In public broadcasting, reputation and reliability are essential; even short-term downtime can diminish public confidence and damage institutional image. These intangible effects though difficult to quantify often generate long-term operational and reputational harm that exceeds the monetary losses indicated by ALE values. Studies by Beckley (2025) similarly emphasize that reputational and service continuity risks must be integrated into holistic IT risk management frameworks (19). Therefore, incorporating both financial and non-financial perspectives enriches the overall interpretation of risk exposure and aligns with contemporary Industry 5.0-oriented resilience strategies.

By integrating asset-based and risk-based perspectives, this study confirms that PCs and computer virus threats represent the most critical combination in terms of financial loss potential. Prioritizing controls in these areas, such as deploying advanced endpoint protection, regular patch management, and robust backup systems, can significantly reduce organizational exposure. Future work should consider incorporating probability-of-occurrence metrics, qualitative impact factors (e.g., reputational damage), and evolving cyber threat trends to refine prioritization further. Additionally, longitudinal monitoring of loss patterns could enhance predictive accuracy and inform adaptive IT security strategies.

Practically, these findings imply that investment in cybersecurity infrastructure such as endpoint protection systems, regular patch management, and employee awareness programs will have a direct and measurable impact in reducing the Annualized Loss Expectancy (ALE). Furthermore, implementing periodic reassessment cycles could ensure that evolving threats are detected before they cause significant operational disruption.

Verification of Findings

The verification process with an industry practitioner served as an important step in strengthening the credibility of the Quantitative Risk Analysis (QRA) outcomes. The alignment between the analytical results and Mr. Yusak's professional judgment indicates that the risk prioritization not only reflects theoretical calculations but also resonates with operational realities at TVRI East Java. Similar approaches have been highlighted by Beckley (2025), which emphasize the value of expert validation in enhancing the accuracy and acceptance of risk assessments, especially in environments where comprehensive data infrastructures are limited (19).

The alignment between quantitative data and expert validation also highlights the relevance of integrating practitioner insight into analytical modeling. Beyond numerical results, this process reflects a socio-technical understanding of risk, where human expertise complements financial estimation to create a more realistic assessment of institutional vulnerabilities.

The confirmation that PCs and computer viruses represent the most pressing risks reinforces the urgency of targeted interventions in these areas. Comparable findings were reported by Kandasamy K. et al. (2020), who found that endpoint hardware and malware threats consistently ranked highest in broadcast and media IT risk assessments (19). The concurrence between calculated loss values and field experience in this study suggests that the data inputs and weighting factors used in the QRA were representative of actual conditions, a point also supported by Daniel G. et al. (2023), who stressed the importance of aligning quantitative models with domain-specific operational knowledge (20).

In practice, incorporating expert verification into the QRA process not only increases the robustness of the results but also facilitates stakeholder buy-in for mitigation strategies, as noted in the work of Nilesh N. J. and James H. L. (2011) (21). Such integration helps identify context-specific factors, such as workflow patterns, infrastructure constraints, and organizational risk culture, that may be overlooked by purely quantitative models. Future research could expand this validation process by including multiple stakeholders from different operational tiers, thereby achieving a more holistic risk prioritization and improving the practical feasibility of control measures.

Conclusion

This study applied the Quantitative Risk Analysis (QRA) method to identify and prioritize IT asset risks at TVRI East Java. The results indicate that personal computers and computer viruses represent the most critical asset-threat combination, highlighting the predominance of technological over environmental risks in public broadcasting contexts.

From a theoretical perspective, the research reinforces the applicability of quantitative risk metrics specifically Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE) as reliable tools for financial-based decision-making in IT asset management. In practical terms, the findings emphasize the necessity of implementing stronger cybersecurity controls and establishing a dedicated IT risk management structure to ensure continuous monitoring and

The study's primary limitation lies in the use of a single expert validator, which may constrain the generalizability of results. Future research should involve multiple stakeholders and adopt real-time data collection to enhance the robustness and cross-institutional applicability of the proposed framework.

Declarations

Author Informations

Lailatul Maulida ✉

Corresponding Author

Affiliation: Department of Information Systems, Faculty of Science and Technology, State Islamic University of Sunan Ampel Surabaya, Indonesia.

Contribution: Data Curation, Formal analysis, Visualization,

Writing - Original Draft, Writing - Review & Editing.

Conflict of Interest

The author declares no conflicting interest.

Data Availability

The unpublished data is available upon request to the corresponding author.

Ethics Statement

Not applicable.

