IT Risk Management Analysis Based on ISO 31000 and Bow Tie Analysis (BTA) in Higher Education Institution

B Prasetyo[1], A Salsabila[2], W E Y Retnani[3]

[1-3]Faculty of Computer Science, Universitas Jember, Indonesia

E-mail: beny.pssi@unej.ac.id[1], bilas3746@gmail.com[2], windi.ilkom@unej.ac.id[3]

Abstract. The Division of Applications and Software is a part of the Academic Support Unit (UPA) for Information and Communication Technology at Universitas Jember (UNEJ) or UPA TIK UNEJ. Based on interviews, UPA TIK UNEJ has not yet implemented risk management, leading to recurring issues in their IT services. Risk management is crucial for preventing and mitigating negative impacts that can harm the organization. Additionally, it is a requirement for internal quality management system audits, according to UNEJ Rector's Decision Number 20588/UN25/LL/2018. This study aims to identify, analyze, and assess potential risks in the Division of Applications and Software at UPA TIK UNEJ and to apply Bow Tie Analysis (BTA) to identify preventive and mitigative actions for the highest-rated risks. The approach used is ISO 31000:2018, which provides a comprehensive framework for risk management. The BTA method combines event tree analysis (ETA) and fault tree analysis (FTA) for in-depth risk analysis. The research begins with context establishment through interviews, followed by risk identification, analysis, assessment, and mitigation. The results show 21 risks identified in developing information systems or applications. The top three priority risks are coded R02, R04, and R19. The second priority includes 17 risks, and the third priority includes 1 risk.

Keywords: Risk Management; ISO 31000; Bow Tie Analysis; UPA TIK UNEJ; Risk Mitigation

1. Introduction

Organizational risk refers to the possibility of events impacting the achievement of goals, either negatively or positively[1]. Risks can arise from various sources, such as regulatory changes, economic shifts, internal and external crime, natural disasters, and other factors[2-3]. As a higher education institution, Universitas Jember (UNEJ) also faces various risks that require effective management. UNEJ has the Academic Support Unit for Information and Communication Technology (UPA TIK UNEJ), which is responsible for providing IT services to the academic community. One of the divisions within UPA TIK UNEJ is the Division of Applications and Software, which provides, enhances, and manages information and communication systems[4].

Interviews indicate that UPA TIK UNEJ has not yet implemented IT risk management. This highlights the need to apply risk management practices to minimize losses and prevent negative impacts that may hinder academic services. For instance, service disruptions or services that do not meet user needs. Therefore, UPA TIK UNEJ needs to implement risk management to optimize academic services and meet the internal quality management system audits requirements at UNEJ.

Previous research underscores the importance of risk management in various contexts. Emphasizes the significance of risk management in construction projects to avoid time, cost, and quality deviations that can harm entities and the economy [5], risk management to make decisions and manage risks in higher education institutions [6], and applied risk management to prevent and mitigate fire hazards in storage buildings [7].

The ISO 31000:2018 framework can be utilized to analyze risk management[8]. ISO 31000:2018 provides practical and integrated guidelines for identifying, evaluating, and managing risks, with a broad scope of application [9]. However, this method has limitations in in-depth analysis, thus, the Bow Tie Analysis (BTA) method is employed [10], [11]. BTA combines event-tree analysis (ETA) and fault-tree analysis (FTA) methods, providing a visualization of the relationship between risks and their consequences (ETA) and the relationship between causes and risks (FTA) [11]. This study analyzes the risks and controls in the Division of Applications and Software of UPA TIK UNEJ through the standard operating procedure (SOP) for submitting, creating, and developing systems or applications.

2. Research Method

The research methodology employs ISO 31000 to identify, assess, and control using an organization's structured and integrated approach[12]. In contrast, Bow Tie Analysis (BTA) demonstrates and analyzes cause-and-effect relationships among high-risk scenarios and provides overview of the connections between causes, hazards, consequences, and controls [10].

This study employs a mixed methods approach. The mixed methods research design collects, analyzes, and integrates quantitative and qualitative methods in a series of studies to understand complex research problems [13]. In this research, the quantitative method is utilized for the risk assessment process, while the qualitative method is employed to gather data and analyze risks[14]. In Figure 1, depicts the research methodology flow of this study.

