International Journal of Asian Business and Management (IJABM)
Vol.4, No.4, 2025: 825-844

Risk Analysis and Mitigation with House of Risk on Supply Chain of Internet Service Provider Start-up Company

Muhammad Riandi[1*], Ratih Hendayani[2]
Universitas Telkom, Bandung
Corresponding Author: Muhammad Riandi ndiriandim@gmail.com

A R T I C L E I N F O

Keywords: Risk Managemenet, Internet Service Provider, Supply Chain

Received: 18 June
Revised : 17 July
Accepted: 2 August

A B S T R A C T

PT. Radja Telcon Utama, an internet service provider company, encounters the possibility of disruption and uncertainty in its supply chain. This research aims to analyze and develop a risk mitigation plan to minimize or eliminate potential disruptions within the company's supply chain. The mapping and analysis are conducted using the Supply Chain Operations Reference model and House of Risk methodology. Primary data was collected through interviews. The qualitative data obtained were then analyzed using data reduction, data display and conclusion drawing techniques. The validity of the data was ensured using triangulation method. Based on the result of this research, a total of 27 risk events were identified, originating from 29 risk agents, of which 14 risk agents were prioritized to be mitigated. It is recommended for the company to implementing mitigation actions which have been identifed that can serve as a strategic reference for the company in managing supply chain risks

DOI: https://doi.org/10.55927/ijabm.v4i4.432
ISSN-E: 2964-3651
https://mryformosapublisher.org/index.php/ijabm

INTRODUCTION

The quality of internet services is a critical determinant of consumer trust, satisfaction, and commitment within the internet service industry (Thaichon & Quach, 2015). The primary factors influencing consumer volatility in internet subscriptions include service reliability, connection speed, affordability, round-the-clock technical support, and the availability of value-added assistance (Naji et al., 2023). To effectively address these demands, it is crucial for PT. RTU to maintain a robust and responsive supply chain to ensure that its services are consistently delivered.

PT. RTU, like many other internet service providers, has encountered several instances of service disruptions, leading to temporary interruptions in network availability. The severity of these disruptions varies, with some affecting only a segment of customers, while others result in complete service outages. Such incidents inevitably have an impact on customer satisfaction and underscore the need for continuous improvement in company operation.

Fornah and Pujawan (2020) emphasize that the overall performance of a telecommunications company is closely linked to the strength of its supply chain. To achieve optimal performance, companies must develop clear and comprehensive strategies for implementing effective supply chain practices. Eliminating quality defects within the supply chain is essential to support sustainable growth and enhance service levels while minimizing costs. These objectives can be realized through the implementation of continuous improvement strategies. To remain competitive in a high-risk business environment, effective supply chain risk management strategies must be implemented. Without proper mitigation, disruptions within the supply chain can lead to costly delays, reduced service levels, and increased operational expenses. Consequently, it is essential for PT. RTU to safeguard its supply chain against potential disruptions and uncertainties to ensure the continuity and reliability of its service.

Based on the risk mitigation research by Hendayani et al. (2021), the Supply Chain Operations Reference (SCOR) model is identified as an effective framework for managing and improving supply chain processes and can also be utilized to systematically describe the structure and flow of supply chain activities. Meanwhile, the House of Risk (HoR) methodology provides a structured approach for risk analysis and mitigation planning, consisting of two sequential phases: the first phase involves the identification and assessment of potential risks, while the second focuses on the development of targeted mitigation strategies based on the evaluated risk priorities. Although the House of Risk (HoR) method has been widely applied in various industries, its utilization within supply chain of Internet Service Provider (ISP) start-ups remains largely unexplored, revealing a significant gap in existing literature.

LITERATURE REVIEW

Supply Chain Management (SCM) is a strategic managerial approach that views the supply chain as an interconnected and holistic system, requiring integration not only among internal functions within an organization but also across multiple companies within the broader supply chain network. The primary objective of SCM is to optimize overall performance, both at the level of individual company and throughout the entire supply chain ecosystem. Achieving this objective requires the implementation of effective managerial practices, including integrated work behaviors, transparent information sharing, proactive risk management, inter-organizational collaboration, alignment with shared goals, and strong customer service orientation. Moreover, process integration and long-term partnerships are essential, as SCM is a key strategy for improving productivity and profitability (Trisnawati & Pujawan, 2021). In business practice, supply chains are inherently exposed to a variety of risks. According to the ISO 31000 Risk Management standard (International Organization for Standardization, 2018), organizations inevitably face operational risks stemming from routine activities, which may include human error, system failures, disruptions in internal processes, as well as external factors involving suppliers or business partners. If inadequately managed, these risks can compromise operational continuity and lead to substantial financial and reputational losses.

