Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Informatics Technologies

Master's Diploma Thesis

Information Technology Change Risk Minimization: A Case of Using Global Service Now (GSN)

2023

Author

Ing. B.Sc. Haydiso Bereket Detamo, MSc

Diploma Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Ing. B.Sc. Haydiso Bereket Detamo, MSc

Informatics

Thesis title

Information Technology Change Risk Minimization: A Case of Using Global ServiceNow(GSN)

Objectives of thesis

The diploma thesis shows how to minimize IT change risk from an inability to manage system changes in a timely and controlled manner, especially during large and complex IT changes.

The main objective of this thesis is to evaluate risk minimization in the IT change management process in a selected company.

The partial objectives are:
- To comprehensively overview IT change management practices and current trends.
- To evaluate the efficiency of the risk management practices in a selected company.
- To analyze the impacts of using GSN in the selected company.
- To formulate recommendations and conclusions.

Methodology

The methodology of solving the theoretical part of the diploma thesis will be based on the study and analysis of professional information sources. The case study will use the ITIL as a reference framework and will be designed for a selected company. Based on the synthesis of theoretical knowledge and the results of the practical part, the recommendations and conclusions will be formulated.

The proposed extent of the thesis

80 pages

Keywords

ITIL, change management, risk assessment, mitigation, efficiency.

Recommended information sources

ALBULESCU, Mădălina; BIBU, Nicolae. Change Management Strategy and ITIL Implementation Process in an IT Company—Study Case. In: International Symposium in Management Innovation for Sustainable Management and Entrepreneurship . Springer, Cham, 2019. p. 611-621.

BACCARINI, David; SALM, Geoff; LOVE, Peter ED. Management of risks in information technology projects. Industrial Management & Data Systems , 2004.

GEADA, Nuno; ANUNCIAÇÃO, Pedro. Change Management Projects in Information Systems: The Impact of the Methodology Information Technology Infrastructure Library (ITIL). In: Handbook of Research on Emerging Technologies for Effective Project Management . IGI Global, 2020. p. 185-199.

GOMAN, Maksim. How to Improve Risk Management in IT Frameworks. In: 2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS). IEEE, 2021. p. 1-6.

HABER, Morey J.; HIBBERT, Brad. Risk Management Frameworks. In: Asset Attack Vectors. Apress, Berkeley, CA, 2018. p. 241-247.

Mahadi Hasan Miraz, January 2016"Change Management in Information Technology",Research Gate, IETI Transactions on Business and Management Sciences, 2016, Volume 1, Issue 1, 39-46. http://www.ieti.net/tc

N Senthil Kumar and Shailendra Narayana Rajan.Apr 2018,"Understanding the Change Management in the Information Technology (IT) Services Industry" Research Gate

---

Expected date of thesis defence

2022/23 SS – FEM

The Diploma Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 14. 11. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 28. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 17. 02. 2023

Declaration

I declare that I have worked on my master's thesis titled “Information Technology Change Risk Minimization: A Case of Using Global Service Now (GSN) " by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights.

In Prague on 31/03/2023

Ing. Haydiso Bereket Detamo, MSc

Acknowledgement

Firstly, I would like to my lord and saviour Jesus Christ. Then I would like to express my deepest appreciation to my thesis advisor Ing. Miloš Ulman, Ph.D for their invaluable guidance and support throughout the research process. Their insights, feedback, and constructive criticism were instrumental in shaping the direction and focus of my thesis.

My heartfelt thanks go to my wife Beza Zelalem, my beloved son Yeamlak Bereket and my family as a whole for their continuous support and understanding when undertaking my research and writing my project. Their love and belief in me were a constant source of inspiration, and I could not have completed this thesis without their support.

Finally, I would like to express my gratitude to all the participants who took the time to participate in this study and share their valuable insights, without whom this research would not have been possible. In the end, I will close by saying Thank you Jesus.

Abstract

This study explores the use of Global Service Now (GSN) to minimize risks associated with information technology (IT) change. The purpose of the research is to investigate the effectiveness of GSN in mitigating the risks associated with IT changes and by describing best feature of GSN for success of IT change implementation. The research did in selected company a case study approach, collecting data from a multinational organization that adopted GSN for managing IT change. The results of the study demonstrate that GSN is an effective tool for minimizing IT change risks, with significant reductions in risk and increased efficiency in managing IT changes. The study also identifies factors such as stakeholder involvement, communication, training, and customization that influence the success of GSN implementation. The findings provide insights into how organizations can effectively implement GSN for minimizing IT change risks and enhance their IT change management processes.

Keywords: ITIL, change management, risk assessment, mitigation, efficiency.

Table of Content

1 Introduction

Modern organizations and companies implement complex IT infrastructures through change management, which organizes how that infrastructure evolves consistently and safely. Managing changes in IT environments involves requesting, planning, deploying, and evaluating them. ITIL is a collection of best practices for managing IT infrastructures in an appropriate manner that addresses the issue of change management specifically(ITIL 2019).

This research paper focuses on the concept of IT change risk minimization in selected company by using Global Service Now (GSN). GSN is a cloud-based IT service management (ITSM) tool that enables organizations to manage and control their IT change management processes effectively(GSN 2021). The paper presents a case study of an organization that implemented GSN to minimize the risks associated with their IT changes. Each change must be performed and described in a document titled a Request for Change (RFC) according to ITIL Service Transition book(ITIL 2019).

This research paper's primary objective is to evaluate the efficiency of Global Service Now (GSN) works in reducing risks associated with IT changes implemented for specific period. Organizations must constantly modify their structural and functional traits in order to exist, survive, and remain competitive at any given time(Gabrie Onuche 2021). Group Information Security Standards and Requirements for Information Security Process in the Organizational Information Technology Risk Control for Managing Information Risks(S. Kumar 2021).

The paper begins with an overview of the change management process and by describing basic principles of successful change management. The study then discusses the how it change process is implemented by service management tool. The change implementation process of GSN and explaining in detail, highlighting the key features and benefits of the tool. The study concludes by evaluating the impact of GSN on risk minimization, including the benefits of using GSN for IT change management.

The study's findings show how successful GSN is at reducing the risks associated with IT changes and enhancing the environment's overall dependability and stability. The study's implications for organizational efficacy of their IT change management processes and minimizing the risks connected with IT changes discussed in the paper's conclusion. The report emphasizes the advantages of utilizing GSN for risk reduction in IT change management and offers insightful information for businesses looking to improve their IT change management procedures.

2 Objectives and Methodology

2.1 Objectives

The diploma thesis shows how to minimize IT change risk from an inability to manage system changes in a timely and controlled manner, especially during large and complex IT changes.

The main objective of this thesis is to evaluate risk minimization in the IT change management process in a selected company.

The partial objectives are:

- To comprehensively overview IT change management practices.
- To evaluate the efficiency of the risk management practices in a selected company.
- To analyse the impacts of using GSN in the selected company.
- To formulate recommendations and conclusions.

2.2 Methodology

The methodology of solving the theoretical part of the diploma thesis will based on the study and analysis of professional information sources. The case study will use the ITIL as a reference framework and will designed for a selected company. Based on the synthesis of theoretical knowledge and the results of the practical part, the recommendations and conclusions will formulated.

3 Literature Review

3.1 Change management

An organization's change management are the methods it uses to describe and implement change both internally and external(Lewis 2019). In addition, defined the coordination of a planned period of change from situation A to situation B to make changes that last in an organization. In a similar manner, change management refers to the procedures, techniques, and methods used to control the human element of organizational change in order to accomplish the desired business goal and realize organizational change successfully within the social framework of the workplace.(Passenheim 2010). This includes training and helps users, setting up the required change processes, and keeping an eye on pre- and post-change activities to guarantee successful implementation.

Change Operation in association are continually changing in response to both external pressures include changes of government, shifting policy dockets, governmental austerity measures or politically driven reforms, while internal pressures include the relinquishment of new practices in order to ameliorate affair and outgrowth effectiveness(Lewis 2019). In today's constantly changing environment, change operation has become one of the most important components for any business's success. There is a rapid-fire change in the business world technology is constantly evolving, consumer trends are changing, new request regulations are be introduced every day, and businesses are passing unknown global heads. In order to manage organizational change effectively, organizations/leaders/managers must manage and sustain employees' emotional trauma during organizational change programs. Additionally, they must offer ways to assist employees through this transition(Hanelt et al. 2021).

Significant organizational change can be gruelling(Caver and Livers 2021). It typically involves a variety of cooperative settings and could involve various separate realities inside an alliance. To ensure a positive transition while easing dislocation, developing an organized strategy to change is essential. Companies that cannot acclimatize and snare growth openings are likely to be outcompeted by nimble challengers and indeed vanish(Lewis 2019). That is why one of the top priorities should be getting ready for change. Changes typically fail for fundamental reasons because their proponents failed to consider the average people's healthy, actual, and predictable reactions to disruptions in their routine.(Cater-Steel and Toleman 2010). One of the most crucial success components for a successful change operation is excellent communication. All parties involved must comprehend the progression through the varied stages and observe the effects as the change occurs. Change operation is a process of overseeing and easing change at any position where it occurs. It is over to operation brigades to decide exactly how this change will be address, develop the process and how to best execute and apply(Lewis 2019).Well planned Organizational change management have many advantage for organization the overall importance described shown in fig 1.

Figure 1Organizational Change management important (Eisenhower 2019)

Organizational change management encompasses all of the methods, tools, and techniques that can assist you in preparing your employees, teams, and the entire organization for structural, strategic, technological, or cultural change(Eisenhower 2019). The purpose of every organizational change management initiative is to successfully implement strategies and methods for The purpose of every organizational change management initiative is to successfully implement strategies and methods for effecting change and helping people to accept and adapt to change(Cho et al. 2015). Teams for change management and change communication have grown to be essential performance drivers for many firms as organizational changes occur often in agile workplaces.

3.1.1 Benefits of Change Management

The goal of change management is to ensure that changes are smoothly implement and yield lasting benefits with as little resistance as possible. Making ensuring the affected parties accept the change is a crucial component of the process(Blackman et al. 2022). Change management in Information technology sector is one of the most studied and utilized elements of the systems and infrastructure management discipline. Most of Service Management expert, reports that in a recent survey of 40 corporate IT infrastructure managers a surprising 60% admitted that their processes to handle change are not effective in communicating and coordinating changes occurring within their production environment(Andrade, Albuquerque, and Teófilo 2016). If the employees not properly engaged, the project could rejected or even sabotaged, wasting time and money. You can reduce fear and anxiety by managing the people-side of the change.

The business environment of the twenty-first century marked by fast change because of technological, economic, political, and social changes. In this decade, managers and employees of firms cannot expect more of the same every year. Organizations that resist

change are doomed to obsolescence, which is so brutal that the only way out for many firms is to change or perish(El-taliawi 2020). As a result, organizations must develop capabilities for adapting and steering change to their advantage. Alter is the as it were consistent in commerce, and the scene of the 21st century is littered with companies that have not adjusted to the changing times.

The goal of Change Management is Plan and implement changes in a controlled and timely manner, Reduce the impact of change to the production environment ,Avoid disruption to business and one of a series essential change information to the proper stakeholders.

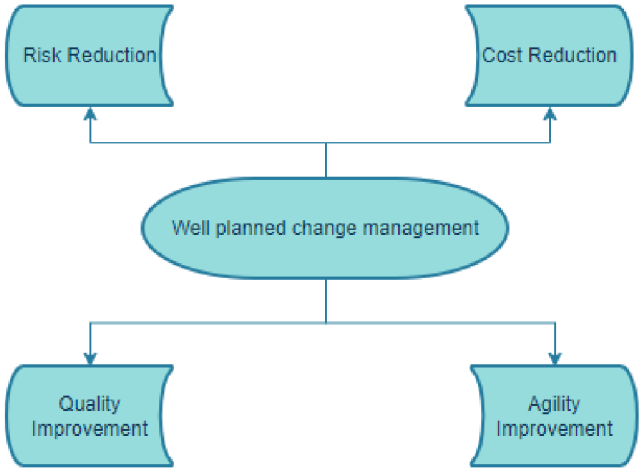

Figure 2 Importance of change management (author)

Within the modern commerce environment, organizations battle the fight of competition by building their versatile capabilities and readiness for adapting against the pressures of alter(El-taliawi 2020). Within the show situation, best administration grant a parcel of significance to alter administration prepare and require for being adaptable as well as versatile for handling the developing natural instabilities or competitive dangers. Change managements could be a complex prepare and requires genuine consideration as well as association from the administration and people from all levels, in arrange to realize an important or a dynamic change over different levels(Rousseau and ten Have 2022). Organizations have been concentrating on global company expansion, establishing excellence in procedures and operations, implementing innovations in technology, and identifying/developing the right talent in order to be ahead in the competitive race and obtain a winning advantage.

The quick changes, which have taken, put and the way in which this has influenced the procedures, individuals, arrangements and forms in an organization, it has ended up even more basic that organizations clearly set up a well-defined alter administration system for realizing the vital targets(Rousseau and ten Have 2022). Within the period of globalization,

organizations work over the social boundaries with huge speculations in human capital as well as physical assets, provide most extreme significance to mechanical alter and inventive hones for a authority advantage(N. S. Kumar and Rajan 2018). Commerce organizations together like mergers, acquisitions, diversifications, takeovers and different other collaborative ventures have ended up the foremost-preferred vital best hones for the organizations to outlive the furious powers of competition, through exchange of individuals, innovation, forms and administration. For effectively dealing with this move and changing over the dangers of alter into openings, organizations must be adaptable and open for Alter Administration.

Organizations can increase their adaptation mechanisms and develop internal capabilities for dealing with future uncertainties or several events that portend various changes by increasing their readiness for change(Petrikina et al. 2017). Because change management demands for a comprehensive, well-planned approach and the implementation of systemic interventions, which would have an overall impact on the system, processes, people, and the organizational structure as a whole, readiness for change management influences organizational strategies and policy-related decisions. Technology and research developments have made it possible to work nearly anywhere in the world. Changes in organizational hierarchy and structure, as well as in the laws and regulations governing human resources, have led to organizational reengineering and a shift in employee work habits(Petrikina et al. 2017). Flexibility in work hours, work from home opportunities, freelancing opportunities, virtual method of working, business operation outsourcing, project driven operations, etc. are just a few of the new working methods that more dynamic and flexible organizations have endorsed to meet the growing demands of ever-changing business operations. These methods give employees plenty of opportunities to work according to their convenience and flexibility.

3.1.2 Types of Change management in Organizational

Leading successful change requires creating a change strategy that fits the kind and scope of the change you are working on. Based on (Bulling 2018)three most common types of organizational change include:

1. **Developmental change**

An enterprise typically plans an experimental alternate to improve or correct a system in the association. Exemplifications of an experimental organizational change encompass perfecting the effectiveness of the employer is billing strategies or streamlining payroll processes. Experimental modifications are small, incremental developments or corrections in the way an affiliation conducts business(Bulling 2018). Some experimental adjustments are deliberate while others do because of outside influences. For illustration, expand in enterprise may additionally bear an enhancement in billing approaches to cope with the

redundant work. Any organizational interchange that enhances and optimizes on processes, strategies, and procedures that have previously connected.

2. Transitional change

A transitional change is Change that moves a company away from its present day state to a new state in order to remedy a problem, such as mergers and acquisitions and automation. It is additionally one in which a business enterprise replaces a current process or manner with a new one. The exchange requires the organization to phase out the historical method and put in force the new procedure. Other kinds of transitional alternate consist of constructing new products or imparting new services to customers. Businesses enforce a transitional alternate to reap a goal such as growing income or getting rid of waste.

3. Transformational change

A transitional change, such as a merger or acquisition or automation, involves moving a business from its current condition to a new one in order to address an issue. A transformational trade is one that involves both developmental and transitional adjustments and represents a significant change in the way an organization works. A corporation implements a transformational exchange over time across all areas of the business as shown in fig 3. The change results in a transformation in the subculture of the organization. Restructuring the company's enterprise strategy and redesigning its products or services are two examples of transformational change. Transformational exchange may be result of enormous decreases in revenue or will increase in competition.

