Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

Management System Project for Textile Company using Risk Management Analysis

Lorio Purnomo*, Chairani Putri Pratiwi, Rizka Astari Rahmatika, Rafki Chandra Wibawa, Siti Paramadita, Desman Hidayat

BINUS Entrepreneurship Center, Management Department, Bina Nusantara University, Jakarta
Jl. Raya Kb. Jeruk No.27, RT.1/RW.9, Kb. Jeruk, Kec. Kb. Jeruk, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta, Indonesia
Email: [1,*]lorio.purnomo@binus.ac.id, [2]chairani.putri@binus.ac.id, [3]rizka.astari@binus.ac.id, [4]rafki.wibawa@binus.ac.id, [5]siti.paramadita@binus.ac.id, [6]d4906@binus.ac.id
Correspondence Author Email: lorio.purnomo@binus.ac.id

Abstract−As technology continues to advance across industries, the strategic role of information in organizations becomes increasingly evident. Recognizing the potential of information technology to enhance operational efficiency and customer satisfaction, various industries have integrated technology into their management systems. However, these innovations also introduce risks to the organization's information landscape. Risk management, therefore, emerges as a crucial discipline to identify, assess, and mitigate information technology-related risks. Textile companies, for instance, employ web-based management systems to support their operations, but encounter challenges hindering effective business process execution. This leads to reduced work performance and hampers goal attainment. This study aims to analyze the risks associated with web-based management systems in the textile industry and to suggest strategies for minimizing these risks. The research combines literature review and analytical methodologies to achieve its objectives. The literature review encompasses topics such as management systems, their components, and risk management. The research proposes a risk management process comprising nine stages: system characterization, identifying threats, determining vulnerabilities, analyzing controls, estimating probability, evaluating impact, assessing risk, proposing controls, and documenting results. Nevertheless, there is very little and/or scarce research on the use of technology throughout the textile industry. Thus, in order to fulfill the research emptiness within the use of information technology to increase the performance of the textile industry, this research underscores the critical role of risk management in safeguarding information technology systems within the textile industry.

Keywords: Risk Management; Management System; Information System; Weaving

1. INTRODUCTION

The impact of the existence of Information Technology is increasingly developing in the current digital era, making various industries capture the opportunity to continue to innovate and optimize the use of digital technology. Especially in the textile and garment industry, it is very important to adapt to those changes and trends to meet market demand and needs (Majumdar & Sinha, 2019). The aim is to create added value that can produce products that are innovative, high quality, and on time with shorter development cycles and greater responsiveness(Chen, 2019). The manufacturing and garment industry must be able to adjust and work hard to improve productivity, quality, and efficiency through the application of modern technology. Nowadays, most textile companies are aging, while technology is changing rapidly. However, most textile companies still running with conventional systems are having a hard time meeting the demand resulting in insufficient textile production.

In order to meet the current demand of the fast fashion industry, textile companies should improve their lead time, productivity, and quality, as well as efficiency. The use of digital technology will help textile companies to improve their overall productivity. Synchronizing production cycles to ensure timely fulfillment of textile fabric orders, warehouse production cycle operations need to be changed because of the increasing complexity in an organization.

Due to the rapid progress of technology, organizations realize that aspects of Information Technology are needed to improve the quality, accuracy, and speed of processes. Most management in various industries also realize that using the right information technology can increase the efficiency and effectiveness of the organization which will have an impact on customer satisfaction. However, due to the many innovations that are applied to the organization, sometimes there is a risk to the information in that organization. Here risk management has a very important role in identifying, assessing, and reducing the risks that exist in the textile company management system.

Though information technology has been used in many types of industries, there is scarce research found within textile industries. Most research throughout textile industries is discussing on the environmental impact. As we know, the textile industry is one of the most energy-consuming fields, described that the textile industry uses large amounts of electricity, fuel, and water, with corresponding greenhouse gas emissions (GHGs) and contaminated effluent. Thus, some studies have mentioned energy-efficiency technologies for the textile industry but have not focused on the textile industry management system itself.(Hasanbeigi & Price, 2015)

Conceptually, from an organizational perspective, risks arise when organizations pursue opportunities to deal with uncertainty, limited by ability and cost. The challenge is finding positions on each of these dimensions in combination, representing a risk profile that is suitable for the initiative and acceptable to internal and external stakeholders. As a result, risk and risk management are strategic and governance issues that usually involve compromise: strategies that avoid risks can limit achievement differently; However, embracing risk strategies can increase project losses(Bannerman, 2008)(Mohammad, 2020).

Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

Risk and risk management are also important because IT projects (including software projects) can be a means to deliver organizational change that is IT-supported, so that the achievement of business goals can be highly dependent on their success(Masso, Pino, Pardo, García, & Piattini, 2020). In this case the textile company applies a web-based Management System in each of its divisions. Each division produces some very crucial and important data. Data obtained from each weaving production cycle becomes crucial because the data are related or dependent on each other at each stage of production. To be able to produce the best weaving grade, there is a detailed calculation of each stage.

The administrator of each organizational unit must be sure that the organization has the capabilities needed to achieve the mission. They can provide the best conditions for dealing with missions with real-world behaviour with the determination of security capabilities. The effective use of the risk management process helps managers identify and carry out the controls needed to maintain IT factors. For this reason most organizations allocate large budgets for IT security(Tucnik, Otcenaskova, & Horalek, 2023).

Risk management is the process of identifying and accessing risks and applying methods to reduce them to acceptable limits. The main purpose of risk management is to help organizations better manage risks associated with their mission, with risk management expected to provide transformation for textile companies in the long run, so that companies can be more productive and develop and there is alignment between business strategies owned by companies to optimize the use of information systems and information technology. Risk management can also be used to make decisions that make sense in all aspects of daily life.(Majumdar & Sinha, 2019).

The rapid evolution of Information Technology (IT) in the digital era has prompted various industries, including the textile and garment sector, to harness digital innovation and technology optimization to meet market demands (Majumdar & Sinha, 2019). Adaptation to these changes has become vital to add value through innovative, high-quality, and timely product development with increased responsiveness (Chen, 2019). However, the challenge arises as traditional manufacturing industries, including textiles, must modernize their practices to enhance productivity, quality, and efficiency amidst fast-paced technological changes. The synchronization of production cycles and the adaptation of warehouse operations have become essential due to the intricate organizational complexities. While IT promises to improve relationships, quality, and accuracy, its rapid integration introduces risks that need effective management strategies.

Scholars have recognized the strategic importance of risk management in IT-intensive projects. Risk emerges when organizations pursue opportunities within limitations of capability and cost, requiring a suitable and acceptable risk profile aligned with stakeholder interests (Bannerman, 2008). This compromise-driven nature of risk management creates challenges in project implementation. Additionally, IT projects, such as software development, serve as vehicles for IT-supported organizational change, making their success pivotal for achieving business goals (Masso et al., 2020).

In the context of the textile industry's adoption of web-based Management Systems, challenges arise due to the interdependence of crucial data at each stage of production. Administrators must ensure that the organization's mission can be achieved by establishing robust security capabilities. Budget allocation for IT security highlights its significance (Tucnik et al., 2023). Effective risk management, involving risk identification, assessment, and reduction, plays a pivotal role in helping organizations manage mission-associated risks (Majumdar & Sinha, 2019).

Despite the recognition of risk management's significance, there exists a gap in understanding the application of risk management principles to web-based Management Systems in the textile industry. While the literature underscores the importance of IT and risk management, limited research specifically addresses the challenges posed by the integration of IT in textile production processes. This research aims to bridge this gap by investigating the risks associated with web-based Management Systems in the textile industry, offering insights into risk management strategies tailored to this sector's unique challenges and needs.

2. RESEARCH METHODS

2.1. Literature Review

This stage, the authors formulates the conceptual framework of the research. Figure 1 below, explain it stages in Research Methods for this paper. Based on figure, 1. The author sees the existence of Information Technology is increasingly developing in the current digital era, making various industries capture the opportunity to continue to innovate and optimize the use of digital technology, this is the identification of the initial problem in discussing this paper; 2. Then continue to conduct Literature review and Methodology, in this discussion the author searches and reads previous Journals that discuss Management System, Risk Management, then in this Methodology apply Stages of Risk Management Analysis, to ensure these steps can help in the search for Results and Discussion; 3. The Result and Discussion stage explains the Risk Estimation that exists in Textile Companies when going to carry out updates using Information Technology which in this case implements a Management System by considering the principles of Risk Management; 4. Conclusion implementation of a management system in the weaving division is the output of this research discussion by first discussing Risk Management at Textile Company.

Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

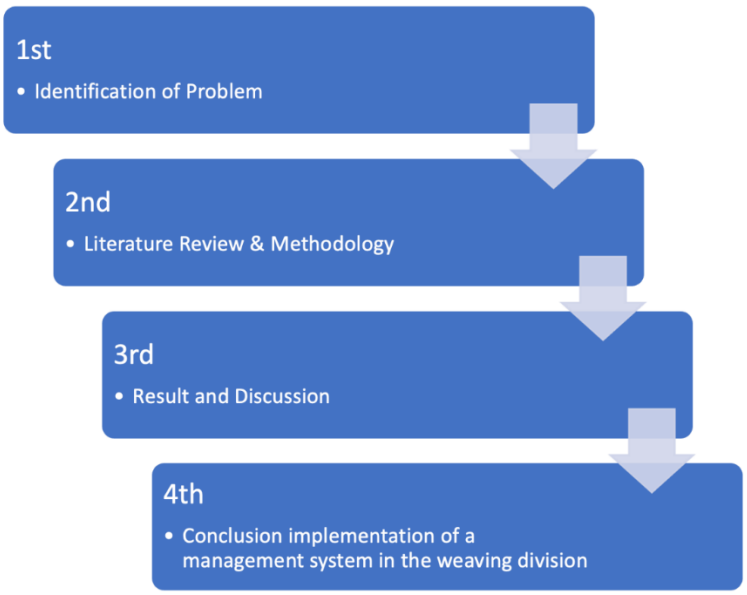

Figure 1. Research Methode

2.1.1 Management System

The management system is the process and procedure used to ensure that the company can fulfill all the tasks needed to achieve its objectives(Hahn, Subramani, & Hahn Mani Subramani, 2000). In other opinions, management systems with various elements such as decision-making, organization, information, and motivational character, and in the organization all management processes and relationships are carried out(Chen, 2019). Management systems in an organization have different management systems, such as quality management systems, financial management systems, and environmental management systems, etc. (Kumar, Maiti, & Gunasekaran, 2018)(Adeleke et al., 2019).

Warehouse Management System (WMS) is a computer-driven database application, which is used by logistics personnel to increase production efficiency in the warehouse by maintaining accurate inventory and recording all transactions in the warehouse. In the management system has its own vision and mission, including (Shiau & Lee, 2010)(Santoro, Vrontis, Thrassou, & Dezi, 2018):

a. Achieve a transportation economy
b. Achieve a production economy
c. Take advantage of quality purchase discounts and future purchases
d. Supports company customer service policies
e. Meet changes in market conditions and uncertainties
f. Overcoming space and time differences between producer
g. s and customers
h. Achieve the lowest total logistics costs with the desired level of customer service
i. Supports supplier and customer just-in-time programs
j. Provides temporary storage of material to be disposed of or recycled
k. Provide temporary storage of raw materials to be disposed of or recycled
l. Provide a buffer location for transportation – shipping

In the management system, there are several challenges in implementing it, as follows:

a. Training, where workers need to be given training in using information systems. Deploying and using a management system that requires time and effort. This is also related to the size of the business and the availability of skilled human resources.
b. Increase Cost, in implementing and maintaining information systems and management systems requires costs that will continue to increase.
c. Interoperability, so many management software systems that can be integrated and operate with different hardware or software. But it requires experts who can integrate and implement it.

2.1.2 Risk Management

Risk management is the process of identifying and assessing risks and applying methods to reduce them to acceptable limits. The main purpose of risk management is to help organizations better manage risks associated with their mission (Fan & Stevenson, 2018). Risk management is a process that enables IT managers to balance operational and economic costs to achieve a mission. With the protection of IT systems and the ability of organizations to achieve missions. Risk management can also lead to decisions that make sense in all aspects of daily life (Jimoh et al., 2022; Manun-Og et al., 2022).

Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

a. The importance of risk management
The administrator of each organizational unit must be sure that the organization has the capabilities needed to achieve the mission. They can provide the best conditions for dealing with missions with real-world behavior with the determination of security capabilities. The use of an effective risk management process helps managers identify the controls needed to maintain IT factors and for this reason, most organizations allocate large budgets for IT security (Babenko et al., 2019).
b. Integration of risk management with System Development of Life Cycle (SDLC)
Effective risk management must be fully integrated and pervasive in SDLC. The main reason for organizations to use risk management processes for their IT systems, is to minimize risks within the organization. Each SDLC, has five stages as follows:
1. Start
2. Development
3. Operation
4. Protection
5. Administration

In some cases, IT systems can occupy several stages. Risk Management is an ongoing process that can be implemented at each stage of the SDLC.
c. Risk Management Steps
The risk management process consists of things(Shiau & Lee, 2010):
1. Risk estimation
2. Risk reduction
3. Assessment and Evaluation
4. Risk estimation

In an organizational risk management analysis, the first process is a risk assessment that considers risk links to IT systems throughout the SDLC, this process is used to determine the minimum risk hazard. This process output also helps identify technical controls to reduce or limit risk during the risk reduction process. To determine the possibility of bad events in the future, an analysis of vulnerabilities and potential threats to IT systems is important.(Esteki et al., 2020; Masso et al., 2020). The analytical method for estimating risk also covers the following nine stages(Ali & Haseeb, 2019; Shiau & Lee, 2010):

1. System characterization
2. Identify threats
3. Identify vulnerabilities
4. Control analysis
5. Determination of probability
6. Analysis of effects
7. Determination of risk
8. Control purchase orders
9. Documented results

Stages 2, 3, 4 and 6 can be done in parallel with each other and after completing the first stage.

Step 1: System characterization:

The first step is the definition of the scope of the action. In this step, to assess IT system risk, fields for risk assessment are applied, valid application boundaries are drawn and important information is provided. In the resource steps, information and IT system boundaries are defined.

First stage output: IT system features that are assessed, provide a good image of the IT system environment and explain system boundaries.

Step 2: Identify threats:

The source of specific threats, vulnerabilities have the potential for successful performance. In determining the probability of a threat, the person must consider the threat's resources, potential vulnerabilities, and existing controls. Second stage output: List of threat resources that can cause some damage.

Step 3: Determine damage:

Threat analysis in IT systems must include vulnerability analysis by considering the environmental system. The aim of this step is to develop a list of system vulnerabilities (weaknesses and weaknesses) that could potentially be used by threatening sources.

Third Phase Output: List of system vulnerabilities that are potentially used by threatening sources.

Step 4: Control analysis:

The purpose of this step is the analysis of controls applied by the organization to minimize or limit the possibility of threats becoming practical in vulnerable systems.

Fourth stage output: List of current or designed controls used for IT systems, so that the risk of vulnerabilities and incompatible events is reduced.

Step 5: Determine the risk of damage:

Determination of the possible level of damage is achieved in accordance with the following criteria:

1. Motivation and ability of source of threat

Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

2. The nature of vulnerability
3. Existence and impact of current controls

In this step the possibility of potential vulnerabilities can be placed by threatening sources at high, low or being explained.

Fifth Stage Output: Rate the risk of damage (high, medium, low).

Step 6: Analyze the effect of the goal:

The main step in measuring the level of risk is to determine the outcome of the inconsistent effects of the success of the practical threat from vulnerability. Before analyzing the effects, it is necessary to achieve the following important information:

1. System missions (for example, processes run by IT systems)
2. Important systems and data (for example, the value of a system or the importance of the organization)
3. System and data sensitivity

This information can be obtained from organizational documents such as securities analysis reports, missions or important information assessment reports. The level of influence associated with the organization's information assets with an analysis of the influence of the objectives, with consideration of qualitative or quantitative sensitivity and criticality of the assets will be prioritized. If these documents do not exist or such estimates for the organization's IT assets are not achieved, given the sensitivity of system data can be based on the level of system protection requirements, availability, integrity and reliability of data.