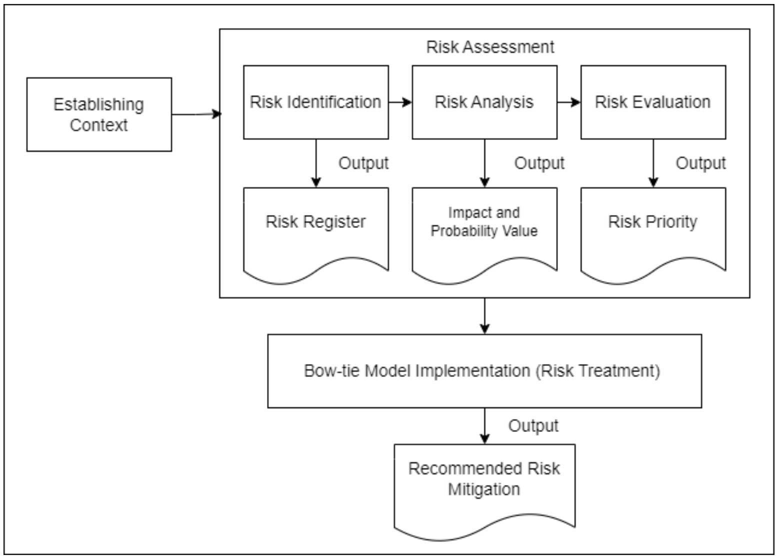

Figure 1. Research flow diagram

2.1. Establishing Risk Context

Refers to Figure 1, risk management begins with establishing the risk context, understanding the environment in which risks occur, and determining the scope and relevant parameters for risk analysis [15]. By establishing the risk context, an organization can ensure its risk analysis is targeted and relevant to its strategic objectives. Information regarding context establishment can be found in Table 1.

Table 1. Risk Context Information

Risk Context Determination	**Information**
General Information Inventory	The aim is to understand the general application of risk management in the Software and Application Division, focusing on its duties, functions, mission, and vision.
Determination of Risk Management Implementation Scope	This study aims to establish the scope of risk management implementation. Specifically, it focuses on the Standard Operating Procedures (SOP) for submitting, creating, and developing systems or applications.
Stakeholder Identification	The aim is to identify the stakeholders responsible for each Standard Operating Procedure (SOP) to obtain information and data regarding potential risks that may occur, as well as the initial steps that have been previously taken.
Assignment of Risk Category	The aim is to ensure that risk analysis, identification, and evaluation are conducted accurately and are tailored to the internal and external situations. Risk categories assist in grouping risks based on severity and help prioritize the necessary mitigation actions.
Risk Impact Determination	The purpose is to identify risk-affected areas by considering internal and external conditions.
Establishment of Risk Criteria	The purpose is to evaluate and determine potential risk events' probability and impact levels. Risk criteria are established in two main parts: assessing the likelihood of occurrence and determining the impact of the risk event.
Risk Analysis Matrix	The objective is to measure and identify the magnitude of risk in numerical values. Once the risk has been assessed using an analysis matrix, it is categorized into risk levels based on the matrix column's color and the combination of likelihood and impact.

2.2. Risk Identification

The risk identification phase aims to recognize and document potential risks that may occur within the business processes of service requests to develop and create systems or applications. Risk identification seeks to generate a comprehensive list of risks based on possible occurrences, causes, and impacts of these risks, which could potentially delay the achievement of organizational objectives[16]. The risk identification process is conducted through interviews and analyses based on the specific categories of risks that need to be identified.

2.3. Risk Analysis

Risk analysis attempts to understand risks in detail, contributing to assessing risks identified in the previous stage[17]. This assessment is conducted based on organizational records, the frequency of risk occurrences, and the impact of those risks on the SOP for service requests in developing and creating systems or applications within the Software and Applications Division. The risk analysis is performed by combining qualitative and quantitative analyses, with the results being grouped according to risk levels derived from interviews and literature reviews.

2.4. Risk Evaluation

The objective of risk evaluation is to support decision-making regarding risk management and to prioritize the risks that have been identified and analyzed [18]. This includes determining whether these risks require mitigation efforts, based on the established risk appetite. Risk evaluation also involves setting priorities for risk management efforts.

2.5. Risk Treatment

Risk treatment is undertaken after assessing and evaluating each identified risk. Following this, a risk response is formulated to manage identified risks[19]. Once risk assessment has been completed and top event risks have been identified, visualization is conducted using Bow Tie Analysis (BTA). This process illustrates the relationship between causes, top events, and the impact of risks, as well as prevention and mitigation measures. The first step in the BTA process is to identify potential hazards that may arise. Subsequently, top events that signify the loss of control over these hazards are determined. This process involves identifying the root causes of emerging threats, which are recorded on the left side of the diagram, while the right side depicts the impact or consequences of the top hazard event. After identifying the causes and impacts of the top hazard event, the next step is to identify preventive actions that can avoid the causes and reduce their impacts. These preventive efforts, known as barriers, consist of two types: preventive barriers aimed at preventing the occurrence of causes and recovery barriers aimed at mitigating the impact of the top hazard event that has occurred. However, preventive actions may be obstructed by other occurrences known as escalation factors (EF). Suppose EFs are identified on one or both sides of the diagram. In that case, the next step is to identify EF barriers using a similar approach to identifying cause and impact barriers, depending on the context of the EF found. EF barriers may include measures such as reducing potential hazards, enhancing the effectiveness of risk mitigation, or implementing changes to external factors that influence the risk impact[20-21].