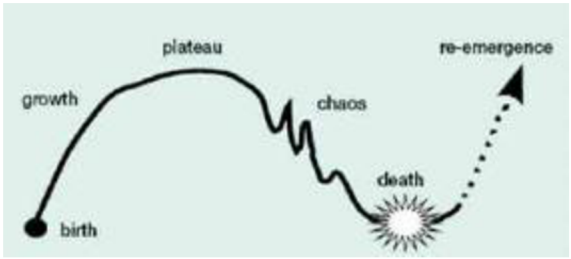

Figure 3.Transformational change(Beynon 2017)

3.2 Basic Principles of Successful Change Management

Organizational leaders should follow to change management principles successfully manage change, transitions, and disturbances within their organizations. Changes may be internal or external(Heckelman 2017). Effectively managing these transitions has steps Create a Climate for Change, Engage and Enable Change, Implement and Sustain Change, Review, and Reflect on Change in the trade administration procedure will increase success. Creating a climate for change, engaging and enabling change, implementing and sustaining change, and reviewing and reflecting on change are just a few of the fundamental principles that tend to be followed when implementing alternate administration in a proper way. The

trade management system customized based on the business and used in unique ways depending on the branch versus organizational levels. (Heckelman 2017).

For any company facing the prospect of change, the first step is to create a climate receptive to change(Zolghadr and Asgari 2016). Change can intimidate, or even frustrate, and it is quintessential for management to decrease resistance via speaking the significance of the change, guiding the teams where trade takes place and supplying a clear imaginative and prescient to jump-start the transition process. Communication and transparency on the "why" and "how" behind change are imperative for gaining worker have faith and buy-in for change. This helps personnel be proprietors and implementers of the change.

Once the climate is favourable for change, the next step is to engage and enable the organization to enact change. When change needed, it is important to assign responsibilities. Does this change require a specific person or group? Is it an organizational change implemented at different levels? If so, who is responsible for coordinating these different levels? The answers to each of these questions can help guide the change process and reduce uncertainty around accountability(Zolghadr and Asgari 2016). Therefore, it is important to keep communication open, transparent and clear. In addition, creating short-term wins can help to keep morale and enthusiasm at high levels.

With the business enterprise engaged and individuals and groups enabled and motivated, it is time to enforce and sustain the change. At this point, it is essential to preserve targeted and hold the pressure to reap the preferred outcome. This step can also appear rudimentary, then again the case that some managers can lose centre of attention and "ease up" throughout the process. If the target intention shifts during the exchange process, do now not hesitate to modify accordingly, transferring obligations or approaches to keep the force and focus sustained. Once the change implemented and the assignment has been complete, it is time to solidify the new status-quo and transition the enterprise from a state of flux to a country of permanence in order to sustain the change.

With the common principles in place, one closing step in the exchange management system is a review. Despite the fine efforts of management personnel to speak efficiently and accurate assign responsibilities, trade is a dynamic process. After completing a duration of transition, it is important to assessment the factors of your technique that did, or did not, work effectively, then analyse from the results. When your agency faces exchange in the future, it can be a benefit to have documented instances of previous procedures that have been most beneficial to your organization(Hansen 2008). With a trade management, team that has already pinpointed any preceding missteps and realized from mistakes, any new changes that occur can be approach with confidence, instead than worry or dread, as high-quality opportunities for the organization.

3.3 Change Management Best Practices

Change management best practices refer to the recommended approaches, techniques, and principles for effectively managing changes within an organization(ITIL 2019). Change management processes can be very complex. Additionally, change in the workplace can cause high levels of stress among employee. Based on the book ITIL recommended best practices regarding change management every organization should as follow.

1.Define clear goals

A well-defined change management plan outlines the specific steps that need to take in order to implement a change successfully, and provides guidance to all stakeholders involved in the process. Companies should make an effort to make the goals as clear as possible even though SMART goals for change management are challenging to articulate. As a result, when assessing change management activities, employees and managers can consult it.

2. Be honest and transparent

It is important for employers to prioritize transparency and honesty when dealing with employees. This can include regular sharing of updates and information about the company's activities, goals and challenges. Additionally, employers should strive to create a culture of openness where employees feel comfortable expressing concerns or questions without fear of retaliation. Employers must be honest and transparent to make the transition successful. Since most employees are uncomfortable with change, transparency in every step of the change management process helps build trust and commitment among employees.

3. Train and reassure your teams

Training and empowering your teams is an important aspect of effective leadership. Trust your employees, offer new training and give employees time to adjust to new ways of working. Empathy and trust help speed up the process and facilitate organizational change in the future.

4. Encourage conversations and communicate regularly

Employee relations have an important influence in shaping the conversations before, during and after the implementation of change. Start talking to your employees to find out how they feel about new initiatives. Realize that true communication is a two-way conversation.

5. **Listen to your employees**

If you are engaged in activities and communication, do not speak alone. Listen to what your employees have to say. Let them lead the conversation, where employees can ask questions, make comments, and offer ideas for improvement.

6. **Bring your leaders on board**

The evidence is clear - excellent change management drives business results from change initiatives. So why is it so difficult to convey these benefits to the leaders? Organizations must work to demonstrate the change management and communicate this to senior management to get them on board and supportive of the change.

7. **Choose the right communication tool**

Millennials expect an easier way to communicate than email at work. In fact, many emails never read and important information is lost. Choose the right employee communications and retention solutions that your employees will actually want to use. Make sure your solution is mobile-friendly. The younger generation is used to doing everything through their mobile phones. Therefore, the company's tools must be adapted for mobile devices.

8. **Empower your employees**

Give your employees the flexibility to make their own decisions and put new ideas into practice in order to empower your change management leaders and staff to participate in the change process. Your employees' engagement level will diminish if they do not feel empowered, which will lead to reluctance to change.

9. **Encourage knowledge sharing**

Some workers become familiar with and adjust to change more quickly than others do. However, sharing knowledge among employees can speed up this learning significantly. Employee collaboration tools make sharing company knowledge easy and fun.

10. **Document and make information easily accessible**

Documenting everything does not help if the information is not available to employees. A central location where all important documents and information are stored makes change management much more efficient. Did you know that workers spend an average of 2.5 hours a day searching for information (Statistics et al. 2022). In the change management process, this can be very frustrating and frustrating for employees.

11. Recognize and reward

Employee recognition and development is an important part of creating a positive and motivated team. Therefore, this approach can be a great incentive for compliance to implement changes more quickly. Recognize and reward employees for performing and adopting new behaviours in the change process. Celebrate victories and achievements.

12. Make it social

If you implement a new technology solution that you are proud of, spread the word. Modern employee communication tools make it easy for you and your employees to share information within and outside the company. Staff attorneys can also assist with talent recruitment and acquisition efforts.

3.4 The Evolution of IT change management

Changes in information systems personnel and information technology over the past seven decades (1950s-2010s)(Niederman, Ferratt, and Trauth 2016). IT change management has evolved significantly over the years. In the early days of IT, change management was often an ad-hoc process, with changes made on the fly without much thought given to potential risks or impact on the business. As IT systems became more complex and critical to business operations, organizations began to recognize the need for a more structured approach to change management.

Base on the book ITIL in the 1990s, ITIL (IT Infrastructure Library) emerged as a framework for IT service management, including change management(Lucio-Nieto and Colomo-Palacios 2012). ITIL provided a set of best practices and guidelines for managing IT changes, including identifying and assessing risks, defining change processes, and communicating and coordinating changes across the organization.

In the 2000s, IT change management continued to evolve with the emergence of new technologies and the increasing complexity of IT systems. Agile methodologies and DevOps practices began to gain traction, emphasizing a more collaborative and iterative approach to software development and deployment(Sacolick 2023). Change management processes were adapted to accommodate these new methodologies, with a focus on rapid and frequent changes.

Today, IT change management continues to evolve in response to new technologies and business needs. Cloud computing, artificial intelligence, and other emerging technologies are changing the way IT systems designed and managed, requiring new approaches to change management. The increasing importance of data privacy and security has led to a greater emphasis on risk assessment and mitigation in IT change management processes(Hoofnagle, Sloot, and Borgesius 2019). As organizations continue to rely on IT systems to support their business operations, effective change management processes will

remain critical to ensuring the smooth operation of these systems and minimizing the risks associated with IT changes.

3.5 Information Technology (IT) change management

IT Change Management has the objective to enable beneficial changes to make with minimal disruption to the live services, and without resulting into incidents. To this end, changes evaluated, prioritized, planned, tested, implemented and documented following a defined process. Information Technology (IT) change management is a structured process for reviewing proposed IT system or service changes(Sousa et al. 2019). This process occurs prior to implementing the requested change on an organization's network, thus minimizing or eliminating network outages. IT change management is necessary to ensure any changes to the network will not degrade the performance of the network. Any changes to the network should be a defined, purposeful action to eliminate a found vulnerability, upgrade a component on the network for improved performance, or replace a currently obsolete or faulty network component. IT Change Management is an IT Service Management (ITSM) process that makes it easier for your organization to roll out change requests to your IT infrastructure(Sousa et al. 2019). It helps your organization to request, prioritize, authorize, approve, schedule and implement any changes. Whether the change is complex or simple, a good IT Change Management process helps you to control risk and keep disruptions to your services to a minimum.

3.5.1 Benefits of IT Change Management

IT Change Management is a process for managing changes to an organization's information technology systems and applications in a structured and controlled way(Sousa et al. 2019). This process involves various stages, including planning, testing, approving, and implementing changes to minimize the risk of disruption to IT services and maintain business continuity. IT Change Management is a process used by organizations to ensure that changes to IT systems, infrastructure, and processes made in a controlled and systematic way, with the goal of minimizing disruption and reducing risk(Jaiswal 2019). The benefits of implementing an IT Change Management process include:

1. **Reduced risk**

One of the primary benefits of implementing an IT Change Management process is that it can help organizations reduce the risk of IT-related incidents, such as unplanned outages or data breaches(Jaiswal 2019). By following a formal process that includes planning, testing, and validation, organizations can identify and address potential issues before changes implemented. This can help minimize the chance of unintended consequences and reduce the risk of disruptions to business operations. In addition, by documenting changes and the steps taken to implement them, organizations can more easily

track and analyse the impact of changes, which can help inform future decision-making and improve overall IT operations(Wickboldt et al. 2009).

2. **Improved communication**

IT change management processes typically involve collaboration between different teams and stakeholders to ensure that changes implemented smoothly and with minimal disruption to business operations(Sousa et al. 2019). This collaboration helps to improve communication and ensure that everyone involved in the change process is aware of the goals and impacts of the changes. Collaboration can take many forms, such as regular meetings, cross-functional teams, or project management software that enables communication and collaboration across different teams and stakeholders.

By working together, teams and stakeholders can share information, identify potential issues, and develop solutions to mitigate risks and ensure that changes implemented successfully(Sousa et al. 2019). Effective collaboration also helps to ensure that everyone involved in the change process is aware of their roles and responsibilities, as well as any dependencies or interdependencies between different teams and stakeholders. This improves communication and helps to ensure that everyone aligned on the goals and impacts of changes, which in turn helps to minimize the risk and impact of changes on business operations.

3. **Increased efficiency**

IT change management can help organizations become more efficient and agile by streamlining the change process and reducing the chance of errors(Cho et al. 2015). IT change management process, organizations can ensure that changes implemented smoothly, efficiently, and with minimal disruption to business operations. This helps to reduce downtime and increase productivity by minimizing the impact of changes on critical systems and services

In addition, companies may execute changes more quickly and confidently, helping them remain ahead of rivals and meet the changing needs of their customers, by identifying possible problems and creating solutions to reduce risks. Ultimately, by reducing downtime, increasing productivity, and improving customer satisfaction, IT change management can help organizations become more efficient and agile, which can lead to greater success and profitability in the end.

4. **Compliance**

IT change management can help organizations meet regulatory and compliance requirements related to data security and privacy. Many regulatory and compliance requirements require organizations to implement strict controls around changes to IT systems and services(Saeidi et al. 2019). Structured IT change management process,

organizations can ensure that changes implemented in a controlled and secure manner, with appropriate testing and approvals, which helps to reduce the risk of non-compliance. IT change management can play an important role in helping organizations meet regulatory and compliance requirements related to data security and privacy by providing a structured and controlled approach to managing changes to IT systems and service.

5. Continuous improvement

IT Change Management processes typically involve a continuous feedback loop to ensure that any issues or problems that arise during the change process addressed and resolved quickly(Sousa et al. 2019). This feedback loop allows organizations to continually improve their processes, make necessary adjustments, and ultimately become more resilient and adaptable to changing business needs.

The feedback loop typically involves collecting feedback from stakeholders involved in the change process, analysing the feedback to identify areas for improvement, and then taking action to implement changes and address any issues that identified. By continually refining and improving the change management process, organizations can better manage risk, minimize disruptions, and ensure that changes delivered smoothly and efficiently(Rousseau and ten Have 2022). This, in turn, can help organizations become more agile and responsive to changing business needs, enabling them to remain competitive and succeed in the long term.

In addition to this IT Change Management, there are a number of benefits like Implement changes more quickly, track the progress of changes to your IT infrastructure, easily trace the roll-out of any changes if something goes wrong and Improve cost estimate for any proposed changes.

3.6 IT Change Management Risks

IT change management risk refers to the potential negative consequences associated with changes made to an organization's IT infrastructure or applications(Jaiswal 2019). Change management is the process of planning, implementing, and evaluating changes to IT systems in a controlled and systematic manner to minimize the risk of disruptions or negative impacts on business operations. However, despite careful planning and execution, changes to IT systems can still result in unexpected risks and consequences. These risks can include system failures, data loss, security breaches, and reduced productivity. IT change management risk is the risk that these negative outcomes will occur because of changes to an organization's IT systems(Sousa et al. 2019).

To mitigate IT change management risks, organizations typically use a variety of processes and tools to manage changes in a controlled and structured way. This may include testing and validation processes, change authorization processes, documentation and communication processes, and monitoring and feedback processes. By managing changes in

this way, organizations can reduce the risk of negative impacts on their IT systems and business operations. IT change is not something that can happen instantly or in a single step. IT change is a process that requires careful planning, testing, and implementation in order to minimize the risk of disruption to IT services and maintain business continuity (Bulling 2018). Within the current commerce environment, a well thought-out and orderly change management prepare is not optional; or maybe, it is essential for an organization to successfully accomplish its commerce targets. Change management can be characterize as the efficient set of forms that are executed inside an organization's IT work to oversee upgrades, overhauls, establishments, usage, incremental fixes, and patches to generation frameworks.

Risk management is a related ITIL 4 practice, followed to ensure the organization understands and effectively manages the risks associated with IT change management (ITIL 2019). Tracking and linking changes is necessary for both change management and risk management to produce an auditable record. Organizations can modify their procedures in a way that skilfully balances risk and speed by having access to data on past changes and their success rates. Data-informed, adaptive practices attempt for efficiency, in contrast with common exchange management, that can regularly be unnecessarily slow, process-heavy, and overburdened(Hoofnagle, Sloot, and Borgesius 2019). Change management all too frequently becomes complex, bureaucratic, and painful because it deals with issues like risk and compliance, auditability, and cross-team cooperation.

In ITSM, trade administration is the "eat your vegetables" part -- no longer appealing, but still vital. With the proper practices and culture, change administration can result in fewer incidents, much less stress on your teams, and greater time spent delivering fee to customers(Cater-Steel and Toleman 2010).

IT change management is the process of managing changes to an organization's IT infrastructure, software, applications, and services. However, change can bring about risks and challenges that need to manage effectively. General Risks like poor change management program can expose an organization to many risks, including the implementation of unauthorized or undocumented changes, system or application failures, security issues, inefficient business processes, conflicting results, and even inaccurate reporting and financial statements (Jaiswal 2019).

In addition, inefficient change management can cost a company failure to meet corporate goals and control flaws that could lead to inconsistent compliance or unfavorable audit outcomes(Sousa et al. 2019). Also, cause poor quality systems that can hinder employee productivity or frustrate customers and missed opportunities to provide innovative or more efficient products and services to Customers. Outages, unplanned work, and inability to test and apply necessary updates can result in the introduction of new, serious security vulnerabilities or the reemergence of old ones. When there is insufficient IT change management, the organization is not appropriately included in the change approval board

and process, which raises the possibility that change, may interfere with the completion of a crucial business activity. System modifications that do not take the needs of the process owner into account, leading to processing problems, lost time from having to redo work, and other undesirable effects(IRM 2011).