In this context, the House of Risk (HoR) presents an effective proactive approach for managing supply chain risks. HoR is a systematic framework designed to identify and mitigate risks in a structured manner. This approach integrates principles from Failure Modes and Effects Analysis (FMEA) and House of Quality (HoQ), enabling organizations not only to comprehensively identify risk agents but also to prioritize mitigation actions based on the severity and likelihood of risk occurrence. By emphasizing preventive measures, HoR facilitates more efficient and effective allocation of resources. Originally developed by Pujawan and Geraldin (2009), the framework has been applied across various industries in many research studies including dairy (Hendayani, 2021), durian cultivation (Jittamai, 2024), food manufacturing (Kristiana,2020) and automotive (Partiwi, 2023)

According to Aldianto et al. (2021), a business entity—particularly a start-up—must understand the necessary precautions and proactively prepare the organization to ensure operational continuity. This includes recognizing its position in terms of business continuity and risk management, with particular attention to critical elements such as personnel, suppliers, and the broader supply chain. The risks encountered by a company can significantly influence the strategies it adopts. One such strategic response is sharing of risk information, as noted by Anggadwita et al. (2019). Recognizing the importance of understanding, managing and sharing such risks particularly in the context of start-up Internet Service Providers, this study was conducted to explore appropriate risk mitigation strategies using the House of Risk framework.

METHODOLOGY

This research has a descriptive objective that aims to describe the characteristics and functions of one or several variables in a situation systematically and accurately. This research uses a qualitative method which approaches to gain an in-depth understanding of a phenomenon or event through descriptive data. The unit of analysis in this study is the company where the researcher focused on analysis of the supply chain business processes carried out by an ISP company.

In this study, the researcher's level of involvement was such that no manipulation or intervention was performed on the data. This research used a non-contrived setting. Information was obtained by interacting directly with people and observing actions in their context. This study was cross-sectional where data was collected over a specific period, then processed, analyzed, and finally, conclusions were drawn.

In this study, structured interviews were employed, utilizing systematic guidelines to ensure consistent and comprehensive data collection. Data were collected from management and employee of the company using source triangulation, which involves obtaining information from multiple sources using the same method. This approach strengthens the validity and reliability of qualitative research findings compared to relying on a single source. The interview questions were designed to elicit comprehensive insights into the company's activities at each stage of the supply chain, as structured by the SCOR framework. Specifically, the questions aimed to gather information on potential risk events associated with each activity, the severity of their impacts, and the corresponding risk agents along with their likelihood of occurrence. Additionally, the interviews explored the relationships between risk events and their triggering agents, possible mitigation strategies, the degree of relevance between each preventive measure and its associated risk agent, and the implementation difficulty of each proposed mitigation step. The qualitative data obtained were analyzed using data reduction, data display and conclusion drawing techniques.

The mapping and analysis of the company's supply chain activities are conducted using the Supply Chain Operations Reference (SCOR) model, which encompasses six core processes: Plan, Source, Make, Deliver, Return, and Enable (Kunrath, 2023). This model is employed as a reference framework due to its capacity to provide a structured representation of company activities in its supply chain, therefore enabling a more focused and systematic approach to risk identification and analysis. By aligning each activity within the supply chain to these well-defined SCOR processes, the company can more effectively identify and trace potential vulnerabilities and implement targeted mitigation strategies. This mapping phase also considers Supply Chain Risk Management, which encompasses both internal and external company risks, reflecting the potential for disruptions from within and outside the organization, and Service Provider Risk Supply Chain Management, which focuses on risks typical of the internet service provider industry, including lost network connections, downtime, unstable internet connections, and decreased internet speeds.

Subsequently, the House of Risk (HoR) method is used as a framework to identify and evaluate risks, and to develop plans and strategies to reduce or prevent those risks from happening. The House of Risk analysis is conducted in the following stages:

- House of Risk Analysis Phase 1

This phase is the initial stage of the analysis, beginning with the identification of risk events that may occur in each activity in the supply chain. This phase also involves analyzing the influence of factors that can cause risk events (risk agents) on the likelihood of risk occurrence. The analysis and discussion process at this stage involves gathering information directly from the company, including historical data, interviews with key stakeholders, and a review of ongoing operational processes. A comprehensive understanding of the root causes and impacts of a risk, reinforced by relevant data collected from the company, allows for the formulation of more targeted and effective mitigation strategies. This understanding serves as the foundation for developing effective action plans to address potential risks and reduce their negative impact on the continuity of ongoing operations.

- House of Risk Analysis Phase 2

This phase involves developing and formulating risk mitigation strategies (preventive actions) based on the findings from the risk identification and evaluation in the previous phase. At this stage, risk mitigation measures are developed by referring to relevant theories and best practices in the existing literature. This process also includes in-depth discussions with relevant stakeholders who have knowledge or interest in the risks faced. The purpose of these discussions is to gain practical insights and perspectives that will be useful in designing effective mitigation strategies. Relevant theories combined with stakeholder input enable the development of a more comprehensive and adaptive mitigation plan, aimed at minimizing the impact of the risks.

RESULT

Model SCOR

The Supply Chain Operations Reference (SCOR) model is applied in this study as a foundational framework due to its capacity to structurally represent end-to-end supply chain activities while supporting a more focused, systematic, and standardized risk analysis process. In the context of the ISP company's operations, supply chain activities are mapped across the six core SCOR processes—Plan, Source, Make, Deliver, Return, and Enable—as follows:

Plan

1. New area development planning
2. Infrastructure and hardware planning
3. Permit and regulatory planning
4. Organizational resource planning

Source

1. Procuring hardware from suppliers
2. Ordering interconnecting bandwidth from Network Access Provider (NAP)
3. Receiving and inspecting hardware components
4. Receiving interconnecting bandwidth services