Sixth Stage Output: Effect size (high, medium, low)

Step 7: Determine risk:

The purpose of this step is to estimate the level of risk in IT systems. Determining the risk of vulnerability or identified threats is a function of the following factors:

1. Possible sources of threats available to try to practice vulnerabilities that might occur.
2. The possibility of threats of vulnerability to be practically successful.
3. Adequacy of existing security controls or designed to reduce or eliminate risk.

Seventh Stage Output: Risk level (high, medium, low)

Step 8: Control Orders:

In this process, controls that can reduce or eliminate the risks identified. The purpose of control is to reduce the risk level of the IT system and its data to an acceptable level. The following factors should be considered when ordering controls to minimize or eliminate the risks identified:

1. Lack of options offered (for example system capability)
2. Laws and Codes
3. Organized policy
4. Operational effects
5. Safety and reliability

Output Eighth stage: Order controls and side solutions to reduce risk.

Step 9: Documented Results:

With the completion of the risk assessment (known threat and vulnerability resources, risks assessed and proposed controls) the results must be documented in an official or brief report.

A risk estimate report is a management report that helps chief managers and mission owners make decisions about policies, procedures, budgeting, articles, operating systems and management changes.

Output Ninth Stage: documented threats and vulnerability reports.

2.2 Methodology

2.2.1. Object of Research

The object used by this research is a project management system module that aims for recording/administration purposes in the Textile section of the Weaving stage. The weaving module itself consists of three major parts, namely the system:

a. Transaction
b. Report
c. Dashboard

2.2.2 Stages of Risk Management Analysis

The stages of Risk Management Analysis used in the process of making this research design have 3 main stages(Tohidi, 2011):

a. Risk Estimation

   The first process is a risk assessment that considers the risk link with the System Management Project on the object of this study, this process is used to determine the minimum risk of danger. The output of this process also helps identify technical controls to reduce or limit the risks that will arise. The analytical method for estimating risk also includes the following nine steps:

   1. Systems characterization

Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

2. Identifying threats
3. Risk determination
4. Control analyses

b. Risk Reduction
Risk reduction is the second stage of the risk management process after the risk estimation process. Which includes determining priorities, evaluating, and applying appropriate risk reduction controls.

c. Assessment and Evaluation
The final stage is evaluation and evaluation. The main role of the assessment and evaluation of the risk management identification process itself is to improve company performance and reduce the risk of failure to work.

3. RESULTS AND DISCUSSION

In this chapter, we will discuss the results of the analysis in making risk management planning in the project management system module. The results obtained from each stage of the risk management analysis described earlier in the methodology chapter are as follows:

3.1 Risk Estimation

3.1.1 Objective / Scope

a. Characterization of the system
In the textile company weaving division, the current production flow to produce textiles starts with woven strands that are connected to different patterns. The flow of weaving production starts based on the client's requirements. The yarn that is passed through is checked for all aspects of the material from the type of fiber, its thickness, strength, and how it is worked on. Of every production cycle, there must be a record, therefore the textile company has provided a platform named Warehouse Management System. The things that are considered important are the data obtained from each weaving production cycle because the data is related or dependent on the others. To be able to produce the best weaving grade, there is a detailed calculation of each stage.(Ayinde, Orekoya, Adepeju, & Shomoye, 2021)(Eskander, 2018). The following are the main activities in the Textile management system:

1. Sales
The Sales division submits the Production Order Letter and/or delivery order to PPIC (Production Planning Inventory Control) based on the fabric availability.
2. PPIC
PPIC receives orders and then plans raw materials for the needs of production materials.
3. Purchase
The purchasing part does purchase raw materials for production needs
4. Raw Material Warehouse
The Raw Material Warehouse receives raw material yarn and sends yarn into the spinning and production process.
5. Production Process
The production process starts with the warping process (rolling yarn from cone to beam), records the warping process, then sizing section (strengthening the yarn with starch), and proceeds to woven patterns to the needle to start the weaving process. The last part is the loom section, inspection, and finished warehouse.

b. Identifying potential risk
1. Downtime
To avoid downtime, testing should be done thoroughly. Testing requires more time, but in the end, it is better to spend more time testing than spending money and energy.
2. Initial drop in productivity
Implementing a new management system in the textile manufacturing process will increase long-term efficiency and productivity but may be accompanied by an initial decline at the beginning. Workers needed to be properly trained before implementation, thus training plans should be designed prior to the new system.
3. Cyber Security Threats
Cyber-security threats can endanger physical assets, intellectual property, and others. Manufacturers, like all companies, must manage and address their own cyber-security risks, and focus on how potential security attacks can affect end users and their customers.