3.7 Source Risk in IT Chance Management

Source failure in IT change management refers to the failure of the processes, tools, or people responsible for implementing changes to an organization's IT systems(Saeidi et al. 2019). Source failure can occur at any stage of the change management process, from planning and design to testing, implementation, and evaluation. Some types of failure are recurrent on change deployment processes and may be capture by the management system during run-time. Identifying source and classification of failures is important to help the operator understanding the behavior of problematic items and for what reasons they fail. The proposed failure classification is based on(Russell, Van Der Aalst, and Ter Hofstede 2006), all failure in IT change management could raise from listed categories.

3.7.1 Activity Failure (AF)

Activity failures in IT change management refer to the failure of specific activities within the change management process(Lewis 2019). The change management process typically involves several key activities, including planning, testing, implementation, and evaluation. Activity failures can occur at any stage of the process and can lead to delays, errors, and ultimately failure in the overall change management process. Activity Failures of this type happen for reasons intrinsic to the execution of activities in the change plan. Usually, they occur during the installation or configuration of software elements. In addition, they may be triggered by failures other activities on the workflow(Machado et al. 2008).

Some examples of activity failures in IT change management include:

- Incomplete or inadequate planning is failing to plan for all aspects of the change, including potential risks and impacts, can lead to implementation failure.
- Poorly executed testing is failing ailing to test the changes thoroughly can result in unexpected consequences or system failures.
- Inadequate communication failing is due to communicate changes effectively to all stakeholders can lead to misunderstandings and resistance, causing delays or errors.
- Insufficient resources failing due to allocate sufficient resources, including staff, budget, and time, can lead to rushed or incomplete activities, resulting in errors and failures.
- Ineffective implementation failing due to implement changes correctly can lead to system failures or negative impacts on business operations.

3.7.2 Human Failure (HF)

Human failure in IT change management refers to the errors and mistakes made by people involved in the change management process(Cater-Steel and Toleman 2010). These errors can range from simple data entry mistakes to more complex failures to follow establish procedures or guidelines. Human failure is a common cause of IT change management problems and can result in system failures, data loss, and other negative impacts on business operations. Humans, therefore, perform some activities on a change plan when humans do not behave the way supposed to, and then human failures have to be raised(Jaiswal 2019). Failures on manual activities, for example, should to be record on the system even if there is no way of capturing it automatically. In these cases, the operator should insert the records to keep the history of changes as accurate as possible

Some examples of human failure in IT change management include:

- Miscommunication Failing is due to communicate effectively, including not providing clear instructions or not receiving clear instructions, can lead to misunderstandings and errors.
- Inadequate training is due to train staff involved in the change management process can lead to errors and mistakes due to a lack of knowledge or understanding.
- Lack of attention to detail is failing to pay close attention to details, such as configuration settings or data inputs, can lead to errors and system failures.
- Poor decision-making failing due to make informed decisions based on all available information can lead to the wrong choices and negative impacts.
- Non-compliance Failing to follow established procedures or guidelines can lead to errors, omissions, or oversights that can result in system failures or data loss.

3.7.3 Time Failure (TF)

Time failure is a critical issue in IT chance management process. It refers to situations where the IT team is unable to complete a task within the expected timeframe, which can have serious consequences for the organization's IT infrastructure and operations(Dempsey et al. 2022). In IT chance management process, time failure can occur due to various reasons such as lack of resources, insufficient planning, poor project management, or unexpected events such as system failures or security breaches. To mitigate the risk of time failure, IT teams should have a comprehensive understanding of the project scope, timeline, and available resources(Rudnev 2020). They should also be proactive in identifying potential risks and developing contingency plans to address them. When needed, deadlines specified to inform when activities should be finished.

Effective communication is also essential in preventing time failure(Jaiswal 2019). The IT team should have open channels of communication with stakeholders, including business leaders and end-users, to ensure that everyone is aware of project timelines and any

potential delays. Regular progress updates and status reports can help keep everyone informed and identify issues before they become major problems.

3.7.4 External Trigger (ET)

An external trigger in IT chance management process refers to an event or situation that originates outside of the organization but has the potential to Impact its IT infrastructure, operations, or business continuity(Araujo Wickboldt et al. 2009). External triggers can come from a variety of sources, including competitors, regulatory changes, natural disasters, cyber-attacks, or changes in customer behavior.IT teams need to be vigilant and responsive to external triggers to minimize the impact on the organization(Bianchin et al. 2010). They should have processes in place to identify and assess the potential risks associated with external triggers, and develop contingency plans to mitigate them. This type of failure occurs when some agent, external to the change process, interrupts the regular execution of the change plan. This could be a signal injected into the system by an external administrator user, informing that the workflow must interrupted for any reason.

3.7.5 Constraint Violation (CV)

In IT chance management process, a constraint violation refers to a situation where a project constraint, such as time, budget, scope, quality, or resources, exceeded or compromised(Saeidi et al. 2019). Constraint violations can have significant consequences for the project's success, including delays, cost overruns, decreased quality, and potential project failure. Usually, it happens when an activity in the change plan needs to perform an operation that violates any of the organization’s policies. Moreover, these failures raised by conflicting scheduling of changes(Lucio-Nieto and Colomo-Palacios 2012).

To avoid constraint violations in IT chance management process, IT teams should take the following steps:

- Define clear project constraints, means IT teams should define clear project constraints upfront and ensure that all stakeholders understand them. This includes setting realistic timelines, budgets, and scope, and identifying the resources needed to achieve project goals.
- Conduct regular risk assessments can help identify potential constraint violations before they occur. IT teams can use risk assessment frameworks, such as SWOT analysis or PEST analysis, to identify and prioritize risks, and develop appropriate risk response strategies.
- Implement effective project management practices can help ensure that project constraints managed effectively. This includes developing detailed project plans, monitoring project progress, and tracking project costs and timelines.
- Communicate effectively with stakeholders is essential in avoiding constraint violations. IT teams should keep stakeholders informed about project progress,

including any potential risks or issues that Impact project constraints. Regular progress updates and status reports can help keep everyone informed and identify issues before they become major problems.

- Develop contingency plans should be developed in advance to mitigate the impact of constraint violations. For example, if a project is at risk of exceeding its budget, IT teams can identify alternative funding sources or prioritize project activities to stay within budget.

3.8 IT Change process by Global Service Now

GSN which is a cloud-based platform that provides various IT service management (ITSM) solutions, there are different types of changes that can be implemented using the Service Now Change Management module(GSN 2021). All Changes shall be managed according to the Change Management Process as implemented in the Global Service Now (GSN) toolset provided by ITS(ITIL 2019). The change management process implemented in GSN used to make sure that the all individuals involved in the change management process follow the same rules and apply the same criteria when they evaluate changes and when they maintain the change records in the GSN tool(GSN 2021).

The type of change in GSN

1. Standard changes or Preauthorized
2. Non-standard changes.
3. Emergency change
4. Critical Changes

3.8.1 Preauthorized

A preauthorized change typically refers to an agreement between a consumer and a service provider, such as a subscription service, to automatically renew or update an existing service without requiring the consumer to take any additional action. Preauthorized and non-standard changes are subject to the change management process and managed as RFC records in GSN, while the fulfilment of requests for standard changes is not(GSN 2021). Regular adjustments are routine and adhere to a set procedure for risk analysis and prior permissions. These adjustments are pre-approved procedures that have undergone testing. It is important to read and understand the terms and conditions of any agreement you enter into with a service provider to ensure that you are aware of any preauthorized changes that may occur. Additionally, it is important and regularly review your billing statements to ensure that you not charged for services no longer wish to receive or that you did not authorize.

Preauthorized and standard changes do not require individual case-by-case authorization:

- The authority to make standard adjustments given to the service owner.
- Every preauthorized change detailed in the GSN Request Catalogue.

Ticket	Type	Authorized by
Incident	Request for Standard change(RFSC)	Service owner
Change Request	Preauthorized	Service owner

Table 1Preauthorized change type and Authorization (GSN 2021)

Conditions for Preauthorized changes

A change request considered a Preauthorized Change if the following conditions met:

- The change has a low impact and risk, non-disruptive, and is easy to reverse.
- Failure to make the change will only affect the unit making the request.
- A minimum of three full implementations of the change must be successful.
- The modification has approved following a CAB meeting.
- The modification added to the Request Catalogue and made available as a template in the GSN of this document for guidelines on the composition of Change Approval Boards (CAB).

3.8.2 Standard Change

Standard changes are pre-approved changes that routinely performed and have a low level of risk and impact on the system. These changes are typically straightforward and do not require additional assessment and evaluation before implementation. It is a change that not requires a more detailed assessment of its impact and risks and may not require a higher level of authorization and resources than a standard change (Servicenow 2019). These changes are usually documented in a standard change procedure or change model and do not require extensive assessment.

3.8.2.1 Request for Standard Change

Requests for Standard Change are those that have a predictable outcome and do not require extensive evaluation or approval(Servicenow 2019). Examples of standard changes might include adding a new user to a system, changing the configuration of an application, or installing a security patch. These changes have a well-defined procedure and are typically low-risk, so they can approved and fulfilled without going through the full change management process.

The goal of automating the fulfilment of Requests for Standard Change is to streamline the process and reduce the workload for IT staff. By automating these requests, organizations can ensure that standard changes processed quickly and efficiently, without requiring manual intervention from IT staff. This can help reduce the risk of errors or delays in processing standard changes, which can help improve the overall reliability and availability of IT services.

However, it is important to note that while standard changes may not require the same level of evaluation and approval as other types of changes, they should still be recorded and tracked to ensure that they properly documented and can audited if necessary. Additionally, organizations should have clear policies and procedures in place for identifying and managing standard changes, to ensure that all changes processed in a consistent and standardized manner.

Standard Change Indication in GSN(GSN 2021)

- Incident type "Request for Standard Change" ticket in GSN.
- Preferably raised by the end user through Request IT
- This type of change advised for those who perform changes frequently.

Conditions for Standard Change

A change considered a Request for Standard Change if and only if the following conditions met(GSN 2021):

- Roll back is completely documented, tested, repeatable, and dependable.
- It is a non-disruptive change with low impact and risk.
- Only one group is responsible for implementing the change
- Users other than the requestor or the team representing will be unaffected if the change fails.

In ITIL best practice, requests for standard changes are typically managed through the Request Fulfilment process, rather than the Change Management process(Lucio-Nieto and Colomo-Palacios 2012). This is because standard changes are usually low-risk and have a well-defined procedure, and therefore do not require the same level of evaluation and approval as other types of changes.

In GSN (Global Service Now), the technical implementation of this reflected by the fact that requests for standard change are treated as Incident (INC) objects, rather than Request for Change (RFC) objects(GSN 2021). This is because users typically initiate requests for standard change as a request for service or assistance, rather than as a request to modify the IT environment.

By treating standard changes as incidents, organizations can use the Incident Management process too quickly and efficiently process requests for standard changes, without requiring the same level of evaluation and approval as other types of changes. This can help improve the overall efficiency of the IT service management process, while still ensuring that standard changes properly documented and tracked for auditing and compliance purposes.

3.8.3 Non-standard changes

A non-standard change is a type of change that falls outside of the pre-approved and standardized change management processes and procedures in an organization. It is a change that requires a more detailed assessment of its impact and risks and may require a higher level of authorization and resources than a standard change. Non-standard changes are typically more complex and can have a greater impact on an organization's operations, processes, and systems(Servicenow 2019). These types of changes may include major system upgrades or modifications, changes to critical infrastructure or applications, or changes that affect a large number of users.

Non-standard changes are changes that deviate from the standard procedures and required additional assessment and evaluation before implementation. The responsible person for minor changes authorized by the Change Manager based on technical reviews and significant and major changes presented and discussed at the Change Advisory Board (CAB) meeting (Servicenow 2019). Because of the potential impact of major changes, they typically require a more formalized change approval process. This may involve a change advisory board (CAB) to review and approve the change before it can implemented. The CAB may include representatives from various IT teams, as well as business stakeholders who may impacted by the change. The CAB is responsible for assessing the potential impact of the change, identifying any risks or issues, and ensuring that the change aligned with the overall business objectives.

Because non-standard changes are more complex and can have a greater impact on an organization, they require a more rigorous change management process(Cater-Steel and Toleman 2010). This may include additional planning and assessment, risk management, testing, and communication with stakeholders. To manage non-standard changes effectively, organizations may have a separate process and team responsible for handling these changes. This team may include experts in the relevant areas, such as technology, operations, or security, who can provide guidance and expertise on the impact and risks associated with the change. Non-standard changes require a higher level of scrutiny and control than standard changes to ensure they implemented successfully without disrupting the organization's operations(Cater-Steel and Toleman 2010). These are all changes, which are not simple user requests, and which are not list in the request catalogue(Servicenow 2019). Change impact reflects the scope and the complexity of a particular change. It determines the necessary authorization level.

Minor change

Minor changes are typically changes that have a low impact on the IT environment and do not require extensive review or approval. These changes may be authorized by the Change Manager based on technical reviews and may not require a CAB meeting. However, the Change Manager is responsible for ensuring that all changes, including minor changes,

are recorded, assessed, and evaluated to ensure that they are appropriate and do not pose a risk to the IT environment.

Characteristics of minor change can identified

- The change has an impact on minor, non-critical aspects of the business.
- The change rollback process is simple and quick.
- The change has no effect on the business.
- Typically, only one group implements the change.
- The failure of the change has no effect on other services or customers, and

Significant change

Significant changes, on the other hand, are changes that have a high impact on the IT environment and require extensive review and approval. These changes are typically presented and discussed at a CAB meeting, where representatives from various departments and stakeholders evaluate the proposed changes and determine whether they should be approved or not. The Change Manager is responsible for managing the CAB meeting and ensuring that all significant and major changes must properly evaluated and approved before implementation.

Characteristics of Significant change can identified

- The update requires server reboot or application restart,
- The modification poses a serious risk to services and has a major impact,
- The change can result in the company's IT services going down.
- The change implemented with the cooperation of various departments.

Major change

Major changes are changes that have a significant impact on IT systems or the business and may require more extensive planning, testing, and approval processes. These changes are typically larger in scope and may require more resources and effort to implement. Major changes could include the implementation of a new IT system, a significant upgrade or update to an existing system, or a major change to the IT infrastructure(Cater-Steel and Toleman 2010).

Characteristics of major change can identified

- The ability to roll back a change is extremely difficult or non-existent.
- The change Impact a crucial area of the company's operations and carries a considerable risk of disrupting essential Services.
- A significant number of users or a system that is essential to business operations could impacted by the change.

Ticket	Type	Authorized by
Change Request	Minor change	Change manager
Change Request	Significant change	CAB Advisory Board
Change Request	Major change	CAB Advisory Board

Table 2 Non-standard changes type and Authorization (author)

3.8.4 Emergency Changes

Emergency changes are changes that made outside of the normal change management process in response to a critical situation or urgent need(Savajia 2021). They typically used when there is an immediate need to restore service or to address a critical security issue. While emergency changes can be necessary in some situations, they also pose a higher risk to the service and the organization as a whole. This is because emergency changes often made without the same level of evaluation, testing, and approval that is required for normal changes.

Conditions for Emergency changes based on (Savajia 2021)

- Unplanned preventive actions that must be implemented right now to avert business impact,
- Unplanned changes where prompt adoption is necessary to end an ongoing emergency incident.

When compared to the standard change management process, the emergency change process has the following differences:

- The emergency incident bridge's members who are authorized approvers or who represent an authorized approver provide their consent.
- The service owner conducts risk assessment in a quick manner.
- Only the RTP plan, not all of the standard approval requirements, are necessary for emergency revisions.
- Critical preventive emergency changes require approval from an Emergency CAB.

3.8.5 Critical Changes

Critical changes determined by the combination of impact and risk. Changes with very high risk are always critical(Prosci 2018). Changes with high risk and major impact are also always critical. In addition, changes with major or significant impact are critical if a service for a critical customer affected by the scope of the change.