Funding Information

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Supplemental Material

Supplementary data can be accessed at the following link: <https://etflin.com/file/document/202508140232282080064492.docx>

References

1. Herdono I, Swastika GLD, Shwari EJA, Anissa MD, Nabilla BF. Dhoho TV management policy. In: 2023. p. 355–63.
2. Subekti P. Internet and social change in rural Indonesia: from development communication to communication development in decentralized Indonesia. Springer VS; 2021. 341 p.
3. Harmonis H, Shabana A. Risk management of broadcasting media in Indonesia. ProTVF. 2022 Sep 29;6(2):185–201.
4. Malik M. Securing next-generation broadcast media enterprises against cyberthreats [Internet]. 2023.
5. Televisi Republik Indonesia. Peraturan Dewan Direksi Televisi Republik Indonesia No. 35 Tahun 2018. Jakarta; 2018 Sep.
6. Janah N, Mayesti N. Maturity model matrix of information governance in the Republic of Indonesia public television broadcasting institution: a technical note. Aust Account Bus Financ J. 2020 Feb;14(1):97–104.
7. Sermhattakit A, Sae-Lim P. Key risks and mitigation strategies in enterprise risk management for private hospitals: a mixed-method study. Inquiry. 2025 May 13;62.
8. Kurniawan MF, Salma TD. Risk management evaluation based on ISO/IEC 27005 framework: a case study of ABC Company IT workshop room. Int J Softw Eng Comput Sci. 2025 Aug 1;5(2).
9. Saudi Y, Rahmawati E. The urgency of digital broadcasting for public interest to get quality broadcasting services. Komunike. 2023;15(1).
10. Trimono T, Fahrudin TM, Ardiani AE. Prediction of loss risk investment on the IDX Indonesia: quantitative approach with VaR and Adj-ES. J Stud Manaj Organ. 2025 Jun 12;22(1).
11. Rahman Akash T, Esmaeili L. Financial risk analysis and fraud detection trends in Big 4 consulting firms (2020–2025): a data-driven approach. J Adapt Learn Technol. 2025;2(5).
12. Yasirandi R, Fefayosa E, Tarigan B. IT asset assessment using quantitative risk analysis (QRA) method at XYZ Cafe. Ind J Comput. 2021.
13. Chandra NA, Yusuf M. ISO/IEC 27005:2022 standard for website security risk assessment in organizational services. J Comput Sci Inf Technol (CoSciTech). 2022.
14. Ariza Flores VA, Zavala Ascaño G. Quantitative risk analysis framework for cost and time estimation in road infrastructure projects. Infrastructures (Basel). 2025 Jun 5;10(6):139.
15. Padang AGR, Ambarwati A, Setiawan E. Penilaian manajemen risiko TI menggunakan quantitative dan qualitative risk analysis. Sistemasi. 2021 Sep 30;10(3):527.
16. Metin B, Özhan FG, Wynn M. Digitalisation and cybersecurity: towards an operational framework. Electronics (Basel). 2024 Nov 1;13(21).
17. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of COVID-19: a survey. J King Saud Univ Comput Inf Sci. 2022 Nov;34(10):8176–206.
18. Hidayatullah DER, Kunthi R, Harwahyu R. Design and analysis of information security risk management based on ISO 27005: case study on audit management system (AMS) XYZ internal audit department. Int J Electr Comput Biomed Eng. 2024 Sep 30;2(3).
19. Beckley J. Advanced risk assessment techniques: merging data-driven analytics with expert insights to navigate uncertain decision-making processes. Int J Res Publ Rev. 2025 Mar;6(3):1454–71.
20. Kandasamy K, Srinivas S, Achuthan K, Rangan VP. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP J Inf Secur. 2020 Dec 26;2020(1):8.
21. Grünbaum D, Stern ML, Lang EW. Quantitative probing: validating causal models with quantitative domain knowledge. J Causal Inference. 2023 Jul 15;11(1).
22. Joshi NN, Lambert JH. Diversification of infrastructure projects for emergent and unknown non-systematic risks. J Risk Res. 2011 Jun;14(6):717–33.

Additional Information


How to Cite

Lailatul Maulida. Quantitative Risk Analysis of IT Assets in Public Broadcasting: A Case Study at TVRI East Java. *Digital System and Computing*. 2025;1(1):6–12

Publisher's Note

All claims expressed in this article are solely those of the authors and do not necessarily reflect the views of the publisher, the editors, or the reviewers. Any product that may be evaluated in this article, or claim made by its manufacturer, is not guaranteed or endorsed by the publisher. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access

 This article is licensed under a Creative Commons Attribution 4.0 International License. You may share and adapt the material with proper credit to the original author(s) and source, include a link to the license, and indicate if changes were made.