2.6. Risk Mitigation

Risk mitigation is developing and implementing risk management strategies within the Application and Software Division of UPA TIK UNEJ to reduce the impact and likelihood of risks occurring. Risk mitigation aims to control risks by minimizing their impact, decreasing their probability, or managing them to prevent significant harm to the organization[22].

3. Result and Discussion

Risk identification was achieved through analysis and interviews with stakeholders involved in the business process of system or application development and submission services. A total of 21 risks with significant potential were identified, which could disrupt the operation of the system or application development and submission services and impede the achievement of organizational goals.

At the identification stage, there are several risk categories: HR knowledge, IT infrastructure, HR performance, user requirements, data and information, finance, security, operations, communication and software testing. The results of the risk identification are explained in Table 2.

Table 2. Risk identification

Risk ID	Risk Name	Causes	Impact	Category
R01	SIKD System Error	1. Operational disruption 2. System instability 3. Service disruption and *downtime*	1. The occurrence of errors or bugs in the SIKD system 2. Delay in document delivery 3. Occurrence of data loss	IT Infrastructure

Risk ID	Risk Name	Causes	Impact	Category
			4. Non-delivery of files	
R02	Objectives Not Clearly Defined in the Development document	1. Lack of Development Needs Analysis 2. Submitted documents do not fully describe the purpose of system development.	1. Difficulty in measuring project success 2. Difficulty in understanding the system to be developed 3. Rejection of development proposal	HR Knowledge
R03	Rejection of system development proposal	1. Mismatch of system development needs 2. Not in line with existing development priorities	1. Dissatisfaction among stakeholders 2. Failure to implement innovations that may be beneficial to the organization 2. Decreased productivity and quality of work 3. Decreased team spirit and motivation	User Requirement
R04	Response Existing Stakeholders	1. Stakeholders take a long time to prepare system development documents 2. Poor communication between teams	1. Hindering the implementation of system development 2. Delay in system development	HR Performance
R05	SOP documents are not in accordance with system development needs	1. Stakeholders do not create SOP in accordance with development needs 2. SOP that are made inconsistent with organizational policies	1. SOP created are not in line with development needs 2. SOP created lack incompatibility with organizational policies.	Human Error
R06	Non-acceptance of System Development Materials	1. No consultation with develop during system development 2. Inability to convey the value or benefits of SOP and development materials 3. Misunderstanding in analyzing system development materials	1. Delay in development implementation 2. Failure to implement development	Communication
R07	Poorly Explained System Requirements	1. Ineffective communication between stakeholders and the development team 2. Lack of understanding of system requirements	1. Compilation of solutions that do not match or do not meet expectations 2. Risk of uncontrolled changes in demand 3. Lack of clarity in prioritizing needs	Communication

Risk ID	Risk Name	Causes	Impact	Category
			4. Difficulty analyzing abstract needs 5. Needs that are not well identified 6. Errors in system development	
R08	Uncontrollable Changes in Needs	1. Changes in regulation or policy 2. Lack of system requirements analysis 3. Lack of change management plan	1. Project implementation that is not on time 2. Occurrence of project complexity 3. The team struggled with project planning 4. Increased team workload	Operational
R09	Lack of System Requirements Data Validation	1. Lack of data collection 2. Lack of data sources and data standardization 3. Lack of communication between teams	1. Mismatch with User Needs 2. Errors in decision-making 3. Implementation errors in system creation	Document Management
R10	Lack of Compliance with Safety Standards	1. Lack of attention to safety aspects 2. Lack of data encryption 3. Lack of strong authentication 4. No effective backup system 5. Lack of access restrictions 6. Lack of adequate security testing 7. No effective auditing and monitoring	1. Undetected security vulnerabilities 2. Loss of critical data or information due to cyberattacks, leaks, or data protection failures 3. Easily exposed to malware or ransomware attacks 4. High cost to restore and repair the system 5. Inability to Protect Confidential or Proprietary Data 6. Service interruption	Security
R11	The System Created is Not in accordance with User Needs	1. Lack of effective communication 2. Lack of clarity in the collection and interpretation of user requirements information 3. Lack of testing and verification with users	1. User dissatisfaction 2. Users are uncomfortable and difficult in using the system 3. Mismatch between functional requirements and user expectations	User Requirement
R12	Inability to Perform Backup and Restore	1. Lack of good backup planning	1. Data loss	IT Infrastructure