Which customer considered as a critical customer relies on the professional judgment of the regions, and can change over time. As a rule, critical customers are ones with high revenue, penalty clauses, where has the opportunity to win more business, visibility to the public, sensitive data, or similar criteria. It should documented by each region, which are their critical customers.

The process for critical changes differs from the normal change management process in that(GSN 2021)

- It is mandatory to do peer reviews of the intended changes (including but not limited to software code, configuration settings, hardware installation) before the change is executed
- It is mandatory to follow the four eyes principle when the change executed.
- Availability of post-implementation support from all involved suppliers has to be ensured
- The customer must be notified before the change is executed

Implementing a specialized change management process for critical changes, organizations can help to ensure that these changes managed in a controlled and transparent manner, and that they do not cause unexpected disruptions or outages. It is important to note that the specifics of the critical change process may vary depending on the nature of the organization and the services provided. Approval by the responsible Global member is required for critical changes(Savajia 2021).

3.9 A Change Advisory Board (CAB)

A Change Advisory Board (CAB) consists of members from an organization that authorized to review and assess the risks for all IT change requests(Savajia 2021). A CAB can reject an IT change request if it is lacking information crucial to the submitted change request, or if all the risk factors not properly addressed.

Base on Service Now guideline(Savajia 2021) the CAB requires the following information to do a rigorous risk assessment:

- A description of the IT Change request to released
- The test results from user acceptance testing
- The test sign-off that applicable systems or systems integration is successful and completed
- The deployment plan and the rollback plan
- A questions and answers session with project or test managers to address all CAB concerns

The CAB's sole purpose is to ensure the integrity of the network remains intact and operational after the IT change request sent to release management for implementation. It

consists of representatives from all groups impacted by the potential changes(Savajia 2021). The Change Manager, Operations Manager, Information Security Officer, Senior Network Administrator, Service Desk Manager, and the Application Manager, if applicable, should be the bare minimum members of the CAB. Each member has an equal vote in the CAB process.

3.10 Roles in Change Management

In Change Management, there are several roles involved in managing changes, including the Requestor, Change Manager, Approver, and Implementer(Prosci 2018). The Requestor is the person who initiates the change request. They identify the need for change and submit a formal request for change to the Change Manager. The Requestor is responsible for providing all necessary information about the change request, including the scope, impact, and benefits(Prosci 2018). The Change Manager is responsible for managing the change process from start to finish. They review the change request and assess its impact on the organization's operations, processes, and systems. The Change Manager is responsible for coordinating with all stakeholders involved in the change process and ensuring that the change implemented successfully.

The Approver is responsible for reviewing and approving the change request. Depending on the scope and complexity of the change, there may be multiple Approvers involved. Approvers may include stakeholders from different departments or areas of the organization who have the authority to approve the change(Andrade, Albuquerque, and Teófilo 2016). The Implementer is responsible for implementing the change. They ensure that the change implemented as per the approved plan and that all necessary testing and validation performed before the change released into production. The Implementer may also be responsible for providing training to end-users to ensure a smooth transition to the new processes, systems, or tools introduced by the change.

Effective collaboration and communication among all stakeholders involved in the change process are essential to ensure that the change implemented successfully and delivers the desired outcomes. Each role in change management plays a critical role in ensuring that changes implemented smoothly and with minimal disruption to the organization's operations. Based on(Prosci 2018) in the table 3 below shows the role ,responsibility and activity of change management role each IT change request.

Role		Activities
Requestor	• Business IT, • Project Manager, • Release Manager, • Service Owner, • Hosting Service Owner, • Solution Support	• Create Change Request in GSN • Provide full documentation, • Implementation detail of release to production, communication plane, back out plan • Impact assessment and Risk analysis and mitigation method • Fulfil change advisory board(CAB) criteria • Clarify concern of approver • Communicate implementation result • Provide post implementation review
Change management	• Change Analyst • Change manager	• Filter and control of RFCs • Review of Urgent or Emergency Justification • Initiate Approval process • Chair the CAB and Appoints Emergency committee • Check the change collision • Review and closure of RFC • Reporting on changes
Approver	• Technical Expert • Service Owner • CAB members • Business IT Representative	• Review the RFC and all document • Technical expertise and capacity check • Impact assessment and Risk analysis • Change the change collision • Approval behalf of business partner
Implementer	• IT service staff • Business IT • Vendor	• Check the RFC approved or not • Implementation of change • Roll back in case of Issue • Provide about feedback about change implementation result

Table 3Roles in Change Management in IT change management process(Prosci 2018)

3.10.1 Change Management Process as implemented in GSN

Change management process in Global service now is a comprehensive process that designed to manage and control changes to IT infrastructure, applications, and services across an organization(GSN 2021). The Global Service Now change management process

built on ITIL best practices, and designed to ensure that changes implemented with minimal disruption to the business while maintaining service availability and performance(ITIL 2019). All Changes shall be managed according to the Change Management Process as implemented in the Global Service Now (GSN) toolset provided by ITS.

The Release to Production (RTP) plan also include a back out plan, which specifies how a roll back is to executed of, needed. This includes a statement as to how the roll back decision taken. The roll back procedure has to be tested, and the tests signed off, as part of testing the change.

It is good practice that if a change triggered by one or more incidents or problems, to link the respective INC and records are linked to the RFC record in GSN(GSN 2021). Business partners, customers and suppliers shall appropriately informed about Changes that may affect them or their services. The change manager is responsible for the information flow to these stakeholders. In addition, the change manager has to make sure that all necessary documentation provided for the CAB decision, namely Risk analysis and mitigation actions, implementation details, communication plan and back out plan. Also responsible for monitor the RFC for any pending tasks and make sure all concerns of approvers clarified.

Based on(Service now 2019) the service now change management process typically follows the following steps:

1) Change request submission

Authorized users through a self-service portal, email, or other channels can submit change requests. The request includes details about the proposed change, such as the reason for the change, the impact on services, and the proposed implementation date. In IT chance management process, a change request submission is a formal request made by a stakeholder to introduce changes to an IT system, service, or product. Change requests can originate from different sources, including end-users, customers, stakeholders, or IT staff, and they can initiated for various reasons, such as correcting errors, improving performance, or adding new features.

2) Risk and Impact assessment

A change manager who evaluates the request and determines whether it meets the criteria for approval reviews the change request. The criteria may include assessing the impact of the change, evaluating the risks and benefits, and ensuring that the change aligned with business objectives. Risk and impact assessment is a crucial step in IT change management process on this stage. It involves evaluating the potential risks and impact of a proposed change before it implemented. By performing a risk and impact assessment, IT teams can identify potential issues and take measures to mitigate them before they cause disruptions to IT systems or services.

3) Change approval

Change approval is a critical step in IT change management process. It involves the review and approval of a proposed change by the appropriate stakeholders before it implemented. The change approval process ensures that proposed changes evaluated for their potential impact on IT systems, services, or products and aligned with the organization's goals and objectives(Prosci 2018). Once the change manager approves the change request, it assigned to a change owner who is responsible for coordinating the change implementation. The change owner works with stakeholders, such as application owners and infrastructure teams, to develop a detailed change plan that includes timelines, resources, and testing requirements. No Change should be implement without proper approval. The Change Manager based on technical reviews authorizes changes with minor impact. Significant and Major changes must be presented to and approved by a Change Approval Boards (CAB).

Change Approval Boards (CAB) are principally service specific. The Regions or Centre of Excellence (CoE) can however set up CAB, which covers a number of different services. The roles which have to be represented in the CAB depend on whether the respective services are owned by ITS.

4) Change implementation

The change implementation stage involves making the approved changes to the IT infrastructure. During this stage, the change planned, executed, and tested in a controlled environment to ensure that it works as intended and does not cause any unexpected problems. It typically conducted during a scheduled maintenance window to minimize disruption to services. The change owner oversees the implementation and ensures that all stakeholders are inform of the progress(Prosci 2018). The implementation process may involve coordinating with various teams, such as developers, network engineers, and IT operations staff, to ensure that the change is implement smoothly and with minimal disruption to business operations. Once the change has been implement, it is typically testing to ensure that it is working as expected, and any issues that arise addressed promptly. Depending on the scope and complexity of the change, implementation may involve multiple IT teams and may require coordination with business units and external vendors.

5) Change Closure

After the change implemented, it reviewed to ensure that it was successful and that services are operating as expected. The change owner prepares a post-implementation review report, which reviewed by the change manager. The change request is then closed, and the change management database updated with the details of the change. All Changes categorized as any failed changes, and any identified unauthorized changes shall be subject to a Post Implementation Review. Changes closed in GSN after their implementation (resp.

after the attempted implementation in case of a failed change). If a Post Implementation Review is required, then it has done within this timeframe. The change manager organizes the Post Implementation Review. Input must asked from and provided a responsible person from the assigned team for each implementation task. In addition, the Requestor has to provide input for the Post Implementation Review.

The result of a Post Implementation review is an analysis, which describes identified root causes, lessons learnt and preventive measures to avoid similar failures in the future. This analysis shared with the Business IT stakeholders; typically as part of the Service Reviews.

Based on current guild service (GSN 2021) In GSN, a change is considered unsuccessful if

- ❑ The change could not implemented because a problem occurred during the implementation process.
- ❑ The change made, however it did not accomplish what it planned to. That means the change implemented, but it did not achieve its goal.
- ❑ The change implemented, but it resulted in emergencies.
- ❑ The change was implemented but then rolled back

Any incidents caused by a change had linked to this change in the GSN tool. Rollback means putting back to the original state. The decision to roll back taken based on the estimated time to fix the issues in the context of the criticality of service. The originally planned downtime can extended by a certain number of hours, but this needs to be predefined, so that if the forecasted estimate time to fix exceeds that of the maximum tolerable extension, then the changed is rolled back.

In GSN, there is an additional closure code for RFCs to recognize rollback from other failed states. As a general rule,

1. One change task closed as rollback but RFC was successfully implemented RFC will be closed as failed in order to highlight complications in RFC
2. One or more change tasks are closed as rollback and the whole RFC has rolled back RFC will be closed with closure code Rollback.

It is good practice for the change manager to inform stakeholders of any failed changes, particularly if they have rolled back. This allows stakeholders to be aware of any potential impacts on the services they are responsible for and to take appropriate actions if necessary. By consistently identifying and addressing the root causes of failed changes, organizations can improve the reliability and stability of their services, and minimize the risk of service disruptions caused by changes.

When a change fails and is rolled back, it is important to identify the root cause of the failure so that appropriate corrective actions can take to prevent similar failures in the

future. The service owner is typically responsible for investigating and producing the root cause analysis for the failure. This involves identifying the underlying reason for the failure, determining what went wrong during the change process, and assessing the impact of the failure on the service.

3.11 Summary of Literature review

Change management is coordination of a structured period of transition from situation A to situation B in order to achieve lasting change within an organization. The goal of Change Management is Plan and implement changes in a controlled and timely manner, Reduce the impact of change to the production environment ,Avoid disruption to business and one of a series essential change information to the proper stakeholders. Benefits of IT Change Management are reduced risk, improved communication, increased efficiency, continuous improvement and help organizations meet regulatory and compliance requirements related to data security and privacy.

Source failure in IT change management refers to the failure of the processes, tools, or people responsible for implementing changes to an organization's IT systems. The source of failure include Activity Failure, Human Failure, Time Failure, External Trigger and Constraint Violation. Risk management is a related ITIL 4 practice, followed to ensure the organization understands and effectively handles risks. Both change and risk management require tracking and linking changes to provide an auditable record. All Changes shall managed according to the Change Management Process as implemented in the Global Service Now (GSN) toolset provided by ITs (ITIL 2019). The change management process implemented in GSN used to make sure that the all individuals involved in the change management process follow the same rules and apply the same criteria when they evaluate changes and when they maintain the change records in the GSN tool (GSN 2021).

By using a centralized tool like GSN, all individuals involved in the change management process can access and update the same records, which helps to maintain accurate and up-to-date information about changes. The use of a centralized tool like GSN and a consistent set of rules and criteria for evaluating changes can help to ensure that changes managed in a consistent and transparent manner, which can help to reduce the risk of incidents resulting from poorly managed changes.

4 Practical Part

In this chapter, the author describes the general research strategy, research procedure, data collection approach, and expected limitations of the research work.

4.1 Case Description

The research conducted with a major company, (in order to keep confidentiality the company will be call Company X). Company X has customer oriented global company, has more than 1000 employee, and located on the Europe. In this regard, the company has proceed different type of IT change process to improve the service to satisfy the customer needs that aims to processes planed change with minimum risk across the company by using IT service management tool service now (SN). This company use comprehensive method of risk assessment that allows the participation of change requester, service owners, approver implementing and change closure by using the plat form automation processes using one common tool. Implementing a change process with minimum risk for the company is to ensure that changes are doing in a controlled and consistent manner, while minimizing the potential negative impact on the company's operations.

Implementing an IT change process with minimum risk can be a complex and challenging task, particularly for organizations with large and complex IT infrastructures. One of the primary reasons why implementing an IT change process with known risk can be difficult is that it requires significant planning and coordination across multiple departments and stakeholders. IT changes can affect multiple systems, users, and business processes, and therefore it is essential to involve all relevant parties in the planning and execution of the change process.

This company use Global Service Now Change Management tools to improve the quality of changes and minimizes the threat of change-induced incidents by ensuring that top standard processes used to handle the changes made to the IT system. Global Service Now's reach and flexibility have contributed to its popularity and success, with many-selected company using the platform to streamline and automate their IT operations, improve efficiency and productivity, and enhance the customer experience. It helps to control IT change management capabilities in selected global companies manage their IT infrastructure changes in a controlled and reliable manner, with minimal disruption to business operations. It wants to make successful changes on the first try. It assesses the impact and benefits of changes at a high-level and communicates the change plans and schedules to all the stakeholders and affected users involved in a timely manner.

IT change management is an ongoing process that requires continuous improvement and adaptation to meet changing business needs and technology trends. Organizations must be willing to invest in the development of their change management processes and tools

helps to implement IT with minimum risk, and to continually monitor and evaluate the effectiveness of these processes in order to ensure ongoing success.

4.2 Problem Statement

It identifies an issue or challenge that needs to be addressed this paper. Currently many IT companies want solutions that are Implement IT change with known risk by participating all party included in the change. Implementing IT change with known risk requires a careful approach to ensure that the change is implement in a way that minimizes the risk and reduces the potential impact on the business. Companies may implement IT change with known risk for a variety of reasons like Business needs, Technology upgrades, Security updates, Efficiency improvements and System integrations. If an IT change implementation fails, it can have significant negative impacts on a company, including Financial losses, Damage to reputation, Loss of customers or market share, Legal and regulatory issues and Reduced competitiveness. To mitigate the risk of IT change implementation failure, it is essential to have a well-planned and well-executed implementation strategy. This should include thorough testing, stakeholder communication, risk management, and contingency planning. This paper focuses mainly focused the efficiency of risk minimization and How Global Service Now, a cloud-based ITSM technology, can reduce the IT change risk IT during change implementation and increase the success and efficiency of the change process.

4.3 Purpose Statement

In this study, the Company X's way of IT change management risk minimization efficiency from implemented change investigated from IT service management tools GSN aspects. The process aspect covers the analysis of the total process of Whole process of the risk assessment from the beginning to end. IT Change management minimizes the risk of adverse service availability impacts when changes are made to the production environment. The Best Practice Change Risk Calculator (which is by default activated in the GSN automated system) and Change Management Risk Assessment are two ways for calculating the risk of a change(Utah 2023). A risk class calculated using the Change Risk Calculator's predefined properties and conditions. The end user's information used in the assessment of the risk value for change management.

Technical person involves various groups and stakeholders in the approval process based on the scope of the change, impact on Services and technology used. In addition, Technical teams review the change, attached documentation, and perform the risk analysis and Impact assessment based on valid ITS Standards, their knowledge and the high-level information provided by Requestor in the IT changes. Therefore, the intention is only to evaluate the efficiency of risk minimization IT change process all changes performed during specific time interval by using IT service management tool GSN. Furthermore, a critical

focus should be apply to the evaluation of the important steps during the implementation of IT change processes to minimize risk.