c. Specifying damages
1. Publicly Exposed ICSs
Critical production machines or production lines. We have seen several cases where HMI was exposed directly to the internet, without authentication. This basically allows anyone to tamper with the value and issue orders on the manufacturing machine. Some of these interfaces provide read only access and are used for monitoring purposes only, while others do not. Any unauthorized damage to the system can result in production delays,

Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

product contamination, physical hazards, or equipment damage. Risks when HMI is exposed directly on the internet, where attacks can occur when actors manipulate SOPs or specifications that have been set by the company's management system(Kazancoglu, Kazancoglu, Kahraman, Yarimoglu, & Soni, 2022; Tohidi, 2011).

2. Data Leakage
   The company website of the manufacturing company also needs to have the right security configuration to prevent data leakage. It is common practice to share design documents with vendors, suppliers and third parties through the company's File Transfer Protocol (FTP) server, which is also usually a web server. Poor security configuration can expose this exclusive design document to the internet and cause data leakage.
3. Document Leakage
   In textile companies, of course, in the process of textile production, every division and every existing process has a predetermined provision or specification which must be followed every day by the system and strict monitoring of its employees. Current conditions in textile companies, apart from data that could have leaked, documents or often called manuals also contain products and information containing manuals and technical information such as component lists, design specifications, or business-related matters such as order details, terms of service, and warranty information. Sharing documents without permission can cause information leakage. Sharing documents only takes place on companies approved channels for audits and paper impressions. This requirement aims to maintain the ability to track with whom certain IPs are shared and whether the shares are authorized. If documents containing IP are shared through non-standard channels, the audit trail is lost, and the access policy cannot be enforced.

d. Control analysis
   Listed below are several recommendations that would be very beneficial for manufacturing companies to control possible threats and reduce vulnerability.
   1. Basic Security Principles
      1) Restrict User Access and permission throughout the domain and particular important documents (directory listing).
      2) Enforce domain or subnetwork restrictions.
      3) Remove or disable unnecessary services.
   2. Asset Identification, Prioritization, and protection application
      One effect of having an OT network connected to an IT network is the introduction of nontraditional devices (e.g., those that are not desktops, laptops, or servers). This places IT administrators in unknown situations and PL engineers in the IT world, with each role carrying a different mindset and priority.
   3. User Education
      Educating personnel about the value of documents containing IP and other proprietary information and the need to protect them.
   4. Making security requirements
      Making security a requirement for sending messages to only security-certified vendors.

3.2 Risk Estimation

Risk reduction step:

A. Assumption of the risk: Accept the potential risks mentioned above from the existing system and use analysis controls to reduce risk to an acceptable level.
B. Risk Control: Risk prevention through the elimination of risk factors or results, namely by taking control of the desire for system changes, because the effect of system changes will greatly affect the production department, in processing product results in time.
C. Elimination: Removing or reducing several but not all existing risks by not using changes in the system that is already running for the sake of not causing additional risks in the future.
D. Minimization: Minimize existing risks in 2 ways, among others:
   1. Minimize pre-loss
      Set the minimum risk-taking steps as possible: schedule system changes properly and carefully so as to avoid downtime, so they can take advantage of a system that is always innovating. Although there will be changes to the system that is running, employees are focused on continuing to work on what they normally do or increasing working hours for periodic testing. Defining more adequate security for the smooth running of the business, despite the risk of high costs in the initial setup but the need for data privacy is very important in the eyes of the customer.
   2. Minimize Post loss
      Risk prevention measures are already outlined above but plan B should be prepared when risks go further. There are steps to act on risks that have occurred for example increasing work hours to replace downtime while continuing to confirm changes to the management system existing so that changes do not occur in half measures, adding a security layer, and resolving what is wrong with the system running.

Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

3.3 Assessment and Evaluation

There are previous researches that highlighted risk management in the era of digital transformation outlining the increasing capability for organizational resilience. However, similar research that connected the implementation of technologies in the textile industry is not available and/or very scarce. One of the research projects suggests the importance of accounting for internal and external factors as key enablers in the adoption of emergent technologies for risk management. However, case-based research is needed since different industries would need different kinds of technical implementations.(Rodríguez-Espíndola, Chowdhury, Dey, Albores, & Emrouznejad, 2022). Based on the results of the above processes, the risk for each risk management can be overcome, resolved here not only in its entirety, but the inability to implement a solution, including dealing with unwanted risks in the future, by applying risk reduction to existing risks will increase the evolution of the system. management itself. These changes mean that the level of new risks and the reduction of previous risks can come back to future attention.

4. CONCLUSION

In conclusion, the implementation of a management system in the weaving division of the textile company has yielded advantages and benefits, particularly in streamlining the production flow and data management throughout the weaving production cycle. However, alongside these benefits, risks and losses have emerged, underscoring the significance of effective risk management. The integration of IT projects within the textile industry underscores the critical role of IT-supported organizational change in achieving business objectives. The findings of the risk analysis and threat management encompass various challenges, including downtime caused by system errors, an initial drop in productivity, and potential cyber security threats. Proper training for warehouse workers is crucial to fully harness the benefits of the management system. The study suggests solutions such as adhering to basic security principles, asset identification and prioritization, protection applications, and user education. This study acknowledges several limitations. First, the research primarily focuses on the weaving division of a single textile company, potentially limiting the generalizability of findings across different segments of the industry. Second, the study primarily discusses risks associated with IT integration and management systems, potentially overlooking other operational or environmental risks. Third, the research scope might not fully capture the evolving landscape of IT risks and their mitigation strategies. Finally, the proposed solutions are conceptual and might require further validation and customization for effective implementation in diverse organizational contexts. Therefore, this study suggests further research addressing these limitations. Future research should also investigate and analyse areas beyond risk management.

REFERENCES

Adeleke, A. Q., Kamaruddeen, A. M., Bahaudin, A. Y., & Bamgbade, J. A. (2019). An Empirical Analysis of Organizational External Factors on Construction Risk Management CONSTRUCTION MANAGEMENT View project Identification and Analysis of Critical Success Factors Influencing IBS performance in Housing Delivery View project. Retrieved from http://excelingtech.co.uk/

Ali, A., & Haseeb, M. (2019). Radio frequency identification (RFID) technology as a strategic tool towards higher performance of supply chain operations in textile and apparel industry of Malaysia. Uncertain Supply Chain Management, 7(2), 215–226. https://doi.org/10.5267/j.uscm.2018.10.004

Ayinde, L., Orekoya, I. O., Adepeju, Q. A., & Shomoye, A. M. (2021). Knowledge audit as an important tool in organizational management: A review of literature. Business Information Review, 38(2), 89–102. https://doi.org/10.1177/0266382120986034

Babenko, V., Lomovskykh, L., Oriekhova, A., Korchynska, L., Krutko, M., & Koniaieva, Y. (2019). Features of methods and models in risk management of IT projects Keyword: IT project risks Project risk management Software Methodology Project management Corresponding Author. 7(2), 629–636. Retrieved from http://pen.ius.edu.ba

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. Journal of Systems and Software, 81(12), 2118–2133. https://doi.org/10.1016/j.jss.2008.03.059

Chen, C. L. (2019). Value Creation by SMEs Participating in Global Value Chains under Industry 4.0 Trend: Case Study of Textile Industry in Taiwan. Journal of Global Information Technology Management, 22(2), 120–145. https://doi.org/10.1080/1097198X.2019.1603512

Eskander, R. F. A. (2018). Risk assessment influencing factors for Arabian construction projects using analytic hierarchy process. Alexandria Engineering Journal, 57(4), 4207–4218. https://doi.org/10.1016/j.aej.2018.10.018

Esteki, M., Gandomani, T. J., & Farsani, H. K. (2020). A risk management framework for distributed scrum using prince2 methodology. Bulletin of Electrical Engineering and Informatics, 9(3), 1299–1310. https://doi.org/10.11591/eei.v9i3.1905