Make

- Developing and constructing infrastructure
- Device setup and configuration
- Bandwidth configuration
- Installing devices and fiber optics from Point of Presence (PoP) to Optical Distribution Point (ODP)

Deliver

1. Pulling fiber optic cables from ODP to customer premises
2. Installing and configuring Optical Network Terminals (ONTs) at customer sites
3. Conducting performance tests
4. Activating customer accounts and services

Return

1. Receiving and managing customer complaints
2. Handling service disruptions and faults
3. Recalling customer devices upon service termination
4. Deactivating customer accounts

Enable

1. Employee training and capacity development
2. Product and service socialization to customers
3. Implementation of HR and administrative systems
4. Implementation of billing and accounting systems
5. Cybersecurity and data protection management
6. Network performance monitoring

HOR Phase 1

Risk events and agents within the company's supply chain were identified through a detailed mapping of core business processes, guided by the SCOR model. Identification was conducted through structured interviews with company business actors as key informants. Each risk event was assigned a unique identification code prefixed "E" followed by a sequential number. Similarly, each risk agent was coded with prefix"A" followed by a sequential number.

The identified risk events are: Low subscriber growth (E1), Uncompetitive selling price (E2), Difficulties in infrastructure development (E3), Unstable network performance (E4), Work halted indefinitely (E5), Lack of trained and experienced personnel (E6), Out-of-stock inventory (E7), High bandwidth costs from NAP (E8), Defective/damaged goods received (E9), Unstable NAP bandwidth (E10), Isolated NAP bandwidth (E11), Server performance degradation (E12), Active devices fail to power on (E13), Server system is running, but internet service is down (E14), Unstable internet connection (E15),

High signal attenuation in cables (E16), Workplace accidents (E17), Errors in interpreting test results (E18), Delays in new customer installations (E19), Poor network quality during peak traffic (E20), Damage to the main distribution network (E21), Damage to the homepass network (E22), ONT device malfunction (E23), Employees unable to resolve network disruptions (E24), Employee absenteeism (E25), Customer misunderstanding of the services provided (E26), Company data lost (E27).

The identified risk events agents are: Incomplete or inaccurate SITAC data (A1), Presence of competitors in the same coverage area (A2), Challenging area in infrastructure development (A3), Design and device selection errors (A4), Lack of permits from local regulators and stakeholders (A5), Ineffective Human Resource management (A6), Suppliers are unable to fulfil order volumes (A7), Overreliance on a single supplier (A8), Absence of alternative NAPs (A9), Poor Quality Control process in receiving goods (A10), Delays in ordering and delivery process (A11), Inadequate NAP interconnecting bandwidth capacity (A12), Disruption in NAP and backhaul network (A13), Delayed payment to suppliers (A14), Overheating of network devices (A15), Power outages (A16), Environmental factor disruptions (A17), Installation errors (A18), Configuration errors (A19), Main device failure (A20), Cyber attacks (A21), Lack of Occupational Health and Safety training (A22), Inaccurate Optical Power Meter (A23), Work tools in poor condition (A24), Low quality ONT devices (A25), Insufficient technical training (A26), Lack of customers education (A27), Damage to storage media (A28), Lack of proper work tools (A29).

Through the interviews, data were collected regarding the severity level of each risk event (severity, Si), the probability of occurrence for each risk agent (occurrence, Oj), and the relationship strength between risk events and their respective agents (Rij). These values were then used to calculate the Aggregate Risk Potential (ARPj) score which serves to prioritize risks for further mitigation using Equation (1) (Pujawan, 2009).

$$ARP_j = O_j \sum_i S_i R_{ij} \quad (1)$$

A higher ARP score indicates a greater potential impact on operational performance and, therefore, a higher urgency for mitigation. The ARP values derived from each informant are presented in Table 1, Table 2, and Table 3.

Table 1. Informan 1 ARP Result

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29	Severity
E1	9	9																												7
E2	3	9							3																					8
E3			9		3																									7
E4				9																										7
E5	3				9		3	3																					3	7
E6						9																				9				7
E7							9	9			9																			6
E8								3	9																					7
E9										9																				6
E10								3				3	9																	7
E11								3	3				9	9																9
E12															9					9										7
E13										3						9		9		9										9
E14				9									9			9	9	9	9	9	9									9
E15				3								9	9					3		3			3							7
E16																	3	3					3	9						7
E17																						9		9						10
E18																							9							5
E19			3		3	9	3				3			3															3	6
E20												9								3										7
E21																	9	3		9										9
E22																	9	3												6
E23										3									9						9					6
E24						3																				9			9	6
E25						9																								7
E26																											9			5
E27																					9							9		9
Occur.	2	2	2	2	1	3	3	2	1	4	4	6	3	2	2	4	5	5	3	2	6	2	4	3	4	2	3	2	2	
ARP	216	270	162	330	102	594	279	288	114	396	288	882	864	198	126	648	118	124	405	696	972	180	348	459	216	234	135	162	186	