Research Questions

1. How to minimize the risk during IT Change Implementation by using service management tool Global Service Now and check the efficiency of risk minimization from Implemented IT changes?

2. What are the main components in GSN automated mechanism of cloud-based ITSM technology helps efficiently to reduce IT risk?

3. How Change Collision resolution and reveal service disruption in GSN?

4.4 Research Strategy

The overall approach for conducting this case study aimed at assessing the existing risk reduction of IT change management using IT service management tool(GSN) and recorded data over a Three-month period(from April-July 2022) to assess the effectiveness and efficiency of risk reduction in IT change management. With this in mind, a qualitative research approach that provides an in-depth understanding of risk mitigation with GSN's IT service management tools. This research based on a case-by-case approach, focusing on one organization. A case study approach, widely accepted as a qualitative approach, demonstrates the efficiency of risk mitigation using GSN IT service management tool, how to reduce risk when implementing IT changes to gain a broader understanding of the tool.

4.5 Research Procedure

Currently the selected company in this research paper process every It change management process by using Global Service Now. It is a popular platform for IT service management and can help organizations in their change management risk mitigation efforts in several ways. The overall process of IT change includes change Initiation, Planning, Approval, Implementation, Testing, Review and Evaluation and Closure of the change. The company has proceed different type of change include minor, significant and major to improve the service using the plat form automation processes using one common tool GSN. The company used comprehensive method of risk assessment that allows the participation of change requester, service owners, approver implementing and change closure. The company proceed more than 350 IT changes per month with major four category Hardware, Release, Infrastructure and Software changes.

4.6 Data Collection

The data collected from the change request data recorded for using IT service management tools GSN. The quantitative data gathered from company open source database.

The sources of qualitative data used to determine the efficiency of risk mitigation process using ITIL benchmarking tool. The reasoning behind this assessment was that the evaluate risk minimization in the IT change management process in a selected company based on using IT service management tools GSN, and to evaluate the efficiency of the risk management practices. Moreover, the strengths and weaknesses of the process could be identify and the using IT service management tools GSN progress could be evaluate. Also, check the efficiency based on feature in GSN using the types of changes, the implemented changes with outage types, the risk levels associated with each change, and the results of each change are collected reporting and analytics tools. To analyse the impacts of using GSN in the selected company and to formulate recommendations and conclusions about IT service management GSN.

4.6.1 Data Analysis framework

Statistical Package for the Social Sciences (version 28.0. IBM SPSS Statistics) software used to analyse the qualitative data documents in order to produce a more effective analysis. SPSS is a program that scholars across disciplines use quantitatively analyse complicated data. Frequency distribution analyses is perform to get meaningful quantitative results. Qualitative and quantitative data that complement each other blended while determining the efficiency of risk mitigation process. The most important statistical results was shown in the tables in specific component of risk mitigation, due to the huge amount of data it was not possible to go too much into details while presenting the data.

4.6.2 IT Change process framework work

The overall IT change management process in the selected company is to making sure changes to IT systems and services made in a controlled and coordinated manner to minimize risk and disruption. The IT change management process typically starts by creating change request. It is can be raised by the person or team that wants to make the change. The change request should be risk and impact assessed to determine the risk and impact on the system and the business. Risk and impact team professional makes it by using IT service management tools GSN, out-of-the-box machine learning capabilities to improve risk-assessment effectiveness. This includes identifying potential risks and benefits, as well as assessing the impact on other systems and processes.

A change advisory board (CAB), which approves or rejects(denied) the change, based on the assessment reviews the change request as shown in fig 6 below.

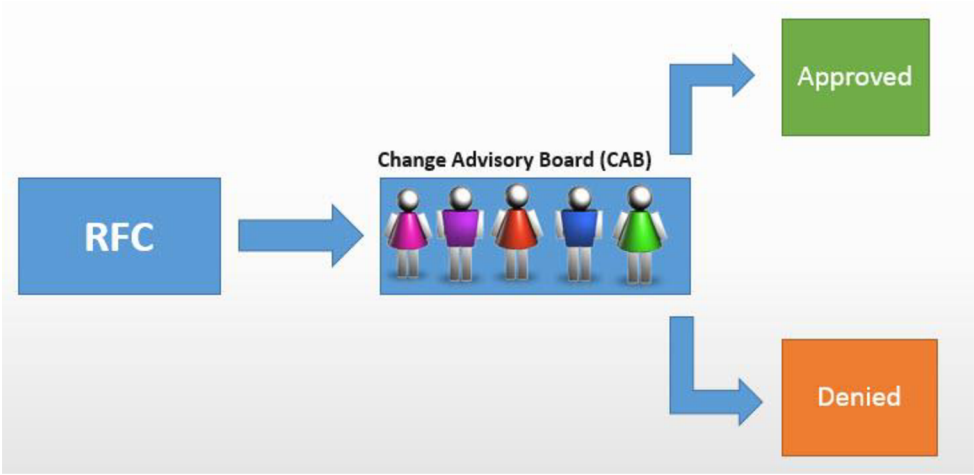

Figure 3 Change advisory board(Shaw 2019)

All changes require testing, back out plane or documentation before approving the change. After affected service owners, Implementers and change management specialist approve the change the implementation starts in the production environment according to an agreed-upon plan. This may include scheduling the change during off-hours or deploying the change in stages to minimize disruption. After the change has been in place for a certain period, a post-implementation review (PIR) conducted to evaluate the effectiveness of the change and identify any areas for improvement in the change management process. The final step is change closure of the change request. It is recording the change management system for future reference. It helps the selected company to track the progress of changes and maintain a record of all changes made to IT systems and services. This whole IT change process for selected company every changes relies on IT to operate effectively.

Process Flow: IT Change Stage

- Change Initiation:- it includes Creation of change and Quality check by change technical person
- Risk & Impact Analysis :- it includes Risk analysis & impact assessment
- Test Change:- it includes Development & test the change
- Approval for Implementation:- it includes Approve changes for implementation
- Implement Change:- it includes Communication and Implementation tasks/rollback
- Review and Close Change:- it includes Post implementation review and Change closure

Figure 4whole IT change management process(Blog 2023)

4.7 Risk mitigation framework work

Person, team or department first should identify the change first. Every change request started first by categorize the change type and followed by prioritizing the change. Change prioritization is the process of identifying and prioritizing changes based on their relative importance and urgency. It helps organizations to allocate their limited resources effectively and manage changes more efficiently. Risk categorization helps IT professionals prioritize and focus their efforts on changes that are high risk, while ensuring that low-risk changes receive an appropriate level of scrutiny. The responsible person before assign Change request the Release to Production should set. It is the process of deploying a change or a new version of a product or service to the production environment. A change plan the work start and end should be scheduled for implement a change request, including the release to production process.

Test a change starting by Identify the areas of the system or application that will be impact by the change. Create a test environment that replicates the production environment where the change will be deploy. This environment should include all the necessary hardware, software, and network configurations. Test a change can be functional testing, performance testing and security testing. The test results determine if the proposed change has met the testing criteria. If the test result is no and the change should be test again and it should be fulfil the requirement.

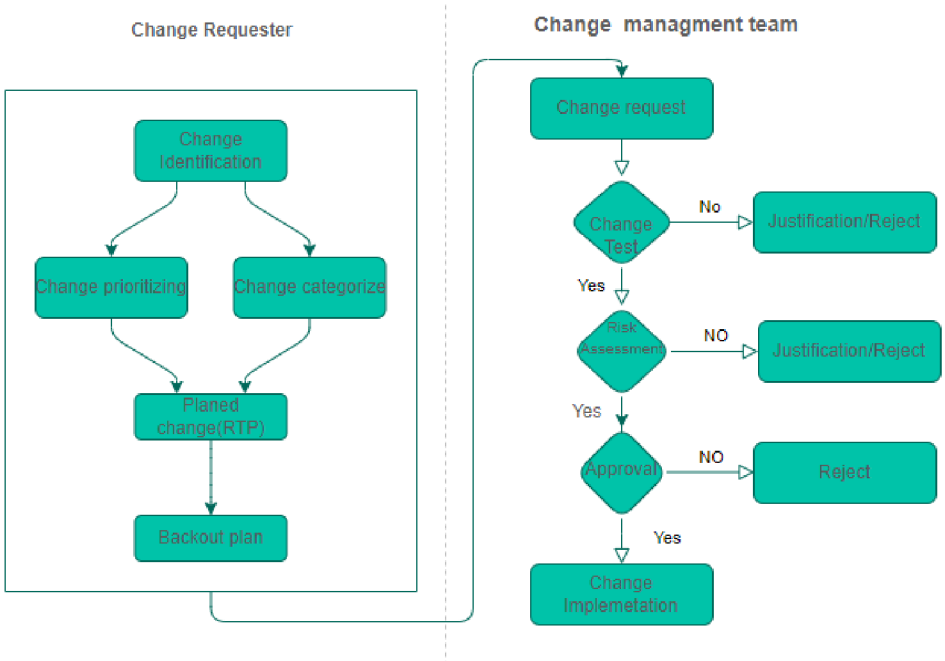

Figure 5 Risk minimization process model and design (author)

Risk classification is the process of categorizing risks based on their potential impact and likelihood of occurrence. There are several different approaches to risk classification, but one common method is to use a risk matrix. Risks typically classified into Low risk, Medium risk and High risk. It used appropriate risk mitigation strategies can be implement to reduce the likelihood and potential impact of the risks.

The classification of an outage can also change based on the severity of the impact. Outage, failure, and performance degradation all related to issues with the availability or quality of a system or service, but they represent different levels of severity. A back out plan is a plan of action that developed in advance to help mitigate risks and minimize the impact of changes or upgrades to a system or application. It outlines a systematic process to reverse the changes made during an implementation, should the need arise.

4.8 Risk Analysis and Evaluation of the company

It is the principal task is to evaluate a risk probability and Impact (consequences) and thus establish risk class (significance). Probability indicates likelihood the event may Impact IT Services. Impact indicates the (negative) result or risk effect on IT Services.

Analysis and evaluation phase includes following activities:

- ❑ Performance of the initial risk assessment
- ❑ Determination of impact (Impact is a damage or negative consequence (outcome) to IT Services that could be caused by an event (incident).
- ❑ Determination of probability (Probability is a likelihood of an event (incident) in which a threat is negatively affecting IT Services).

- ❑ Determination of risk classes(Evaluated risk is categorized into one of the risk classes defined)
- ❑ Validation of risk evaluation by skilled risk manager
- ❑ Documentation of risk assessment results

To limit the effort and costs the initial risk assessment used to determine if full risk analysis and evaluation is necessary for assessed service, IT asset and process. Initial risk assessment used for triggers information security concept and information security vulnerability, compliance assessment and governance.

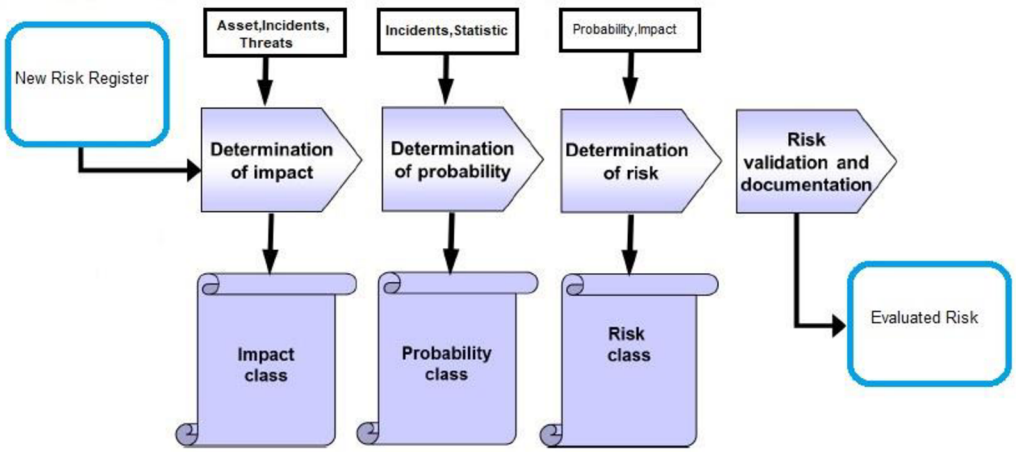

Figure 6risk analysis and evaluation flow diagram (author)

During the analysis and evaluation phase the following parameters must evaluated and defined for all identified information risks.

1) Impact – consequence (outcome) of an event affecting objectives
2) Probability – likelihood of an event happening

Risk – effect of the impact on objectives considering the risk probability (Risk = Impact x Probability)based on(ITIL 2019).

4.8.1 Determination of Impact

Impact is a damage or negative consequence in IT Services and company that could cause by an event (incident).

During evaluating Impact class following consequences must be consider

1) The financial impact included penalties and legal liabilities resulting from the breach of legal, regulatory, tax, or contractual obligations, additional costs, and revenue loss.

2) Operational Impact including loss of management control, competitiveness, employee productivity, employee satisfaction and engagement, imposition of legal or regulatory sanctions.

3) Customer impact including reputational impact, delayed delivery processes, loss of customers or investor' confidence, business partner satisfaction, and service quality degradation.

The Impact Class classified as Low (1), Medium (2), High (3) and Very high (4) based on Financial Impact, Operational Impact and Customer Impact. The confidentiality, integrity, and availability of information assets to be consider when assessing the inherent risk. If the risk affects many records or special categories of personal data then the impact can be higher.

The personal data privacy aspects to be consider when assessing the risk Impact using the following guideline:

1. **Low (1) Risk Impact: -** It is the kind of risk where individuals will either not impacted or may experience a few inconveniences but will easily get over them.
2. **Medium (2) Risk Impact: -** This is the kind of risk where individuals might have major annoyances, yet they can get by despite a few challenges.
3. **High (3) Risk Impact: -** That is the kind of risk where individuals could experience serious repercussions. Despite having significant obstacles to overcome.
4. **Very high (4) Risk Impact**: - Individuals can experience serious, or perhaps irreversible, effects because of this risk category, which they may not be able to overcome.

- ❑ The final stage or output of Risk Analysis and Evaluation is to Impact class assigned to a risk class.

4.8.2 Determination of Probability

Probability is a likelihood of an event in which a threat is negatively affecting IT Services and the company. In case the probability is 100%, the risk becomes the issue. To determination of Probability, the mandatory components are a list of services, IT assets, processes and a list of threats and vulnerabilities, past incidents.

The activity doing during determination of Probability is Assessment of probability should take into the account how often the threats occur and how easily the vulnerabilities may exploited.

The following factors need to be taking into account during determination of Probability:

- ❑ Expertise and statistical details for threat likelihood
- ❑ A purposeful threat source's intent, capability, and resources, as well as the perceived appeal of any potential attackers
- ❑ Geographical variables, potential human mistake triggers, and equipment failures are potential sources of unintentional hazard

- Existing controls and Vulnerabilities

Probability class	Information Security Event Occurrence	Likelihood of Project Risk
Less probabile(1)	Event occurs every 10 years or less	0% - 25%
Likely probabile (2)	Event occurs once every ten years or up to once per year	26% - 50%
Very Likely probabile (3)	Event occurs once per year or up to once per month	51% - 75%
Frequent probabile (4)	Event occurs more often than once per month	76% - 100%

Table 4 Probability classes are classification criteria(ITIL 2019)

- The final stage or output of Determination of Probability is to Probability class assigned to a risk class.

4.9 How the company determination of Risk Classes

In the selected company, evaluating Risk class is an important step in the IT change management process. It involves assigning a level of risk to a proposed change based on the potential impact and chance of the change causing problems in the IT system, application, or service.

There are several ways to categorize risks class in IT change management, but a common approach but the selected company is to use a risk matrix that combines impact and likelihood to determine the level of risk(ITIL 2019). The impact of a change assessed as low, medium, or high, and the likelihood of the change causing problems assessed as low, medium, or high. The resulting risk class typically categorized as low, medium, or high.

Impact class and probability class of the risk calculate evaluated risk categorized into one of the risk class defined. Risk classes are derived by multiplying the impact class (1-4) with the probability class (1-4).Based on the calculation the following risk classes are defined: critical risk (16), high risk (9-12), elevated risk (4-8), medium risk (2-3), and low risk (1).