Risk ID	Risk Name	Causes	Impact	Category
		2. Disruption of the data return process in the database	2. Unexpected downtime 3. Ineffective recovery	
R13	Maintenance and Update Difficulties	1. Complex database 2. Does not have a documented maintenance and update process 3. Too infrequent updates	1. Poor database performance 2. Difficulty updating new functionality or features 3. Difficulty in integration with new technology 4. Decrease in service quality	IT Infrastructure
R14	Delay in Development	1. Long stakeholder response 2. Changing needs 3. Unexpected project complexity 4. Limited resources	1. Delay in project implementation 2. Increased project cost 3. Uncertainty in the planning of other projects	Operational
R15	System Testing Imperfections	1. Lack of system test coverage	1. Incomplete or insufficient testing 2. No bugs or issues detected 3. Increase the risk of failure in production 4. Not able to measure system performance 5. Increased downtime 6. Service interruption	Software Testing
R16	Imperfections in Checking System Testing Results	1. Lack of clarity on system checking criteria 2. Lack of expertise in system testing 3. High complexity of the system or application	1. Undetected error 2. Ineffective testing 3. System bug deployment 4. Occurrence of security threats	HR Performance
R17	Increased Maintenance Costs	1. Lack of maintenance planning	1. Maintenance costs to fix bugs or problems increase 2. Limitations of the development plan	Operational
R18	Delays in repair	1. Lack of planning or inadequate resource allocation to address system improvements	1. Delayed project completion time	Operational
R19	Service Interruption	1. Software or hardware issues	1. Operational disruption (downtime)	IT Infrastructure

Risk ID	Risk Name	Causes	Impact	Category
		2. System configuration error 3. Network or server overload 4. Lack of testing	2. System instability 3. Data loss 4. User dissatisfaction	
R20	Security Breach by user	1. Lack of two-factor authentication 2. Non-conformance with security policy 3. Use of unsafe hardware or software	1. Occurrence of security issues 2. Loss of important data	Security
R21	Waiver of Updates or Upgrades	1. Not understanding the importance of renewal 2. Discomfort or change resistance 3. Disagreement or mismatch with design changes 4. Lack of information or communication	1. Use of versions that are outdated or prone to security issues 2. Data loss or corruption 3. Functional mismatch 4. Operational disruption	HR Knowledge

The next step involves determining the risk values by assigning scores to both likelihood and consequence based on interviews with stakeholders involved in the business process. This process considers the probability and impact of each risk[23-24]. Following the assessment of likelihood and consequence, the risk exposure value (risk significance level) is calculated by summing the scores for likelihood and consequence. The criteria for assessing likelihood are explained in Table 3, while the criteria for assessing consequence are detailed in Table 4.

Table 3. Likelihood value criteria

Value	criteria	Description	frequency of occurrence
1	*Rare*	Not likely to happen	(> 4) year
2	*Unlikely*	The probability of occurrence is small	(2 - 3) year
3	*Possible*	Risk may occasionally occur	(1 - 2) year
4	*Likely*	Risk of frequent occurrence	(7 - 12) month
5	*Certain*	Almost certainly can occur	(1 - 6) month

Table 4. Consequence value criteria

Value	criteria	Description
1	*Insignificant*	Risk has no impact on the course of business process activities
2	*Minor*	Risks begin to impact business process activities with slight non-achievement of goals and performance.

Value	criteria	Description
3	*Moderate*	Risk of partial obstruction of business process activities with delays in achievement and performance against targets
4	*Major*	Risk disrupts almost all business process activities and can delay the achievement of goals and targets that are far below target
5	*Catastrophic*	The risk of disrupting all business process activities and failing to achieve goals and performance.

Table 5 presents the results of the risk assessment conducted for each identified risk in the business processes related to the service requests for creating and developing information systems or applications. These risks have been mapped into a risk matrix.

Table 5. Risk assessment

Risk ID	Risk Name	Risk Impact	Probability	Risk Exposure
R01	SIKD System Error	4	3	7
R02	Objectives Not Clearly Defined in the Development document	4	4	8
R03	Rejection of system development proposal	3	2	5
R04	Response Existing Stakeholders	4	4	8
R05	SOP documents are not in accordance with system development needs	4	2	6
R06	Non-acceptance of System Development Materials	4	2	6
R07	Poorly Explained System Requirements	4	2	6
R08	Uncontrollable Changes in Needs	4	3	7
R09	Lack of System Requirements Data Validation	3	2	5
R10	Lack of Compliance with Safety Standards	5	2	7
R11	The System Created is Not in accordance with User Needs	4	2	6
R12	Inability to Perform Backup and Restore	4	1	5
R13	Maintenance and Update Difficulties	4	2	6
R14	Delay in Development	4	3	7
R15	System Testing Imperfections	5	2	7
R16	Imperfections in Checking System Testing Results	4	2	6
R17	Increased Maintenance Costs	2	1	3
R18	Delays in repair	4	2	6
R19	Service Interruption	5	4	9
R20	Security Breach by user	3	3	6
R21	Waiver of Updates or Upgrades	3	2	5

After conducting a risk assessment by determining the values of likelihood and consequence, the risks are mapped into a risk matrix, as shown in Table 6. The risk matrix is a tool used to visualize the level of risk based on these two parameters, and it helps determine the priority for risk handling[25-26].