Table 1. Informan 2 ARP Result

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29	Severity
E1	9	3																												7
E2		9																												7
E3	3		9																											7
E4				9																										8
E5	3				9		9										3												3	6
E6						9																				9				7
E7							9	3			9																			7
E8									9																					7
E9										9																				6
E10												3	3																	8
E11								3					9	9																9
E12															9					9										7
E13										3						9		9		9										9
E14				9									9				9		9	9	9									9
E15				9								9	9					3		3			3							7
E16																		3					3							6
E17																						9		9						9
E18																							9							5
E19			3		3	9	3				9			3															3	6
E20												9							3	3										6
E21																	9	3		9										9
E22																	9	9	3											5
E23										9									3						9					6
E24						9																				9			3	6
E25						9																								7
E26																											9			4
E27																					9							9		9
Occur.	2	1	2	3	1	2	2	2	2	4	4	5	4	3	2	5	4	4	3	2	5	2	4	4	2	2	2	2	2	
ARP	204	84	162	648	72	468	270	96	126	540	468	705	996	297	126	405	900	768	396	690	810	162	336	324	108	234	72	162	108	

Table 2. Informan 3 ARP Result

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29	Severity
E1	9																													7
E2		9																												7
E3	3		9																											7
E4				9																										8
E5					9																								3	6
E6						9																				9				6
E7							9	9			9																			6
E8									9																					6
E9										9																				6
E10													9																	7
E11								3	3				9	9																9
E12															9															7
E13										3						9		9		9										9
E14				3									3			9	9		9	9	9									9
E15				9								9	9					9		3			3							8
E16																		3					3	3						6
E17																						9		9						10
E18																							9							6
E19					3	9	3				3			3															3	6
E20												9								3										6
E21																	9	3		9										9
E22																	9	3												6
E23										3									9						9					5
E24						3																				9			9	6
E25						9																								7
E26																											9			4
E27																					9							9		9
Occur	1	2	2	2	1	2	3	2	2	3	4	6	4	2	1	4	5	4	4	2	5	1	3	4	3	2	3	2	3	
ARP	84	126	126	342	72	378	216	162	162	288	288	756	972	198	63	648	1080	864	504	570	810	90	288	432	135	216	108	162	270	

Following the ARP calculation, a risk evaluation was carried out to determine which risk agents should be prioritized. This was achieved using the Pareto 80/20 principle, focusing on agents that contribute to the top 80% of cumulative ARP values as identified by at least two of the three informants.

Based on this evaluation, 14 priority risk agents were identified as requiring immediate mitigation attention: Design and Device Selection Errors (A4), Ineffective Human Resource Management (A6), Poor Quality Control process in receiving goods (A10), Delays in ordering and delivery Process (A11), Inadequate NAP interconnecting bandwidth capacity (A12), Disruptions in NAP and backhaul network (A13), Power outages (A16), Environmental factor disruptions (A17), Installation errors (A18), Configuration errors (A19), Main device failure (A20), Cyber attacks (A21), Inaccurate Optical Power Meter (A23), Lack of proper work tools (A24). These 14 risk agents were subsequently used as the focus for the House of Risk Phase 2 analysis, in which mitigation strategies are developed and prioritized

HOR Phase 2

In Phase 2, interviews were conducted with informants to gather insights into potential mitigation measures that the company could implement to address the previously identified risk agents. Each proposed proactive action was assigned an identification code, denoted by the prefix "PA," and the corresponding sequence number.

The identified risk mitigation actions are: Having two or more NAPs for interconnecting bandwidth (PA1), Implementing 24/7 real-time network monitoring through NOC (PA2), Developing and implementing SOP (PA3), Providing personnel training (PA4), Implementing additional bandwidth based on traffic patterns and load balancing (PA5), Assigning standby personnel for 24 hours (PA6), Maintaining the availability of spare parts stock (PA7), Configuring firewalls and router (PA8), Ensuring the availability of back up hardware components (PA9), Monitoring device conditions in real-time (PA10), Providing Uninterruptible Power Supply and generators (PA11), Conducting routine maintenance of work tools (PA12), Implementing Human Resources Information System (PA13), Conducting simulations before implementation (PA14), Performing regular calibration of measurement instruments (PA15), Implementing Enterprise Resource Planning system (PA16).

Based on the proactive action (PA) steps identified in the previous stage, an evaluation was conducted to assess the level of difficulty associated with the implementation of each action (Dk). Additionally, the strength of the relationship between each risk agent and the corresponding mitigation action was rated, using expert judgment to assign scores reflecting the perceived effectiveness of each pair (Rjk). These evaluations were recorded in the assessment instrument. Subsequently, the Total Effectivness (TEk) and Effectiveness to Difficulty (ETDk) ratio was calculated using equation (2) and equation (3) for each mitigation action to determine its priority level.

$$TE_k = \sum_j ARP_j R_{jk} \quad (2)$$

$$ETD_k = {}^{TE_k}/_{D_k} \quad (3)$$

This ratio reflects the balance between a mitigation action's potential to reduce risk and the complexity of its implementation. Actions with the highest ETD values are prioritized, as they offer a significant impact on risk reduction while remaining relatively feasible to execute. The results of the House of Risk Phase 2 analysis, including ETD values for each informant are presented in tables 4, table 5, and table 6.