Risk classes				
Impact class	Probability class			
	Less probabile(1)	Likely probabile (2)	Very Likely probabile (3)	Frequent probabile (4)
Very high (4)	Elevated risk (4)	Elevated risk (8)	High risk (12)	Critical risk (16)
High (3)	Medium risk (3)	Elevated risk (6)	High risk (9)	High risk (12)
Medium (2)	Medium risk (2)	Elevated risk (4)	Elevated risk (6)	Elevated risk (8)
Low (1)	Low risk (1)	Medium risk (2)	Medium risk (3)	Elevated risk (4)

Table 5 Determination of Risk Classes by risk matrix(ITIL 2019)

One ITIL's recommendation is to use a risk categorization matrix like the one represented in the Table 5. It is possible to observe that risks classified into four categories in a crescent scale, where category 1 means highest risk and category 4 the lowest. Another important fact is that greater importance given to the impact, since the category 2 is before the category 3 on the scale.

By categorizing risks in this way, IT professionals can ensure that they are focusing their efforts on the most critical changes, while still giving appropriate attention to lower risk changes. This helps to ensure that the IT change management process is efficient and effective, and that changes implemented with a minimum of risk to the IT system, application, or service.

4.10 Evaluating risk class by GSN

GSN to evaluate IT change risk, you can take a structured and systematic approach to risk management, which can help to minimize the impact of IT incidents and ensure the continuity of IT services. The risk of a change in GSN can be determined using one of two ways(GSN 2021).

1. The Best Practice - Change Risk Calculator is by default turned on in the basic system. The Change Risk Calculator determines a risk estimate using predefined properties and conditions.
2. Change Management - Risk Assessment is optional and Change Management Risk Assessment uses information provided by the end user to assess a risk value.

The two methods can used individually or together, depending on your requirements. If the methods used together, the highest risk value from both methods always selected.

4.10.1 Risk class

The risk class tab shows the result of potential risks from IT changes, and by controlling the result, it is possible to minimize the risk of disruption to service operations and customers. The risk class assigned to each change based on its potential impact and likelihood of occurrence. By evaluating the risk class, it is possible to determine the appropriate level of scrutiny, approval, testing, and communication required for each change. There are six risk levels selected in the field “Risk” in the “Risk Assessment section of the “Change Request” form in GSN:

1. None
2. Very low
3. Low
4. Moderate
5. High
6. Very high

The risks class ranked in order of priority based on the level of impact. Prioritizing risks in IT change management is critical to ensure that limited resources are focus on the most significant risks. Risk class results in GSN shows various reports, dashboards, and visualizations that provide a comprehensive view of the identified risks and their severity.

4.11 Tabs in GSN helps to mitigate the risk in IT change process

Using Global Service Now's have advantage in reporting and analytics tools to collect data on the number of changes, the types of changes, Implemented change with Outage Type, the risk levels associated with each change, and the outcomes of each change. There are some features in GSN that helps to control the risk during change Implementations.

Some Tabs in GSN helps to minimum risk of IT change management process also

- Prioritizing the change
- Outage Type
- Change tested result
- Back out plan result

4.11.1 Prioritizing the Change tab

The Priority tab in Global Service Now (GSN) provides information about the priority level assigned to a particular change request. Priority levels used to prioritize change requests based on their impact and urgency, and to ensure that the most critical issues

addressed first. The priority level is typically assign based on the impact and urgency of the change or incident. Change priority reflects the urgency of a particular change. Prioritizing the Change helps to reduce the risk during consideration decisions about implementation order in case of change conflict.

1. Low / Medium / High priority

The change follows the normal change management process and the normal deadlines and lead-times apply.

- Low = not pressing, but would be advantageous, can be postponed if necessary
- Medium = should be implemented to gain benefit
- High = important for organization and must be implemented soon

2. Urgent priority

The change follows the urgent change process with shortened deadlines and lead-times. Urgent changes can be

- Planned changes which need to be implemented in reduced time due to inadequate planning
- Planned changes, which need to be implement in reduced time in order to meet the need of a last moment customer/business driven request.

If a high-priority change identified during the change management process, it may require re-prioritization of other changes that scheduled to take place. This ensures that the most critical changes are implemented first, minimizing disruption and potential risks. If a change request escalated to a higher priority level, it may require additional resources to be assign to ensure that it completed in a timely manner. Higher-priority changes are typically subject to greater scrutiny and review, which may involve additional approvals, testing, or documentation requirements. Changes with higher priority are typically implementing more quickly to minimize the impact on the business. Conversely, changes with lower priority may be delay to prioritize other changes or may be accelerate if they become more critical.

4.11.2 Risk Prioritization tab

Risk priority is a critical component of IT change management that helps organizations prioritize their efforts and allocate resources appropriately based on the level of risk associated with a proposed change. By assigning a priority level to each risk, organizations can focus their attention on the highest priority risks and take steps to mitigate them before implementing the change.

There are different ways to prioritize risks in IT change management, but a common approach is to use a risk matrix that combines the probability and impact of a risk to determine the risk priority level. For example, the probability of a risk may assessed as low,

medium, or high, and the impact of the risk may be assessed as low, medium, or high. The resulting risk priority level categorized as follows:

1. High priority: Risks with a high likelihood of occurrence and a significant impact on the IT system, application, or service.
2. Medium priority: Risks with a moderate likelihood of occurrence and a moderate impact on the IT system, application, or service.
3. Low priority: Risks with a low likelihood of occurrence and a minimal impact on the IT system, application, or service.

It is important to note that risk priority should not be the sole criterion for deciding whether to implement a change. Other factors, such as the business needs and the technical feasibility of the change, should also take into consideration when making decisions about change implementation.

4.11.3 Back out plan result tab

The back out Plan tab in Global Service Now (GSN) provides information about the back out plan associated with a particular IT change request. A back out plan is a plan to undo or reverse the changes made by an IT change request in case something goes wrong during the implementation process or if the change does not produce the expected results. A back out plan is a critical part of IT change management that outlines the steps to taken to reverse the changes made in a change request, and restore the system to its original state, in the event of an unexpected issue or failure during the change implementation.

The main advantages of back out plan in the IT change management process are minimizes the risk of downtime and service disruption, if the change fail quickly revert the system to its previous state if something goes wrong during the change implementation. Also provides a safety net that is implement changes with greater confidence, knowing that they have a plan in place to reverse the changes if something goes wrong. A back out plan helps to minimize the impact of such failures by providing a clear and concise plan for quickly reverting the system to its previous state. Finally, back out plan improves communication and collaboration.

4.11.4 Test tab

The Test tab in Global Service Now (GSN) provides information about the testing activities associated with a particular IT change request. Testing is an important aspect of the change management process, as it ensures that the IT change request has been thoroughly tested and validated before it implemented in the production environment. In IT change management, change testing is the process of evaluating changes to an IT system, application or service to ensure that they meet the expected results and do not cause any adverse effects. Change testing is a critical component of the overall IT change management process because

it allows IT professionals to identify and mitigate any risks associated with a change before implemented into production.

When change not tested during the IT change management process, it can lead to various negative consequences like System downtime, Data loss or corruption, Security breaches and Inefficiencies. Changes that are not tested can also introduce security vulnerabilities or weaknesses, which can expose by attackers to gain unauthorized access to systems, steal sensitive data, or cause damage to IT infrastructure. Also, cause inefficiencies in IT operations, such as slow response times, poor system performance, or reduced reliability, which can negatively Impacts business processes and operations. By testing changes before they are deployed to production environments, IT teams can identify and fix issues early on, which can help to minimize the risk of downtime, data loss, security breaches, and other problems. This can also help to ensure that end users have a positive experience with the IT systems they use, which can improve productivity and satisfaction.

4.12 Service Outage Type tab

This tab shows the most affected service by specific change and shows outages potential risk that can occur during implementing changes to a system, application, or service. The potential outage can be outage, failover, and performance degradation. By considering the potential outage types result, IT teams should have develop appropriate strategies and contingency plans to mitigate the risks and minimize the impact of downtime or service disruption during implementing changes. This includes implementing appropriate backup and recovery solutions, developing failover plans, monitoring system performance and availability, conducting regular testing and validation, and communicating effectively with stakeholders and users to manage expectations and minimize disruptions. It is also important to prioritize risks based on their potential impact and likelihood, and to allocate resources and investments accordingly to mitigate those risks.

4.13 Risk Treatment

If once already known and accepted risk present during implementation of change with potential impact like failover, outage and performance degradation on prioritization of evaluated risks and deciding on appropriate treatment. Response can vary from tolerating the risk as-is, treating to lessen its probability or impact (or both), transferring to a third party, or avoiding the risk entirely. When the final response selected and approved, implementation of suggested activities will start.

The risk Treatment during change implementation includes following activities:

- Identify risk treatment options, if available
- Decision on risk treatment options

- ❑ Validation of risk treatment options on compliance with relevant information security standards
- ❑ Specification of residual risk (after application of proposed treatments
- ❑ Review and acceptance of residual risk and Escalations, if necessary and

Risk prioritized according to risk evaluation criteria (assigned risk class) and during the treatment phase so called risk treatment class must evaluated and defined for all identified information security risks.

The type of risk treatment class, option in the selected company is,

Risk treatment class	Description
Risk modification (reduction)	The probability and/or the impact of a risk should be reduced by implementation of a mitigation plan (introducing, removing, or altering controls) so the residual risk can be reassessed as being acceptable.
Risk retention (acceptance)	The decision on retaining the risk without further action should be taken depending on risk evaluation (i.e., the impact of a threat does not justify the cost to reduce or eliminate it).
Risk avoidance	The activity or condition that gives rise to the particular risk should be avoided.
Risk sharing (transfer)	The risk should be transferred to another party that can most effectively manage the particular risk depending on risk evaluation, thus reducing the residual risk to an acceptable level

Table 6 Risk treatment classes options(ITIL 2019)

4.14 Documentation of Risk Treatment

Detail at which a risk treatment documented and followed up depends on the risk treatment class and on the criticality of the risk. A detailed and formally documented mitigation and contingency plan must maintained for all critical risks and should be maintained for all high risks, especially if the proximity is lower than 30 days. For elevated, medium, and low risks, a mitigation plan documented within the risk repository is sufficient.

Risks affect multiple business must presented, reviewed and accepted by respective stakeholders. Finally the Risk treatment (mitigation) plan and residual risk accepted by relevant management.

4.14.1 Risk Monitoring and Review

This phase assures that risks reviewed regularly or when needed due to changed situation. In addition, it assures that residual risks communicated to stakeholders. Evaluating by using Risk with treatment plan and evaluated residual risk

Monitoring and review phase includes following activities:

1. Performance of risk re-evaluation (review) on a regular basis or in cases of changed situation
2. Communication (reporting) of residual risks to stakeholders

4.14.2 Review

Risks associated with IT change management must regularly reviewed to ensure that the risk management approach is effective and up-to-date(ITIL 2019). Regular risk reviews help the company identify new risks or changes to existing risks, as well as evaluate the effectiveness of existing risk management controls. Regular risk reviews should involve key stakeholders from the IT organization, as well as business stakeholders who may impacted by IT changes. The purpose of the risk review is to evaluate the effectiveness of existing risk management controls, identify any new or emerging risks, and ensure that the risk management approach aligned with the organization's overall risk management strategy.

4.15 Risk Closure

Risk closure is the final stage of the risk management process, in which risks that have identified and assessed formally closed out. Risk closure involves documenting the risk, its impact, the risk management approach taken, and any risk management controls that put in place(Prosci 2018). The risk closure process may involve a review of the effectiveness of the risk management approach, including an evaluation of whether the risk effectively mitigated or transferred, or whether it was simply accepted. The risk closure process may also involve a review of any residual risks that may remain after risk management controls have put in place, and the development of plans to monitor and manage those residual risks.

The purpose of risk closure is to provide a formal process for documenting and closing out risks, which helps to ensure that the organization has a complete and accurate record of its risk management activities. By formally closing out risks, organizations can demonstrate that they have taken appropriate steps to manage risks and that they are committed to a culture of continuous risk management improvement. In the context of IT change management, risk closure may involve the closure of risks associated with specific

changes, as well as the closure of risks associated with the change management process itself. By closing out risks associated with IT change management, organizations can help to ensure that changes implemented successfully and with minimal disruption to IT systems and the business.

Risks can closed in the following cases:

- Risk treatment actions were completed which resulted in the avoidance of the risk or full removal.
- Risk is not relevant due to user or system error, is duplicated or adequately covered by other risk
- Risk is unclear or ambiguous and the risk author is unreachable
- Security exception is not needed due to a change in the information security standard or other relevant control requirements document
- Security exception is not needed as the root cause of incompliance was fixed

4.16 Key Success Factors for change Implementation with minimum risk

4.16.1 Communication

Based on primary data found recorded data from GSN the most effective way of information Sharing. Communication is critical during IT change management process because it ensures that stakeholders informed, engaged, and supportive of the change, which increases the chances of successful implementation. The efficiency of an IT change management process can be evaluated successful IT change implementation process with minimum risk. Planned IT change involves by defining the scope of the change, identifying key stakeholders, and establishing a timeline and budget for the implementation.

In addition, effective communication is critical to ensuring that stakeholders understand the need for the change, informed about the implementation process, and are prepared for any disruptions that may occur. Effective communication is a critical component of any successful IT change management process of selected company. It places a strong emphasis on communication to ensure that its employees, customers, and other stakeholders are well informed and engaged. Global Service Now provides various communication channels for customers and users to get support and feedback and effective. Communication is likely a critical component of their overall business strategy to ensure the success of their platform and the satisfaction of their customers. Successful IT change implementation through IT service management tool Global service now process requires careful planning, effective communication, thorough testing, close monitoring, and continuous improvement.

Communication approach are:

Communication is even more important in Global Service Now during IT change management process because it involves teams and stakeholders across different geographical locations and time zones. Here are some ways communication can be effective in this context(GSN 2021):

1. **Use of Digital Tools:** In a global service environment, it is important to leverage digital tools such as video conferencing, instant messaging, and email to facilitate communication between teams and stakeholders across different time zones. These tools can help to ensure that everyone is on the same page and reduce misunderstandings that can arise due to differences in language and culture.
2. **Multilingual Communication:** If teams and stakeholders speak different languages, it is essential to ensure that communication delivered in a language that everyone understands. This can achieved by providing translations for important documents, using multilingual speakers during meetings, and providing language training where necessary.
3. **Clear and Consistent Communication:** Clear and consistent communication is crucial to ensure that everyone understands the changes that are taking place and what is expected of them. This can achieved by providing regular updates, ensuring that key messages are consistent across all communication channels, and using simple language that is easy to understand.
4. **Managing Time Zones:** When teams spread across different time zones, it is important to ensure that communication scheduled in a way that is convenient for all parties. This may involve rotating meeting times or ensuring that all critical information communicated via email or recorded messages that can accessed at any time.
5. **Stakeholder Engagement:** It is important to engage with stakeholders at all stages of the IT change management process. This can achieved by providing regular updates on the progress of the change, soliciting feedback, and addressing concerns in a timely manner.

Communication in GSN during IT change management process requires the use of digital tools, multilingual communication, clear and consistent messaging, managing time zones, and stakeholder engagement to ensure that everyone is informed, engaged, and supportive of the change, regardless of their geographical location.

5 Results and Discussion

This chapter presents the results of the empirical data collected through this single case study. The findings from the conducted recorded data were analysed as objectively as possible and presented in three different parts. The first part presents the efficiency of risk minimization by GSN using Key performance indicators, the second part reveals are the main feature in GSN automated mechanism of cloud-based ITSM technology used to reduce IT risk assessment. The third part highlights result of Change Collision resolution and reveal service disruption in GSN and final describe the summary of Key Findings and limitation of the tools.

The primary data sample were the data recorded for Three-month period (from April-July 2022). The company has proceed different type of change include minor, significant and major change. The analysed through frequency distribution from 1128 changes. Overall, 172 minor change, 956 significant change and no major change. From the three type of change in this minor change (with no risk) excluded from analysed. The company IT change management process and categorized the changes, which are Infrastructure Change (15.5%), Software changes (25.0%), Hardware changes (19%) and Release change (17.9%). Test change ensure that implemented successfully and do not cause any unexpected disruptions or negative impacts on the organization's operations.