Table 6. Institutional Risk Map

Consequence / Likelihood		Insignificant	Minor	Moderate	Major	Catastrophic
		1	**2**	**3**	**4**	**5**
Rare	**1**	🟩	🟩 R17	🟩	🟩	🟨
Unlikely	**2**	🟩	🟩	🟨 R03, R09, R21	🟨 R05, R06, R07, R11, R12, R13, R16, R18	🟨 R10, R15
Possible	**3**	🟩	🟨	🟨 R20	🟨 R01, R08, R14	🟥
Likely	**4**	🟩	🟨	🟨	🟥 R02, R04	🟥 R19
Certain	**5**	🟨	🟨	🟥	🟥	🟥

After the risk assessment, a risk evaluation is conducted. Based on interview data and brainstorming sessions, this stage determines the priority of risks to be addressed. There are three levels of risk based on their significance: high risk (red), moderate risk (yellow), and low risk (green)[27], [28]. If a risk is categorized as high risk, mitigation measures must be implemented immediately. For moderate risk, mitigation processes are prioritized next after addressing extreme risks. Meanwhile, risks classified as low risk are addressed last or may be accepted (accepted) due to their unavoidability or minimal impact[26].

The priority risks in the Software and Applications Division of UPA TIK UNEJ include three identified risks, namely those with risk codes R02, R04, and R19. Meanwhile, the second priority handling includes a list of 17 risks, and the third priority risk handling consists of a list of 1 risk.

Subsequently, the risk treatment phase was conducted using the Bow Tie Analysis (BTA) method. From the risk assessment results, the highest-rated risks or top events identified include R02 (Objectives Not Clearly Defined in the Development Document), R04 (Response of Existing Stakeholders), and R19 (Service Interruption). The BTA visualization for risk R02 can be seen in Figure 2, the BTA visualization for risk R04 in Figure 3, and the BTA visualization for risk R19 in Figure 4. The BTA diagram illustrates the causes and preventive measures on the left side, and the impacts and mitigation strategies on the right side. Both sides are susceptible to escalation factors due to disorder or failure in prevention and mitigation. Escalation factors must be addressed through escalation controls.

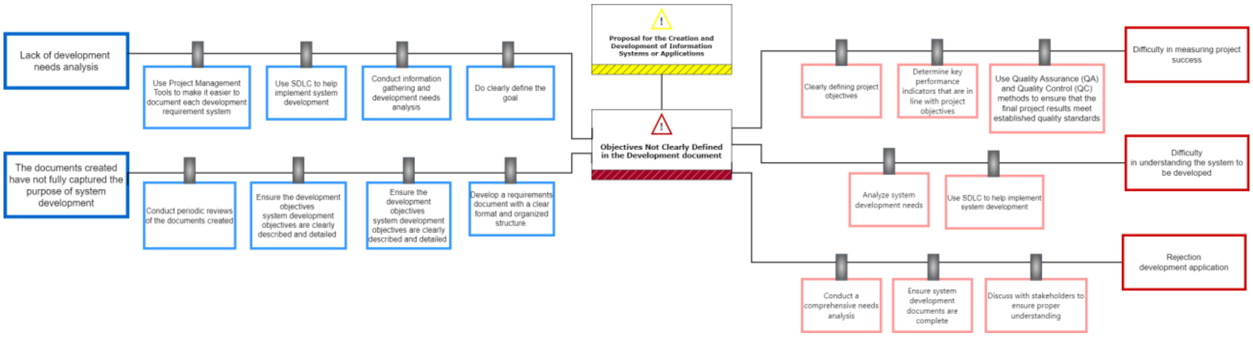
Lack of development needs analysis
Use Project Management Tools to make it easier to document each development requirement system
Use SDLC to help implement system development
Conduct information gathering and development needs analysis
Do clearly define the goal
The documents created have not fully captured the purpose of system development
Conduct periodic reviews of the documents created
Ensure the development objectives system development objectives are clearly described and detailed
Ensure the development objectives system development objectives are clearly described and detailed
Develop a requirements document with a clear format and organized structure.
Proposal for the Creation and Development of Information Systems or Applications
Objectives Not Clearly Defined in the Development document
Clearly defining project objectives
Determine key performance indicators that are in line with project objectives
Use Quality Assurance (QA) and Quality Control (QC) methods to ensure that the final project results meet established quality standards
Difficulty in measuring project success
Analyze system development needs
Use SDLC to help implement system development
Difficulty in understanding the system to be developed
Conduct a comprehensive needs analysis
Ensure system development documents are complete
Discuss with stakeholders to ensure proper understanding
Rejection development application