Table 4. Informan 1 ETD Result

	Proactive Action																
Risk Agent	PA 1	PA 2	PA 3	PA 4	PA 5	PA 6	PA 7	PA 8	PA 9	PA 10	PA 11	PA 12	PA 13	PA 14	PA 15	PA 16	ARP
A4														9			330
A6				9									9				594
A10			9														396
A11																9	288
A12	3	3			9												882
A13	9	9															864
A16											9						648
A17						9	9										1185
A18			9	9													1245
A19			9	9													405
A20									9	9							696
A21								9									972
A23															9		348
A24												9					459
TE	10422	10422	18414	20196	7938	10665	10665	8748	6264	6264	5832	4131	5346	2970	3132	2592	
Dk	3	4	4	4	3	4	3	4	5	3	3	3	3	4	3	4	
ETD	3474	2605	4603	5049	2646	2666	3555	2187	1252	2088	1944	1377	1782	742	1044	648	

Table 5. Informan 2 ETD Result

	Proactive Action																
Risk Agent	PA 1	PA 2	PA 3	PA 4	PA 5	PA 6	PA 7	PA 8	PA 9	PA 10	PA 11	PA 12	PA 13	PA 14	PA 15	PA 16	ARP
A4			3											9			648
A6				3									9				468
A10			9														540
A11																9	468
A12	9	3			9												705
A13	9	3															996
A16											9						405
A17						9	3										900
A18			9	9										3			768
A19			9	9													396
A20									9	3							690
A21		3						9									810
A23															9		336
A24												9					324
TE	15309	7533	17280	11880	6345	8100	2700	7290	6210	2070	3645	2916	4212	8136	3024	4212	
Dk	3	4	4	4	3	4	3	3	4	3	3	3	4	4	3	4	

	Proactive Action																
Risk Agent	PA 1	PA 2	PA 3	PA 4	PA 5	PA 6	PA 7	PA 8	PA 9	PA 10	PA 11	PA 12	PA 13	PA 14	PA 15	PA 16	ARP
ETD	5103	1883	4320	2970	2115	2025	900	2430	1552	690	1215	972	1053	2034	1008	1053	

Table 6. Informan 3 ETD Result

	Proactive Action																
Risk Agent	PA 1	PA 2	PA 3	PA 4	PA 5	PA 6	PA 7	PA 8	PA 9	PA 10	PA 11	PA 12	PA 13	PA 14	PA 15	PA 16	ARP
A4				3										9			342
A6				3									9				378
A10			9														288
A11																9	288
A12	3				9												756
A13	9	9															972
A16											9						648
A17						9	9										1080
A18			9	9											3		864
A19			9	9										3			504
A20									9	3							570
A21								9									810
A23															9		288
A24												9					432
TE	11016	8748	14904	14472	6804	9720	9720	7290	5130	1710	5832	3888	3402	4590	5184	2592	
Dk	4	4	4	3	3	4	3	3	5	3	3	3	3	4	3	4	
ETD	2754	2187	3726	4824	2268	2430	3240	2430	1026	570	1944	1296	1134	1147	1728	648	

Based on the ETD values derived from the House of Risk Phase 2 evaluation, an ABC 20-30-50 analysis was conducted to establish the implementation priority of each mitigation measure. This prioritization is determined by ranking the mitigation actions from those with the highest ETD values—indicating high effectiveness and relatively low implementation difficulty—to those with lower ETD values. Consequently, mitigation steps that are both impactful and feasible are positioned at the top of the implementation plan, ensuring that risk reduction efforts are carried out in the most efficient and strategic manner. Tabel 4.7 shows ABC analysis results of proactive actions from each informant.

Table 7. Proactive Action Priority

RN			CU			AF		
Agent	ARP	Category	Agent	ARP	Category	Agent	ARP	Category
PA4	5049	A	PA1	5103	A	PA4	4824	A
PA3	4604	A	PA3	4320	A	PA3	3726	A
PA7	3555	A	PA4	2970	A	PA7	3240	A
PA1	3474	B	PA8	2430	B	PA1	2754	B
PA6	2666	B	PA5	2115	B	PA6	2430	B
PA5	2646	B	PA14	2034	B	PA8	2430	B
PA2	2606	B	PA6	2025	B	PA5	2268	B
PA8	2187	B	PA2	1883	B	PA2	2187	B
PA10	2088	C	PA9	1553	C	PA11	1944	C
PA11	1944	C	PA11	1215	C	PA15	1728	C
PA13	1782	C	PA13	1053	C	PA12	1296	C
PA12	1377	C	PA16	1053	C	PA14	1148	C
PA9	1253	C	PA15	1008	C	PA13	1134	C
PA15	1044	C	PA12	972	C	PA9	1026	C
PA14	743	C	PA7	900	C	PA16	648	C
PA16	648	C	PA10	690	C	PA10	570	C

DISCUSSION

Based on the analysis conducted using the House of Risk (HoR) method, a total of 14 risk agents within the company's supply chain have been identified as priorities for mitigation. The prioritized risk agents, along with their corresponding mitigation actions, are outlined as follows:

1. Environmental Factor Disruption (A17). Extreme weather conditions (e.g., heavy rainfall) and human activities (such as collisions involving heavy vehicles) have the potential to cause significant damage to vulnerable components such as fiber optic cables and supporting structures like distribution poles. Cable damage may also result from a variety of environmental factors, including rodent bites, falling trees or branches, impacts from trucks, road construction, utility work (PLN/PDAM), or even being entangled by kites (Bustommy et al., 2021). To mitigate this risk, the company should establish a clear and responsive emergency recovery protocol to ensure timely restoration of services in the event of disruption. It is also essential to maintain sufficient inventory of critical infrastructure components, such as fiber optic cables, connectors, and other passive devices, to support swift repairs and reduce service downtime.
2. Installation Errors (A18). Errors during the installation process, whether on central devices or network endpoints, represent one of the key risk agents that must be addressed. Such issues can occur during the deployment of Fiber to Homet (FTTH) installation, including incorrect device installation or improper cable termination in cabinets or terminals. Additionally, during optical fiber installation, macro-bends or bends that exceed acceptable limits may arise, leading to signal degradation or

attenuation (Ridho et al., 2020). The quality of installation plays a crucial role in signal integrity, as attenuation in optical fibers can result from excessive bending, poor splicing, or suboptimal connector usage, ultimately degrading the optical signal to the point where it cannot be fully recovered at the receiving end (Soothar et al., 2024). To mitigate this risk, the company should design and implement structured and comprehensive Standard Operating Procedures (SOPs) for installation activities. In parallel, technical training programs must be provided for field technicians to ensure they possess the necessary expertise and a clear understanding of the SOPs. As technicians are the frontline representatives interacting directly with customers during installation and troubleshooting, it is essential to maintain consistent technical standards and continuously enhance their skills and competencies (Nurrahman et al., 2023).

3. Disruption in NAP and Backhaul Network (A13). Disruptions in the NAP and backhaul network can lead to unstable or even isolated interconnecting bandwidth on the company's side. These issues often occur when one of the bandwidth providers experiences a service outage or disconnection (Mustofa & Ramayanti, 2020). To mitigate this risk, the company should adopt a network redundancy strategy by integrating connections to multiple NAPs. This ensures that if one provider fails, alternative routes remain available to maintain uninterrupted service. As an additional measure, the company should operate a 24/7 Network Operations Center (NOC), supported by a real-time monitoring system, to detect issues early and respond quickly to potential disruptions.
4. Inadequate NAP Interconnecting Bandwidth Capacity (A12). During periods of high customer demand, the available interconnecting bandwidth from the Network Access Provider (NAP) can become overloaded, as it must simultaneously accommodate multiple user requests (Mustofa & Ramayanti, 2020). This often leads to network instability and a decline in overall service quality. As noted by Gunantara et al. (2022), ISPs must allocate bandwidth effectively to prevent bottlenecks in data transmission, which can negatively impact network performance. To mitigate this risk, the company should implement a dynamic bandwidth management system that automatically adjusts network capacity based on real-time traffic patterns. This approach enables more efficient resource utilization and helps maintain stable service during peak usage times.
5. Main Device Failure (A20). Malfunction or damage to critical main devices can lead to a significant decline in operational performance, deterioration in internet service quality, and in severe cases, complete service outages.To mitigate this risk, it is essential for the company to maintain an inventory of backup devices to facilitate immediate replacement in the event of main device failure and implement a preventive maintenance program, including regular cleaning and continuous monitoring of operational parameters such as temperature and voltage to prevent

deterioration in device functionality. Maintaining an adequate inventory of hardware is crucial to sustaining uninterrupted service delivery (Benjarattanapakee & Ongkunaruk, 2023).

6. Inaccurate Optical Power Meter (A23). Damage or reduced accuracy of measuring tools like Optical Power Meters (OPM) can affect the reliability of measurement data and lead to incorrect technical analysis. Inaccurate OPM readings prevent technicians from accurately assessing signal attenuation, which is a key challenge in fiber optic communications caused by factors such as dispersion, absorption, bending, splicing, and damaged connectors (Soothar et al., 2024). To mitigate this risk, companies should establish a comprehensive management system for measuring instruments, including keeping detailed logs of their use, condition, and maintenance schedules.
7. Design and Device Selection Errors (A4). Errors in network design or inappropriate device selection can significantly affect system performance and limit network scalability. Key aspects, such as the placement of passive devices, the number of splitters, and the fiber optic connections between customers and the central station, play a critical role in determining the overall quality of service (Yazar et al., 2016). To mitigate this risk, companies should undertake comprehensive design simulations and testing, including performance evaluations, peak traffic load scenario analyses, and compatibility assessments between hardware and software components.
8. Power Outage (A16). Power outages can cause main active devices to cease functioning, leading to widespread service disruptions. To mitigate this risk, companies must ensure the availability of reliable Uninterruptible Power Supply (UPS) systems and backup generator sets (gensets) at each Point of Presence (PoP) and other critical network device locations.
9. Configuration Error (A19). Inappropriate network device configuration often results from unclear standards, human error, or insufficient coordination among technicians. Proper configuration, such as effective bandwidth management, is crucial to maintaining consistent internet speeds, ensuring that upload and download capacities are balanced among users during periods of high network traffic. To mitigate this risk, companies should develop and implement standardized configuration templates tailored to each device type and network function.
10. Poor Quality Control Process (A10). Failures in the inspection process can lead to delays in procurement evaluation and acceptance of materials that do not meet required specifications (Illaritzqi et al., 2024). To mitigate this risk, companies should develop and implement comprehensive and rigorous Quality Control Standard Operating Procedures (SOPs). These SOPs must encompass all inspection stages, including physical examination of devices, verification of technical specifications against contract documents, basic functionality testing, and validation of product certifications and warranties.