5.1 Efficiency of risk minimization

The IT change success rate is a measure of the percentage of IT changes that are successfully implement without causing any major disruptions or negative impacts on the IT systems or business processes. It is an important metric for evaluating the effectiveness of an organization's change management process and assessing the overall reliability and stability of its IT systems and services.

A high IT change success rate indicates that the organization has a well-defined change management process in place that is effective in minimizing the risk of disruption and ensuring that changes are implement successfully. This can help to improve the reliability and availability of IT systems and services, enhance the user experience, and support the achievement of business goals and objectives. Evaluating the efficiency of risk minimization in IT change process by Global Service Now evaluated by Key performance indicators.

5.1.1 Key performance indicators (KPIs)

Key performance indicators (KPIs) used to evaluate the efficiency of risk minimization in the IT change process(Andrade, Albuquerque, and Teófilo 2016). The number of high-risk changes that have been successfully implement refers to the total number of changes that were deemed to carry a high level of risk but were successfully implemented without causing any significant incidents or problems. This is an important

metric for evaluating the effectiveness of the change management process and assessing company ability to handle high-risk changes. This include metrics such as the number of high-risk changes that have been successfully implement, the percentage of changes that have implemented without incident, and the time it takes to resolve incidents that do occur.

The percentage of changes that have been implemented without incident is a measure of how often changes are implemented successfully without causing any negative impact on the system or process. This metric can be calculated by dividing the total number of changes that were implemented without incident by the total number of changes made during a given time period. The percentage of changes implemented without incident calculated as the total number of successful changes divided by the total number of changes implemented, multiplied by 100.

Overall change				
Risk class	Change Requested	Requested percentage	Implemented change	Implemented percentage
High	155	16.2%	152	16.1%
Low	522	54.6%	517	54.8%
Medium	241	25.2%	236	25.0%
None	10	1%	10	1.1%
Very high	1	0.1%	1	0.1%
Very low	27	2.8%	27	2.9%
Total	956	100%	943	100%

Table 6 Key performance indicators (author)

From the result in the table, the total number of change requested high and very high-risk level is 155 and 1 respectively and change Implemented high and very high-risk level is 152 and 1 respectively. The cumulative percent of the change requested and implemented with high risk of the total change is 156 and 153 respectively.

Percentage of changes implemented without incident

$$= \left(\frac{Total\ number\ of\ successful\ changes}{Total\ number\ of\ changes\ implemented}\right) \text{ x } 100$$

$$=98.08\%$$

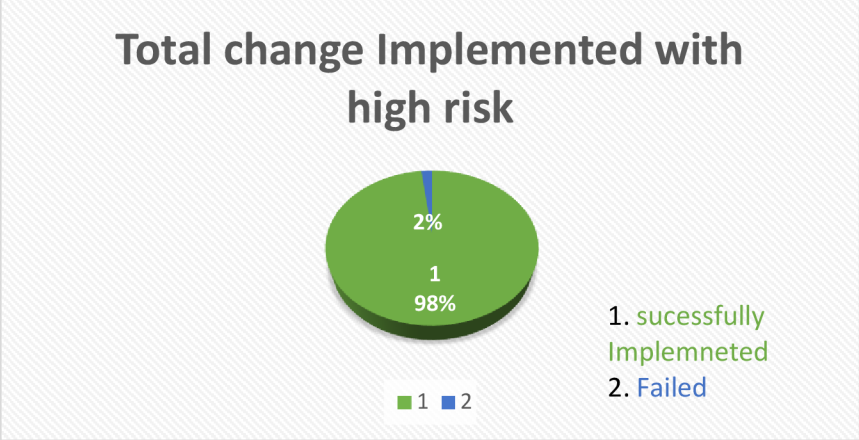

Figure 7 Recorded result from the three months in 2022(author)

From the result, 98.08% of high-risk changes implemented successfully without any incidents. A high percentage of changes implemented without incident indicates that the company has a well-established and effective change management process that is capable of identifying and mitigating risks associated with high-risk changes. However, low percentage of changes implemented without incident indicates that change management process may need improvement and that there may be gaps in the process that need to address. The Company identify trends and patterns in the success rate of high-risk changes and make data-driven decisions to improve their change management process. Reducing the number of incidents caused by high-risk changes, improve system availability and stability, and ultimately improve the overall quality of IT services provided by the organization.

Implementing changes without incident through IT change management process can help mitigate the financial risks associated with changes to an organization's IT systems and contribute to the overall financial health of the company. Effective IT risk minimization can have a positive impact on a company's income. By minimizing IT risks, a company can protect its data, systems, and operations from potential disruptions and losses that could affect its revenue and profitability.

5.1.2 Components result in GSN improves efficiency of risk mitigation

The effectiveness of implementing IT change management process with minimum risk in Global Service Now supported by features mainly including the change success rate with outage type, change tested result, and back-out plan result. Use Global Service Now's reporting and analytics tools to collect data on the number of changes, the types of changes, Implemented change with Outage Type, the risk levels associated with each change, and the outcomes of each change. By monitoring these metrics, evaluate the effectiveness of the IT change management process in Global Service Now and identify areas for improvement to minimize risk and maximize change success rate. The research question the main components in GSN automated mechanism of cloud-based ITSM technology used to reduce IT risk assessment addressed here.

5.1.2.1 Change success rate with Outage Type

The classification of outages caused by the change into different types based on their severity and impact on the business done. A planned outage period of downtime that known to users ahead of time, while an unplanned outage is a period of downtime that was not planned and cause significant trouble for a business. The parts of the change management process that need to been fixed was identified by looking at the different types of outages. The change success rate by outage type calculated using a tool like Global Service Now to generate reports and visualize the data. The data can be analysed to find patterns and trends in the types of changes that are more likely to cause outages or incidents and the types of changes that are more likely to implement successfully. In Table 7 described the change that implemented for period (three months) regarding to outage type and failed changes.

Implemented change with Outage Type		
Service outage type	Number of changes	Percentage
Not Implemented	13	1.4%
Failover	49	5.1%
None	603	63.1%
Outage	256	26.8%
Performance Degradation	35	3.7%
Total	956	100%

Table 7 Implemented change with Outage result (author)

The IT change success rate implemented with outage (Failover, Performance Degradation and Outage) typically calculated by dividing the total number of successfully implemented changes by the total number of changes attempted, expressed as a percentage. All change pass with risk and Impact analysis with satisfactory result and Accepted risk did implemented based on time took to implementing a change from the point of submission of the request for change to the point where the change fully implemented. Percentage of changes implemented with Outage type

$$= \frac{Total\ number\ of\ successful\ changes\ with\ outage}{Total\ number\ of\ changes\ implemented}) \times 100$$

=98.64% the overall implementation rate

From this result shows Global Service Now is tool for managing changes in a way that minimizes disruption and ensures maximum efficiency. During implementing changes

with known outages, the tools configured to ensure that the change been properly documented, communicated, and scheduled to minimize disruption to users. From total change of 956 significant change 1.4 % of the change not implemented. Based on the recorded data most of the change not implemented because of Rescheduling. It is common reason why changes may not be implement as originally planned. The other reason not implemented was Dependencies. Some Changes have dependencies on other changes, or activities, and if these dependencies delayed, the change may need to reschedule. The change implemented with failover is 5.1 %. It means a change process of automatically switching from a primary system or service to a secondary system or service in the event of a failure. Failover can help to minimize downtime and service disruption, but it can also introduce additional risks, such as data loss, inconsistencies, or configuration issues. Almost more than half 63.1% change implemented without potential impacted. In addition, the change implemented with outage was 26.8% and it implies an unplanned disruption or interruption to a system or service, which can result in downtime, service unavailability. Finally, the change implemented with performance degradation was 3.7% of the total change. It shows a situation in which a system or service experiences a decline in performance, such as slower response times, increased latency, or decreased throughput. It caused by a variety of factors, including increased user demand, changes to the system or application, or issues with network connectivity or infrastructure.

5.1.2.2 Change tested result in IT change management

Testing the change is a critical step in the change management process that ensures that the change has been implement successfully and that it will not negatively affect the IT environment or business operations. This metric measures the effectiveness of the testing process that conducted before the changes implemented. A high change tested result indicates that the changes are thoroughly tested before they are deployed, reducing the likelihood of any negative impact on the IT environment. Without proper testing, issues or defects can go unnoticed, leading to unplanned downtime, loss of productivity, or other negative consequences. Here are the result the recorded data change based on Change tested result but the change before recorded in GSN calculate the change tested result.

Test change		
Test result	Number of change	Percentage
No	117	12.2%
Yes	839	87.8%
Total	956	100%

Table 8 Change Tested result (author)

From the total implemented change based on the table, 87.8% of change processes have passed through testing process, while 12.2% of not tested. The majority of changes that have been implemented have passed through the testing process, which tracked and reported on by the change management module that is already included in the platform.

According to the report in GSN, changes that have previously passed testing do not require testing again if they are of the same type. However, all types of changes must pass through testing before implementation. The testing process varies based on the category of change. The expected outcomes and requirements of a change assured through the testing process in IT change management.

5.1.2.3 Back out plan result during Implementation

A back out plan is a critical component of IT change management. It is a contingency plan that outlines the steps to be taken if a change fails or causes any negative impact on the IT environment. By analysing the back-out plan result, it possible to improve the effectiveness of the contingency planning process. A back out plan is a critical part of IT change management that outlines the steps to taken to reverse the changes made in a change request, and restore the system to its original state, in the event of an unexpected issue or failure during the change implementation. It is a contingency plan that outlines the steps to take to reverse the changes made in a change request, and restore the system to its original state, in the event of an unexpected issue or failure during the change implementation. Here are the result the recorded data change based on Back out plan result during Implementation describe below.

Blackout planned		
Back out plane result	Number of change	Percentage
Yes	755	21.0%
No	201	79.0%
Total	956	100%

Table 9 Blackout planned result based on the data recorded (author)

Based on the result shown in the table 79% of the change has back out plane and is designed to minimize the impact of a failed change by quickly restoring the system to its previous state. It includes detailed steps on how to undo the changes, who is responsible for carrying out each step, and how long it should take to complete each step. The rest 21% of change have no back out plane. Some changes are consider low-risk and have minimal impact on the IT environment, where a back-out plan may not be strictly necessary.

Therefore overall success rate of IT change processes with minimum risk can vary widely depending on a variety of component result, including the size and complexity of the change, the level of risk associated with the change, the quality of planning and preparation, and the effectiveness of communication and collaboration among stakeholders. The overall success rate of recorded change data with minimum and managed risk is 98.6 % successfully implemented without major distribution. The rest 1.4% implemented with major distribution business service and stakeholders.

5.1.3 Change Collision resolution and reveal service disruption

The research question Change Collision resolution and reveal service disruption in GSN discussed here. Change collision is implementation of two or more changes, which are going to be, performed either based on the same Configuration Item (CI), Server or Service within the same time. In GSN Change Module, "check conflict" which contains multiple scripts that triggered on request by clicking on the "Check Conflicts" link under the related links section in the change request form or triggered automatically when a change updated and saved. If there is conflict, the system will display a message and Change Requestor/Change Approver can view this information easily. All change implemented had collision with other changes implemented during the same time but the GSN automatically aware the requester about the change collision.

Change Collision			
	Number of change	Percentage	Communication by email
With Collision	912	95.4%	100%
Without Collision	44	4.6%	100%
Total	956	100%	

Table 10 Change Collision result (author)

Based on the result 95.4% of the change implemented with Change Collision and only 4.6%implelemented without Change Collision. If there are conflicts then this information communicated to the Change Requestor via GSN by updating this info into the internal work notes when setting the change to risk assessment stage. This action would trigger an email to the Change Requestor and would serve as a reminder. In the email content instruction to the Change Requestors of the selected changes to view the collision information and discuss with the Service Owner and the colliding Change Requestor. The outcome of the discussion and decision made shared upfront to the change team or in the CAB meeting. If the collision was not addressed by the Change Requestor either prior to or during CAB meeting, it'll be recorded as a condition in the change and it must be clarified by the Change Requestor prior to the change is being approved.

To reduce the risk of change collisions in Service Now, it is important to establish a robust change management process that includes clear communication and collaboration between different teams involved in making changes. This includes identifying potential conflicts and coordinating changes to minimize the risk of collisions. Communication is a critical tool for preventing change collisions in Global Service Now. Effective communication allows different teams and departments involved in making changes to the Service Now instance to coordinate their efforts and avoid potential conflicts.

5.2 Discussion

The study found that using GSN for IT changes has helped the selected company improve its IT change management processes, reduce the risk of errors and disruptions, and enhance collaboration among stakeholders. The GSN platform provided a structured framework for managing changes, with features such as change requests, approvals, and documentation that facilitated collaboration among stakeholders. Additionally, the risk assessment and management capabilities of GSN helped identify and mitigate risks associated with IT change. This finding is consistent with previous research that has shown that using a structured approach to IT change management can improve organizational efficiency and reduce the risk of errors and disruptions.

One of the key factors contributing to the success of the GSN implementation was the involvement of key stakeholders from across the company. This research highlighted the importance of risk assessment and management throughout the IT change management process. The study found that effective risk management requires a proactive approach that involves identifying, assessing, and mitigating risks before they become major issues. This finding is consistent with best practices in IT change management, which emphasize the importance of risk assessment and management at every stage of the change process.

Another important finding was the importance of risk assessment and management throughout the IT change management process. The study highlights the need for a proactive approach to risk management, which involves identifying, assessing, and mitigating risks at every stage of the IT change process. By taking a proactive approach to risk management, companies can reduce the likelihood of errors and disruptions, and ensure that IT changes implemented smoothly and efficiently. This study identified the benefits of using a dedicated IT change management platform such as GSN, which provides a structured framework for managing changes and facilitating collaboration among stakeholders. The study found that the use of GSN helped the selected company to standardize its change management processes, resulting in improved consistency and reliability in the change management process.

However, this study also revealed some differences from other studies that have investigated IT change risk minimization. The implementation of the change management process need to adapt the process to the culture and maturity of the company, requiring dedication commitment and effort everyone involved, so that break resistance and paradigms related to this change with the use of the process(da Silva et al. 2016). In addition, the paper studies have highlighted the importance of organizational culture in reducing IT change risks, while the study found that the use of GSN as a tool could mitigate IT change risks regardless of the organizational culture. This suggests that the effectiveness of IT change management tools can vary depending on the specific context of their use. The comparison of the results with similar research or studies from other authors provides additional insights

into the factors that contribute to the success of IT change management tools and the importance of their proper use and support.

Finally, the study highlighted the need for ongoing evaluation and improvement of IT change management processes to ensure their continued effectiveness. The study found that regular review of IT change management processes and associated risks is essential to identify areas for improvement and to ensure that the processes remain effective in mitigating the risks associated with IT change.

Overall, the findings of this study have important implications for organizations looking to improve their IT change management processes and minimize risk. The study demonstrates the value of using a structured and collaborative approach to IT change management, and highlights the importance of ongoing risk assessment and management. The study also suggests the need for ongoing training and support for staff to ensure that IT change management initiatives are successful. Based on the result from recorded data analysis Global Service Now offers automated change management workflows that helped organizations to manage changes more efficiently and effectively with minimize risk. Global Service Now refers to the use of Service Now in a global context, where it used by organizations with a global presence to manage their IT and business processes across different locations and business units. This typically involves implementing Service Now across different regions and integrating it with other systems and applications used by the organization. This can help reduce the risk of delays or errors in the change management process.

5.3 Summary of Key Findings

5.3.1 Summary of Key Findings

Global Service Now is an IT service management platform that provides a range of tools and capabilities to help selected company and for manage IT change management processes. The platform used to support risk management efforts, its effectiveness in minimizing risk during IT change management processes ultimately depends on how it used by the company. Here are some advantage of using Global Service Now support risk minimization during IT change management process:

- Global Service Now provides capabilities for automating risk assessments for IT changes. This can help company to identify potential risks associated with changes and take appropriate measures to minimize those risks. It can analyse the impact of proposed changes to identify potential issues that may cause downtime or service disruption. This can help company proactively address these issues before they occur.
- Global Service Now provides capabilities to manage conflicts between changes. This includes identifying conflicting changes, determining the best course of action, and communicating with stakeholders about the impact of the conflict.