Figure 2. Application of Bow Tie Analysis at the risk treatment stage of R02 Objectives Not Clearly Defined in the Development document

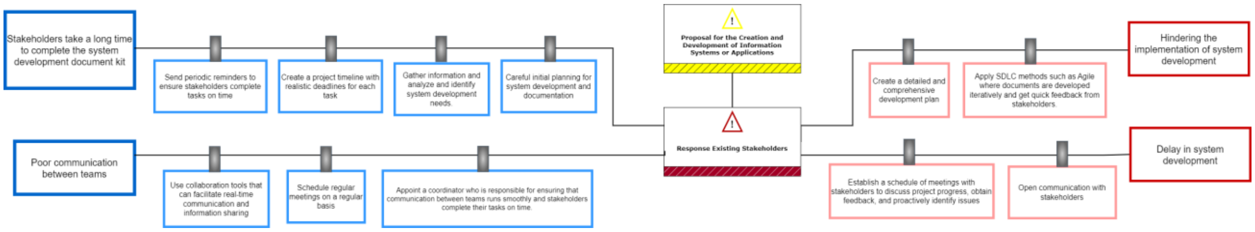
Stakeholders take a long time to complete the system development document kit
Send periodic reminders to ensure stakeholders complete tasks on time
Create a project timeline with realistic deadlines for each task
Gather information and analyze and identify system development needs.
Careful initial planning for system development and documentation
Poor communication between teams
Use collaboration tools that can facilitate real-time communication and information sharing
Schedule regular meetings on a regular basis
Appoint a coordinator who is responsible for ensuring that communication between teams runs smoothly and stakeholders complete their tasks on time.
Proposal for the Creation and Development of Information Systems or Applications
Response Existing Stakeholders
Create a detailed and comprehensive development plan
Apply SDLC methods such as Agile where documents are developed iteratively and get quick feedback from stakeholders.
Hindering the implementation of system development
Establish a schedule of meetings with stakeholders to discuss project progress, obtain feedback, and proactively identify issues
Open communication with stakeholders
Delay in system development

Figure 3. Application of Bow Tie Analysis at the risk treatment stage of R04 Response Existing Stakeholders

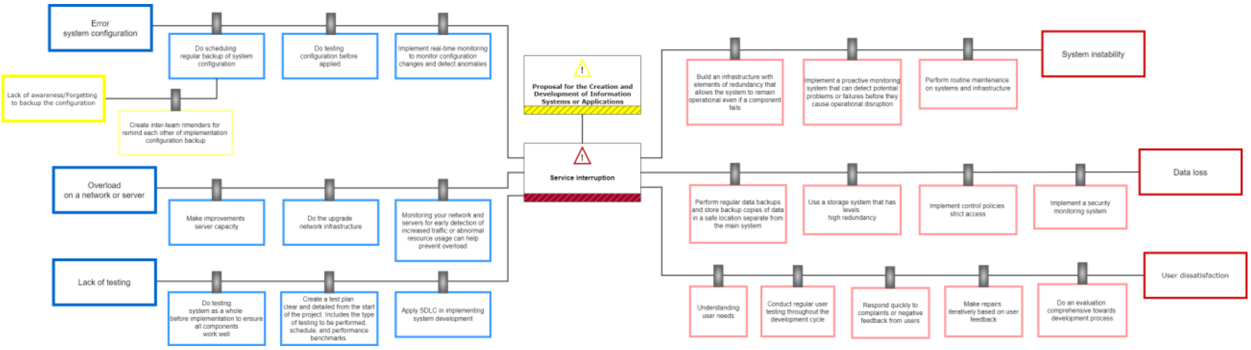
Error system configuration
Do scheduling regular backup of system configuration
Do testing configuration before applied
Implement real-time monitoring to monitor configuration changes and detect anomalies
Lack of awareness/Forgetting to backup the configuration
Create inter-team rimenders for remind each other of implementation configuration backup
Overload on a network or server
Make improvements server capacity
Do the upgrade network infrastructure
Monitoring your network and servers for early detection of increased traffic or abnormal resource usage can help prevent overload
Lack of testing
Do testing system as a whole before implementation to ensure all components work well
Create a test plan clear and detailed from the start of the project. Includes the type of testing to be performed, schedule, and performance benchmarks.
Apply SDLC in implementing system development
Proposal for the Creation and Development of Information Systems or Applications
Service interruption
Build an infrastructure with elements of redundancy that allows the system to remain operational even if a component fails
Implement a proactive monitoring system that can detect potential problems or failures before they cause operational disruption
Perform routine maintenance on systems and infrastructure
System instability
Perform regular data backups and store backup copies of data in a safe location separate from the main system
Use a storage system that has levels high redundancy
Implement control policies strict access
Implement a security monitoring system
Data loss
Understanding user needs
Conduct regular user testing throughout the development cycle
Respond quickly to complaints or negative feedback from users
Make repairs iteratively based on user feedback
Do an evaluation comprehensive towards development process
User dissatisfaction