11. Ineffective Human Resource Management (A6). Ineffective human resource management can lead to operational challenges such as workload imbalances, miscommunication among personnel, and delays in task completion. These issues may reduce employee productivity and negatively impact on the quality of service delivered to customers. To mitigate this risk, companies should implement a Human Resource Information System (HRIS) that includes workload analysis, task prioritization, and employee performance monitoring features. Utilizing HRIS can enhance HR management, improve employee productivity, and ultimately support the overall achievement of organizational goals and performance (Lubis and Adlina, 2025).
12. Delays in Ordering and Delivery Process (A11). Delays in the procurement and delivery of essential hardware and critical network components represent significant logistical risks that may result in stock shortages. Such shortages can adversely affect the timely execution of new service installations, network expansions, and infrastructure maintenance activities (Illaritzqi et al., 2024). To mitigate this risk, companies must implement an integrated and predictive demand planning system through the deployment of an Enterprise Resource Planning (ERP) platform. This system should include Material Requirement Planning (MRP) based on demand projections, project cycles, and available stock to facilitate proactive and precise procurement activities.
13. Cyber Attacks (A21). Cyber attacks pose a significant threat that can severely disrupt network infrastructure, leading to widespread service outages. Such security incidents can also erode user trust in the integrity and reliability of the service provider. To mitigate this risk, companies must implement multiple layers of robust security measures, including well-configured firewalls. Firewalls serve as a fundamental security barrier by filtering all incoming and outgoing traffic at both the device and network levels, thereby preventing unauthorized access to the network (Alsaqour et al., 2021).
14. Lack of Proper Work Tools (A24). Damaged or malfunctioning work tools, such as fiber optic splicers, can significantly impede the efficiency and quality of network installation and maintenance activities. Such deficiencies may adversely affect the stability and reliability of internet service. To mitigate this risk, it is essential for companies to implement a scheduled maintenance program for all work tools, including routine functional assessments, calibration procedures, and cleaning protocols.

CONCLUSION AND RECOMMENDATION

Based on the findings and analysis of this study, the following conclusions can be drawn:

1. The company is exposed to 29 risk agents within its supply chain, of which 14 have been identified as priority risks that require immediate attention. These include design and device selection errors, ineffective human resource management, inadequate quality control in goods reception, delays in ordering and shipping, limited interconnection bandwidth from the Network Access Provider (NAP), disruptions in NAP and backhaul networks, power outages, environmental disturbances, installation and configuration errors, damage to core devices, cyberattacks, inaccurate Optical Power Meter (OPM) readings, and malfunctioning work tools.
2. From the risk agents identified, a total of 27 potential risk events were mapped that could impact the company's operations.
3. To address the prioritized risk agents, mitigation actions have been identifed that can serve as a strategic reference for the company in managing supply chain risks. It is prioritized to be actionable in operational settings of the company.

It is recommended for the company to implementing the steps outlined in their risk mitigation plans to address the identified risk sources. These mitigation plans can be implemented directly in the field and reviewed periodically to measure the level of success outlined in the mitigation plan resulting from this study.

FURTHER STUDY

Suggestions for further research include conducting a more in-depth study of the risk analysis and supply chain performance of ISP companies by integrating the SCOR model with sustainability principles. The House of Risk (HOR) approach can be utilized to identify and mitigate various sustainability-related risks, including environmental, social, and economic aspects.

REFERENCES

Aldianto, L., Anggadwita, G., Permatasari, A., Mirzanti, I. R., & Williamson, I. O. (2021). Toward a business resilience framework for startups. Sustainability, 13(6), 3132. https://doi.org/10.3390/su13063132

Alsaqour, R., Motmi, A., & Abdelhaq, M. (2021). A systematic study of network firewall and its implementation. International Journal of Computer Science & Network Security, 21(4), 199-208. https://doi.org/10.22937/IJCSNS.2021.21.4.24

Anggadwita, G., Profityo, W. B., Permatasari, A., Alamanda, D. T., & Hasfie, M. (2019, May). Analysis of value chain model on small and medium enterprises (SMEs): A case study of coffee shops in Bandung. In IOP Conference Series: Materials Science and Engineering (Vol. 505, No. 1, p. 012098). IOP Publishing. https://doi.org/10.1088/1757-899X/505/1/012098

Benjarattanapakee, C., & Ongkunaruk, P. (2023). Analyzing the supply chain sustainability of an internet service provider in Thailand. In E3S Web of

Conferences (Vol. 408, p. 01011). EDP Sciences. https://doi.org/10.1051/e3sconf/202340801011

Bustommy, A. Y., Saroso, D. S., & Hasibuan, S. (2021). Improving the quality of IndiHome services using six sigma DMAIC method: Case in industrial area. Mercu Buana University. http://ieomsociety.org/singapore2021/papers/824.pdf

Fornah, H. A., & Pujawan, I. N. (2020). Assessing supply chain practices and how they are perceived to impact performance of firms in Sierra Leone: A Case Study in a telecommunication company (Sierratel). In IOP Conference Series: Materials Science and Engineering (Vol. 847, No. 1, p. 012095). IOP Publishing. DOI https://doi.org/10.1088/1757-899X/847/1/012095

Gunantara, N., Widyantara, I. M. O., Ardana, I. P., Saputra, K. O., & Bernadus, I. N. (2022). Improving Internet Network Performance through Bandwidth Management. Int. J. Emerg. Technol. Adv. Eng. DOI: https://doi.org/10.46338/ijetae1222_07