- Global Service Now provides capabilities for collaboration and communication among stakeholders involved in IT change management processes. This can help ensure that everyone is aware of changes and any associated risks, and can coordinate efforts to mitigate those risks.
- Downtime and service disruption are common risks associated with IT change management, as changes can cause unexpected issues that impact business operations. It provides capabilities to schedule changes during low-impact times, such as outside of business hours and provides workflows for managing approval processes for IT changes. Also provides capabilities to support reduced downtime and service disruption, its effectiveness in this area depend on how it implemented and used by the organization. Effective use of the platform requires a clear understanding of the organization's IT change management processes and a commitment to following best practices for minimizing downtime and service disruption.

The selected company have efficient high rate of successful IT change implementation with minimum risk. Because of successful implementation of IT changes with minimum risk the selected company got progress to maintain business continuity, protect their data and assets, avoid financial losses, and maintain customer satisfaction. IT change management process, effective use of IT change management tools GSN, and a commitment to following best practices for risk management. Also by implementing changes successfully with minimum risk, the company could ensure that they maintain customer satisfaction and minimize any negative impact on their reputation. Overall, the company could avoid unnecessary financial losses and ensure that they are making the most of their IT investments.

Communication were key issues for successful IT change Implementation process with minimum risk. Effective communication is critical during IT change management, as it helps ensure that all stakeholders are aware of changes, their impact, and any associated risks. Global Service Now provides capabilities to support communication during IT change management process. Its effectiveness in this area depends on how it implemented and used by the selected company. Effective use of the platform requires a clear understanding of the company communication needs and a commitment to following best practices for effective communication during IT change management.

5.4 Limitation of using Global service now for IT change management process

The study also identified some limitations of the GSN platform, including its complexity and the need for ongoing training and support. While GSN provides a powerful tool for IT change management, its effectiveness is dependent on the skills and expertise of the individuals using it. The study found that, there are some General limitations of using a global service now platform for IT change management processes includes

- The complexity of a Global service now platform can be a significant limitation, especially for smaller organizations. Setting up and configuring the platform can be a complex process that requires a significant investment of time and resources. A global service now platform can be quite complex, with many features and customization options. This can make it difficult to set up and use, especially for smaller organizations that may not have the resources to invest in extensive training and support. Additionally, the platform may have many features and customization options that are not relevant to the organization's specific needs, which can make it difficult to navigate and use effectively. This complexity can also result in a steep learning curve for users, which may require extensive training and support to overcome. This can be a significant barrier for smaller organizations with limited resources, as they may not have the budget or staff to invest in extensive training and support for the platform. A global service now platform can be quite complex, with many features and customization options. This can make it difficult to set up and use, especially for smaller organizations that may not have the resources to invest in extensive training and support.
- The cost of implementing and maintaining a global service now platform can be significant, especially for organizations that need to manage a large number of IT change management processes. The platform may require a significant upfront investment in hardware, software, and implementation services, as well as ongoing costs for licensing, maintenance, and support. These costs can be difficult for smaller organizations to justify, particularly if they have limited IT budgets. As a result, smaller organizations forced to rely on manual or ad-hoc change management processes, which can be less efficient and effective than using a dedicated platform and difficult for smaller organizations to justify the investment. It is expensive, especially for organizations that need to manage a large number of IT change management processes.
- Integrating the platform with existing IT systems can be challenging and can lead to data synchronization issues and other integration problems. This can affect the accuracy and completeness of change management data, which can in turn impact decision-making and overall IT service delivery. Integration challenges can arise from a variety of factors, such as differences in data structures or incompatible APIs. Resolving these challenges may require significant technical expertise and resources, which can be a barrier for smaller organizations or those with limited IT staff. In addition, ongoing maintenance and support may be required to ensure that data remains synchronized and that the integration remains functional over time. This can lead to data synchronization issues and other integration problems, which affect the accuracy and completeness of change management data.
- Relying on a single global service now platform for IT change management processes can create a dependency on that platform limitation of relying on a single global service now platform for IT change management processes. Depending on a single platform can create a dependency that can make it difficult to switch to a

different platform if the need arises. This can limit flexibility and agility in responding to changing business needs, as well as vendor lock-in, which can be costly and difficult to escape. Additionally, changes to the platform itself, such as upgrades or modifications, may have a significant impact on an organization's IT change management processes. This can require additional training and support, and can potentially disrupt ongoing operations. As a result, organizations need carefully evaluate the potential risks and benefits of relying on a single platform, and should consider strategies for minimizing the impact of any potential disruptions or changes. This can make it difficult to switch to a different platform if the need arises, and limit flexibility and agility in responding to changing business.

6 Conclusion

In this research, the author discussed some of the aspects related to risk minimization in the IT change management process in selected company with a Case of Using Global Service Now. The use of a dedicated IT service management platform such as Global Service Now (GSN) helped the selected company to manage the IT change management process more effectively, providing a range of tools and features to support the identification, assessment, and mitigation of risks associated with IT changes. The case study presented in this thesis has demonstrated the effectiveness of GSN in minimizing IT change risks for a selected company. By implementing a structured change management process and leveraging GSN's risk management tools, the company was able to identify and assess risks associated with IT changes, and implement appropriate risk management controls to mitigate those risks.

In this approach, the author evaluate the efficiency of risk minimization in the IT change management process in a selected company. The Risk minimization is a critical component and a crucial aspect of the IT change management process and Global Service Now provides several features and tools that can help organizations minimize risks in their IT change management processes. From the result, it showed most of the changes implemented without incident indicates the company has a well-established and effective change management process that is capable of identifying and mitigating risks associated with high-risk changes. IT service management tool Global Service Now helped the company to implement changes efficiently and with minimal incidents by providing a centralized platform for change management, automated workflows, and robust reporting and analytics tools. This is why the tools ensure that risks properly assessed and addressed throughout the change management process, and that all stakeholders are aware of the risks and controls in place.

No system or process can eliminate all risks associated with implementing IT changes but it should be implement changes efficiently and with minimal risk. From this case study, the result shows using GSN highly helped the company by providing a structured and consistent approach to change management, as well as the tools and visibility needed to manage risks effectively. Using GSN tools provide three main advantage for IT change management regarding risk minimization. Firstly, provide centralized platform for IT change management, which allows change management team to track and manage all changes in a single location. This can help reduce the risk of changes processed without proper authorization or oversight, as all changes must go through the change management process in the platform. Secondly, provide automated change approvals, which can help reduce the risk of errors or delays in the change management process. Thirdly, provide robust reporting and analytics tools that can help company identify potential risks and areas for improvement in their change management processes.

I recommend Global Service Now tools for IT change management because they improve change quality and reduce the risk of change-induced incidents by ensuring that top-quality processes used to handle changes made to the IT system. It aims to make successful changes on the first try. IT change management can be a difficult and time-consuming process to implement and maintain. It necessitates cooperation between cross-functional teams within a company, and its success or failure can have a big impact on how that organization runs. The number of processes that require change management will only grow as firms adopt automated, digital, and cloud-based processes in place of manual ones. In addition, it will be crucial for these systems to operate correctly and have adequate and effective controls.

Overall, the findings of this thesis suggest that the use of a dedicated IT service management platform such as GSN can help organizations to minimize IT change risks and ensure the successful implementation of changes, while also promoting a culture of continuous risk management improvement.

7 References

Andrade, Paulo Roberto Martins de, Adriano B. Albuquerque, and WeskleiDourado Teófilo. 2016. "Change Management: Implementation and Benefits of The Change Control in the Information Technology Environment." *International Journal of Advanced Information Technology* 6(1): 23–33.

Araujo Wickboldt, Juliano et al. 2009. "Improving IT Change Management Processes with Automated Risk Assessment." *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 5841 LNCS: 71–84.

Beynon, C. 2017. "Critical Evaluation of a Range of Principles and Frameworks for Managing Change." *FPH*: www.healthknowledge.org.uk. https://www.healthknowledge.org.uk/public-health-textbook/organisation-management/5c-management-change/critical-evaluation.

Bianchin, Luís Armando et al. 2010. "Similarity Metric for Risk Assessment in IT Change Plans." *Proceedings of the 2010 International Conference on Network and Service Management, CNSM 2010*: 25–32.

Blackman, Deborah Ann, Fiona Buick, Michael Edward O'Donnell, and Nabil Ilahee. 2022. "Changing the Conversation to Create Organizational Change." *Journal of Change Management* 22(3): 252–72. https://doi.org/10.1080/14697017.2022.2040570.

Blog, SSDSI. 2023. "What Is Change Management?" *Six Sigma Development Solutions, Inc.*: sixsigmadsi.com. https://sixsigmadsi.com/change-management/ (March 27, 2023).

Bulling, Kai. 2018. "Organizational Change and Change Management: Phenomenon, Task and Approaches." (February): 29–91.

Cater-Steel, Aileen, and Mark Toleman. 2010. "IT Service Management Standards." : 225–41.

Caver, Keith, and Ancella Livers. 2021. "The Paradox of the Seed and Soil: Cultivating Inclusive Leadership for a 'New Normal.'" *Leadership* 17(1): 18–31.

Cho, Jin Young, Dong Youl Lee, Yong Jun Lee, and Min Jae Lee. 2015. "Effective Change Management Process for Mega Program Projects." *Journal of Asian Architecture and Building Engineering* 14(1): 81–88.

Dempsey, Mary, Lisa Geitner, Attracta Brennan, and John Mcavoy. 2022. "A Review of the Success and Failure Factors for Change Management." *IEEE Engineering Management Review* 50(1): 85–93.

Eisenhower, Dwight D. 2019. "No TitThe Definitive Guide to Organizational Change Management." *SweetProcess*. https://www.sweetprocess.com/organizational-change-management/ (March 27, 2023).

El-taliawi, Ola G. 2020. "Global Encyclopedia of Public Administration, Public Policy, and Governance." *Global Encyclopedia of Public Administration, Public Policy, and Governance* (May).

Gabrie Onuche. 2021. "World Journal of Management and Business Studies (ISSN: 2795-2525)." 1(2): 87–104.

GSN. 2021. “Create an Organizational Change Management Plan.” : 1–26.

Hanelt, André, René Bohnsack, David Marz, and Cláudia Antunes Marante. 2021. “A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change.” *Journal of Management Studies* 58(5): 1159–97.

Hansen, Michael Motet. 2008. “Reßective Writing about a Change Management Role Play.” (November): 1–3.

Heckelman, Wendy. 2017. “Five Critical Principles to Guide Organizational Change.” *OD Practitioner* 49(4): 13–21.

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. 2019. “The European Union General Data Protection Regulation: What It Is and What It Means.” *Information and Communications Technology Law* 28(1): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

IRM. 2011. Federation of European Risk Management Associations *Risk Management Standard*.

ITIL. 2019. *ITIL Service Transition Version 4.0.* Office of Government Commerce.

Jaiswal, Manishaben. 2019. “Risk Analysis in Information Technology.” *International Journal of Scientific Research and Engineering Development* 2(6): 857–60. http://www.ijsred.com/volume2/issue6/IJSRED-V2I6P110.pdf.

Kumar, N Senthil, and Shailendra Rajan. 2018. “Understanding the Change Management in the Information Technology (IT) Services Industry.” 5(April): 26–34.

Kumar, Sonjai. 2021. Researchgate.Net *Sonjai Kumar ,*.

Lewis, Laurie. 2019. *Origins and Traditions of Organizational Communication*. 1st Editio.

Lucio-Nieto, Teresa, and Ricardo Colomo-Palacios. 2012. “ITIL and the Creation of a Service Management Office (SMO): A New Challenge for IT Professionals - An Exploratory Study of Latin American Companies.” *Iberian Conference on Information Systems and Technologies, CISTI*: 1–6.

Machado, Guilherme Sperb et al. 2008. “Enabling Rollback Support in IT Change Management Systems.” *NOMS 2008 - IEEE/IFIP Network Operations and Management Symposium: Pervasive Management for Ubiquitous Networks and Services* (May 2020): 347–54.

Niederman, Fred, Thomas W. Ferratt, and Eileen M. Trauth. 2016. “On the Co-Evolution of Information Technology and Information Systems Personnel.” *Data Base for Advances in Information Systems* 47(1): 29–50.

Passenheim, Olaf. 2010. 1 Introduction to Information Security *Change Management Change Management; The People Side of Change*. bookon.com.

Petrikina, Jurate et al. 2017. “Improving the Readiness for Change – Addressing Information Concerns of Internal Stakeholders in the SmartPORT Hamburg.” *AMCIS 2017 - America’s Conference on Information Systems: A Tradition of Innovation* 2017-Augus: 1–10.

Prosci. 2018. Thought Leadership Articles *The Best Practices in Change Management*.

https://www.prosci.com/resources/articles.

Rousseau, Denise M., and Steven ten Have. 2022. "Evidence-Based Change Management." *Organizational Dynamics* 51(3): 100899. https://doi.org/10.1016/j.orgdyn.2022.100899.

Rudnev, Evgeny A. 2020. "Five Challenges of Change Management." *International Journal of Human Resource Studies* 10(4): 333.

Russell, Nick, Wil Van Der Aalst, and Arthur Ter Hofstede. 2006. "Workflow Exception Patterns." *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 4001 LNCS: 288–302.

Sacolick, Isaac. 2023. "A Brief History of the Agile Methodology." *www.infoworld.com*. https://www.infoworld.com/article/3655646/a-brief-history-of-the-agile-methodology.html (March 27, 2023).

Saeidi, Parvaneh et al. 2019. "The Impact of Enterprise Risk Management on Competitive Advantage by Moderating Role of Information Technology." *Computer Standards and Interfaces* 63(April 2018): 67–82. https://doi.org/10.1016/j.csi.2018.11.009.

Savajia, Vishal. 2021. "What Is IT Change Management." *sevice now*. https://www.servicenow.com/community/itsm-articles/what-is-it-change-management/ta-p/2307751.

Servicenow. 2019. "01 Developer Platform Introduction - Module 1 - Platform Basics Introduction to an Instance."

Shaw, Marcel. 2019. "Why Is Change Management Critical for Software Asset Management?" *Experfy Inc.* https://resources.experfy.com/bigdata-cloud/why-is-change-management-critical-to-software-asset-management/ (March 28, 2023).

da Silva, Fátima Aguiar da, WeskleiDourado Teófilo, Adriano B Albuquerque, and Paulo Roberto Martins de Andrade. 2016. "C Hange M Anagement and B Usiness a Nalysis P Ractise." *International Journal of Advanced Information Technology (IJAIT)* 6(1): 31–33.

Sousa, Eduardo Da Silva, Carlos Eduardo Machado Pires, Simone Borges Simão Monteiro, and Ana Carla Bittencourt Reis. 2019. "It Change Management Process Improvement." *Revista Singular - Engenharia, Tecnologia e Gestão* 1(1): 21–26.

Statistics, Labor et al. 2022. "American Time Use Survey - 2021 Results." (202).

Utah. 2023. "Risk Assessment." *ServiceNow*. https://docs.servicenow.com/en-US/bundle/utah-it-service-management/page/product/change-management/concept/c_RskAsmtCalc.html (March 27, 2023).

Wickboldt, Juliano Araújo et al. 2009. "A Solution to Support Risk Analysis on IT Change Management." *2009 IFIP/IEEE International Symposium on Integrated Network Management, IM 2009*: 445–52.

Zolghadr, Mahsa, and Farid Asgari. 2016. "Creating a Climate and Culture for Sustainable Organizational Change." *Management Science Letters* 6: 681–90.

7.1 List of pictures

7.2 List of tables

7.3 List of abbreviations

IT	Information Technology
ITIL	Information Technology Infrastructure Library
GSN	Global Service Now
RFC	Request of Change
CAB	Change Advisory Board
CI	Configuration Item
INC	Incident
AF	Activity Failure
ITSM	IT Service Management
HF	Human Failure
TF	Time Failure
CV	Constraint Violation
ET	External Trigger
RTP	Release to Production
ROI	Return on Investment
RFSC	Request for Standard change
CoE	Centre of Excellence
ROI	Return on Investment)
PIR	Post-implementation review