Figure 4. Application of Bow Tie Analysis at the risk treatment stage of R19 Service Interruption

4. Conclusion

This study conducted a risk management analysis for the Division of Applications and Software within the Unit for Academic Support in Information Technology and Communication (UPA TIK UNEJ), which provides information technology services to the academic community of UNEJ. 53 risks were identified within the business processes related to creating and developing information systems or applications. The top three priority risks are those coded R05, R11, and R48, while the second priority handling includes 24 risk items, and the third priority handling encompasses 26 risk items.

IT risk management fosters awareness of risks within the Division of Applications and Software, thus helping to prevent and mitigate negative impacts that could harm the organization. The use of the comprehensive ISO 31000:2018 framework and the Bow Tie Analysis (BTA) method, which combines Event Tree Analysis (ETA) and Fault Tree Analysis (FTA), provides a clear and in-depth understanding of the risks faced and their mitigation strategies. However, the study also has limitations, including the lack of implementation of the recommended mitigation actions and the absence of long-term effectiveness evaluation.

Future development should focus on implementing and monitoring the effectiveness of the identified mitigation actions and revising and adjusting risk management practices periodically to enhance the effectiveness and efficiency of IT services at UPA TIK UNEJ. Additionally, risk management should be extended to other divisions within UPA TIK UNEJ, and training and awareness programs regarding the importance of risk management should be implemented across all divisions to optimize the risk management process.

References

[1] G. H. S. Rampini, H. Takia, and F. T. Berssaneti, “Critical success factors of risk management with the advent of ISO 31000 2018 - Descriptive and content analyzes,” in *Procedia Manufacturing*, Elsevier B.V., 2019, pp. 894–903. doi: 10.1016/j.promfg.2020.01.400.

[2] T. George and D. Nurhadi, “Manajemen Risiko Pada Bandara Soekarnao Hatta Berbasis ISO 31000.” *Indonesian Journal of Information Systems and Informatics*, vol. 1, no. 2, pp. 23-35, 2020.

[3] P. P. Thenu, A. F. Wijaya, C. Rudianto, U. Kristen, and S. Wacana, “Analisis Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 (Studi Kasus: PT Global Infotech),” Salatiga, Indonesia, 2020, doi: 10.33557/binakomputer.v2i1.799.

[4] UPT TI, “Tugas pokok dan Rencana Strategis UPT Teknologi Informasi Tahun 2016-2020. Universitas Jember,” 2016.

[5] S. H. N. Alani, “Managing the corruption risk at the operation and maintenance stage in the construction projects in Iraq,” *Innovative Infrastructure Solutions*, vol. 7, no. 1, Feb. 2021, doi: 10.1007/s41062-021-00710-x.

[6] H. Argadinata, B. B. Wiyono, A. Imron, Mustiningsih, and Moch. F. Pramudya, “Identifying Risks Based on ISO 31000:2018 Using Risk Factors at Public Universities of Legal Entities,” *in Proceedings of the International Conference on Risk Management* (ICRM), 2023, pp. 43–60, doi: 10.2991/978-2-38476-156-2_7.

[7] L. Ding, F. Khan, and J. Ji, “Risk-based safety measure allocation to prevent and mitigate storage fire hazards,” *Process Safety and Environmental Protection*, vol. 135, pp. 282–293, Mar. 2020, doi: 10.1016/j.psep.2020.01.008.

[8] I. F. Creed, P. N. Duinker, J. N. Serran, and J. W. N. Steenberg, “Managing risks to Canada’s boreal zone: Transdisciplinary thinking in pursuit of sustainability1,” 2019, *Canadian Science Publishing*. doi: 10.1139/er-2018-0070.

[9] Ivan Lanin, “Standar Baru Manajemen Risiko ISO 31000:2018,” 2020.

[10] A. Alijoyo, Q. B. Wijaya, and I. Jacob, “Bow Tie Analysis Analisis Dasi Kupu-kupu,” Bandung, Indonesia: Risk Management Institute, 2019. [Online]. Available: www.lspmks.id.