Fan, Y., & Stevenson, M. (2018, March 22). A review of supply chain risk management: definition, theory, and research agenda. International Journal of Physical Distribution and Logistics Management, Vol. 48, pp. 205–230. Emerald Group Holdings Ltd. https://doi.org/10.1108/IJPDLM-01-2017-0043

Hahn, J., Subramani, M., & Hahn Mani Subramani, J. R. (2000). Association for Information Systems AIS Electronic Library (AISeL) A Framework of Knowledge Management Systems: Issues and Challenges for Theory and Practice Recommended Citation 'A Framework of Knowledge Management Systems: Issues and Challenges for Theory and Practice' A FRAMEWORK OF KNOWLEDGE MANAGEMENT SYSTEMS: ISSUES AND CHALLENGES FOR THEORY AND PRACTICE 1. Retrieved from http://aisel.aisnet.org/icis2000/28

Journal of Trends Economics and Accounting Research
Vol 4, No 1, September 2023, Hal. 98-106
ISSN 2745-7710 (Media Online)
Website https://journal.fkpt.org/index.php/jtear
DOI 10.47065/jtear.v4i1.798

Hasanbeigi, A., & Price, L. (2015, May 15). A technical review of emerging technologies for energy and water efficiency and pollution reduction in the textile industry. Journal of Cleaner Production, Vol. 95, pp. 30–44. Elsevier Ltd. https://doi.org/10.1016/j.jclepro.2015.02.079

Jimoh, R. G., Olusanya, O. O., Awotunde, J. B., Imoize, A. L., & Lee, C. C. (2022). Identification of Risk Factors Using ANFIS-Based Security Risk Assessment Model for SDLC Phases. Future Internet, 14(11). https://doi.org/10.3390/fi14110305

Kazancoglu, I., Kazancoglu, Y., Kahraman, A., Yarimoglu, E., & Soni, G. (2022). Investigating barriers to circular supply chain in the textile industry from Stakeholders' perspective. International Journal of Logistics Research and Applications, 25(4–5), 521–548. https://doi.org/10.1080/13675567.2020.1846694

Kumar, P., Maiti, J., & Gunasekaran, A. (2018). Impact of quality management systems on firm performance. International Journal of Quality and Reliability Management, Vol. 35, pp. 1034–1059. Emerald Group Publishing Ltd. https://doi.org/10.1108/IJQRM-02-2017-0030

Majumdar, A., & Sinha, S. K. (2019). Analyzing the barriers of green textile supply chain management in Southeast Asia using interpretive structural modeling. Sustainable Production and Consumption, 17, 176–187. https://doi.org/10.1016/j.spc.2018.10.005

Manun-Og, M. B., Manun-Og, M. R., Rey, A., Wales, F., Balili, D. A., & Togonon, J. N. (2022). Development of a records management system with GIS integration: enabling tool for disaster risk management. In SciEnggJ (Vol. 15).

Masso, J., Pino, F. J., Pardo, C., García, F., & Piattini, M. (2020, August 1). Risk management in the software life cycle: A systematic literature review. Computer Standards and Interfaces, Vol. 71. Elsevier B.V. https://doi.org/10.1016/j.csi.2020.103431

Mohammad, S. M. (2020). Risk Management in Information Technology.

Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022). Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. Technological Forecasting and Social Change, 178. https://doi.org/10.1016/j.techfore.2022.121562

Santoro, G., Vrontis, D., Thrassou, A., & Dezi, L. (2018). The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity. Technological Forecasting and Social Change, 136, 347–354. https://doi.org/10.1016/j.techfore.2017.02.034

Shiau, J. Y., & Lee, M. C. (2010). A warehouse management system with sequential picking for multi-container deliveries. Computers and Industrial Engineering, 58(3), 382–392. https://doi.org/10.1016/j.cie.2009.04.017

Tohidi, H. (2011). The role of risk management in IT systems of organizations. Procedia Computer Science, 3, 881–887. https://doi.org/10.1016/j.procs.2010.12.144

Tucnik, P., Otcenaskova, T., & Horalek, J. (2023, April 13). Project and Risk Management in the Context of IT Projects (J. Maci, P. Maresova, K. Firlej, & I. Soukal, Eds.). https://doi.org/10.36689/uhk/hed/2023-01-071