Hendayani, R., Rahmadina, E., Anggadwita, G., & Pasaribu, R. D. (2021, August). Analysis of the house of risk (HOR) model for risk mitigation of the supply chain management process (case study: KPBS pangalengan bandung, Indonesia). In 2021 9th International Conference on Information and Communication Technology (ICoICT) (pp. 13-18). IEEE. https://doi.org/10.1109/ICoICT52021.2021.9527526

Illaritzqi, D., Istiqomah, S., & Albana, A. S. (2024). Analisis dan mitigasi risiko dalam pengadaan menggunakan pendekatan House of Risk pada perusahaan jaringan broadband. Jurnal Penelitian Rumpun Ilmu Teknik, 3(3), 98-116. https://doi.org/10.55606/juprit.v3i3.4233

Jittamai, P., Toek, S., Sathaporn, P., Kongkanjana, K., & Chanlawong, N. (2024). Risk Mitigation in Durian Cultivation in Thailand Using the House of Risk (HOR) Method: A Case Study of Pak Chong GI Durian. Sustainability, 17(1), 222. https://doi.org/10.3390/su17010222

Kristiana, S. P. D., Oktavia, C. W., Magdalena, R., & Lilajati, M. A. (2020, April). Risk mitigation strategies on Supply Chain PT. X. In IOP Conference Series: Materials Science and Engineering (Vol. 847, No. 1, p. 012052). IOP Publishing. https://doi.org/10.1088/1757-899X/847/1/012052

Kunrath, T. L., Dresch, A., & Veit, D. R. (2023). Supply chain management and industry 4.0: a theoretical approach. Brazilian Journal of Operations & Production Management, 20(1), 1263-1263. https://doi.org/10.14488/BJOPM.1263.2023

Lubis, R. A., & Adlina, H. (2025). Penerapan Human Resources Information System (Hris) Dalam Meningkatkan Efektivitas Dan Efisiensi Sumber Daya Manusia. Jurnal Ilmiah Wahana Pendidikan, 11(4. D), 135-143. http://jurnal.peneliti.net/index.php/JIWP/article/view/10216

Mustofa, A., & Ramayanti, D. (2020). Implementasi Load Balancing dan Failover to Device Mikrotik Router Menggunakan Metode NTH (Studi Kasus: PT. GO-JEK Indonesia). Jurnal Teknologi Informasi Dan Ilmu Komputer, 7(1), 139-144. https://doi.org/10.25126/jtiik.2020701638

Naji, M., Thiruchelvam, S., & Khudari, M. (2023). An investigation of Internet Service Provider selection criteria: A systematic literature review. Iraqi Journal for Computer Science and Mathematics, 4(4), 156-172. https://doi.org/10.52866/ijcsm.2023.04.04.013

Nurrahman, A. H., Noviaristanti, S., & Firli, A. (2023, August). Analyzing The Continuance Intention Of Fixed Broadband Using Modified Utaut2 Model (A Case Study Of Indihome In Indonesia). In 2023 International Conference on Digital Business and Technology Management (ICONDBTM) (pp. 1-6). IEEE. https://doi.org/10.1109/ICONDBTM59210.2023.10326740

Nyoman Pujawan, I., & Geraldin, L. H. (2009). House of risk: a model for proactive supply chain risk management. Business Process Management Journal, 15(6), 953-967. https://doi.org/10.1108/14637150911003801

Partiwi, S. G., Islami, V. N., & Firmanto, H. (2023). House of Risk (HOR) Approach to Manage Risk involving Multi-stakeholders: The Case of Automotive Industry Cluster of Multifunctional Rural Mechanized Tool (MRMT). Operations and Supply Chain Management, 16(1), 133-139. http://doi.org/10.31387/oscm0520378

Ridho, C. S., A'isya Nur Aulia Yusuf, S., Andra, D. N. S. S., & Apriono, C. (2020). Perancangan Jaringan Fiber to the Home (FTTH) pada Perumahan di Daerah Urban. J. Nas. Tek. Elektro, 3. https://doi.org/10.22146/jnteti.v9i1.138

Soothar, K. K., Chen, Y., Magsi, A. H., Hu, C., & Shah, H. (2024). Optimizing Optical Fiber Faults Detection: A Comparative Analysis of AdvancedMachine Learning Approaches. Computers, Materials & Continua, 79(2). http://dx.doi.org/10.32604/cmc.2024.049607

Thaichon, P., & Quach, T. N. (2015). The relationship between service quality, satisfaction, trust, value, commitment and loyalty of Internet service providers' customers. Journal of Global Scholars of Marketing Science, 25(4), 295-313. https://doi.org/10.1080/21639159.2015.1073419

Trisnawati, N., & Pujawan, I. N. (2021, April). Analysis of supply chain performance based on the supply chain management maturity level in manufacturing industry. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Sao Paulo, Brazil (pp. 5-8). https://doi.org/10.46254/SA02.20210691

Yazar, B., Arslan, O., Karaşan, O. E., & Kara, B. Y. (2016). Fiber optical network design problems: A case for Turkey. Omega, 63, 23-40. https://doi.org/10.1016/j.omega.2015.10.001