[11] B. Bramantio and F. Rachmawati, “Analisis Risiko Kecelakaan Kerja Menggunakan Metode Bowtie pada Proyek The Grandstand Surabaya,” *Jurnal Teknik ITS*, vol. 10, no. 2, pp. D170–D175, 2021.

[12] SNI ISO 31000:2011, “Standar Nasional Indonesia Manajemen risiko-Prinsip dan pedoman Risk management-Principles and guidelines Badan Standardisasi Nasional.”

[13] N. Ivankova, J. Creswell, and S. Stick, “Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice,” *Field methods*, vol. 18, pp. 3–20, Feb. 2006, doi: 10.1177/1525822X05282260.

[14] M. I. Fachrezi, A. Dwika Cahyono, and P. F. Tanaem, “Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga,” *Jurusan Sistem Informasi*, vol. 8, no. 2, 2021, [Online]. Available: http://jurnal.mdp.ac.id

[15] R. Fahlepi *et al.*, “Analisis Manajemen Risiko IT Pada Sistem Informasi Akademik Menggunakan ISO 31000,” 2023.

[16] M. Miftakhatun, “Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000,” *Journal of Computer Science and Engineering (JCSE)*, vol. 1, no. 2, pp. 128–146, Aug. 2020, doi: 10.36596/jcse.v1i2.76.

[17] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, “Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ,” *JURIKOM (Jurnal Riset Komputer)*, vol. 7, no. 1, p. 91, Feb. 2020, doi: 10.30865/jurikom.v7i1.1791.

[18] V. Patrick, P. Wijaya, and A. D. Manuputty, “Manajemen Risiko Teknologi Informasi Pada BTSI UKSW Menggunakan ISO 31000:2018,” vol. 9, no. 2, pp. 1295–1307, 2022.

[19] L. E. Hutagalung, “Analisa Manajemen Risiko Sistem Informasi Manajemen Rumah Sakit (SIMRS) Pada Rumah Sakit XYZ Menggunakan ISO 31000,” *in Proceedings of the 5th International Conference on Health Informatics* (ICHI), 2022.

[20] K. Mokhtari, J. Ren, C. Roberts, and J. Wang, “Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals,” *J Hazard Mater*, vol. 192, no. 2, pp. 465–475, Aug. 2011, doi: 10.1016/j.jhazmat.2011.05.035.

[21] F. Aqlan and E. Mustafa Ali, "Integrating lean principles and fuzzy bow-tie analysis for risk assessment in chemical industry," *J Loss Prev Process Ind*, vol. 29, no. 1, pp. 39–48, 2014, doi: 10.1016/j.jlp.2014.01.006.

[22] H. I. Pribadi and E. Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)," *JURNAL SISTEM INFORMASI BISNIS*, vol. 10, no. 1, pp. 28–35, May 2020, doi: 10.21456/vol10iss1pp28-35.

[23] W. Peeters and Z. Peng, "An Approach Towards Global Standardization of the Risk Matrix," *Journal of Space Safety Engineering*, vol. 2, no. 1, pp. 31–38, Jun. 2015, doi: 10.1016/S2468-8967(16)30037-4.

[24] A. N. Rahmatika, M. Fajar Apriyadi, M. A. Kahfi, and N. Aibi, "ANALISIS MANAJEMEN RISIKO TEKNOLOGI INFORMASI PADA SISTEM INFORMASI AKADEMIK (SIAK) UNIVERSITAS MUHAMMADIYAH SUKABUMI (UMM) MENGGUNAKAN ISO 31000," *Jurnal Manajemen dan Teknologi Informasi (JMTI)*, vol. 14, pp. 48–57, doi: 10.59819.

[25] S. Sidik, S. Tinggi Manajemen Asuransi, and J. A. Jend Yani Kav, "Manajemen Risiko Sistem Informasi Ujian Secara Daring Di Sekolah Tinggi Manajemen Asuransi Trisakti," *Growth dan Manajemen Lingkungan*, vol. 12, no. 1, 2022, doi: 10.21009/jgg.121.06.

[26] N. N. Setyaningrum and E. Maria, "PENERAPAN ISO 31000:2018 UNTUK MANAJEMEN RISIKO PADA SISTEM INFORMASI SEKOLAH TERPADU," 2024.

[27] D. P. Natalie and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi dengan ISO 31000:2018 pada PT Bayu Buana Tbk," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 5, p. 1290, Oct. 2022, doi: 10.30865/jurikom.v9i5.4797.

[28] W. Peeters and Z. Peng, "An Approach Towards Global Standardization of the Risk Matrix," *Journal of Space Safety Engineering*, vol. 2, no. 1, pp. 31–38, Jun. 2015, doi: 10.1016/S2468-8967(16)30037-4.