Risk Management Project

[Author’s name]

[Institute’s name]

Risk Management Project

**Introduction**

Currently, risk management is recognised as a necessary condition for business organisations to successfully enhance their performance level. Proper planning and implementation of the broad idea of risk management is a critical condition to effectively avail possible opportunities and avoid various forms of business risks. The approach of risk management is comprised of practical steps of anticipation and assessment of different forms of risks. The central aim of this approach is to strategically minimise the impact of different business hazards under the spectrum of the risk management process (Olechowski et al., 2016). In simple words, risk management can be characterised as the systematic procedure of classifying, evaluating, and controlling different forms of threats with the help of wide-ranging organisational resources. It is mandatory for the organisations to follow specific protocols or principles to reduce the effect of uncertainty that appeared as great risk or uncertainty for the organisations. In this report, the primary focus is to consider the issue of risk management for the organisation of Optus to critically analyse the practical perspective of risk management project.

**Discussion**

The application of risk management can be observed in many different forms that require the adoption of appropriate guidelines under the domain of risk treatment. A critical consideration of any specific organisation under the scenario of organisational risk is the feasible condition to make better inferences about the suitability of different standards of risk management. The corporate organisation of Optus is selected to comprehensively examine the overall prospect of risk management by identifying the issue of specific risk. The company of Optus is categorized as the second-largest telecommunications company operating in Australia that provides broadband and internet services to potential customers.

**Organisational Context**

Identification of the organisational context of Optus is an obligatory condition to completely apprehends the entire scenario of risk in this manner. This form of understanding further helps to figure out the organisation’s performance in case of appropriate risk management. Furthermore, exploration and examination of risk criteria of Optus is also a crucial approach to determine the real success of the scenario of risk management.

**Summary of Optus’s Scope**

The higher management of Optus is committed to offer and establish a significant plan of action to successfully achieve the objective of risk management effectively and efficiently. The wide-ranging idea of organisation’s scope is helpful to explore the overall planning of Optus when it comes to utilising organisational resources to achieve the objectives of security and risk management. The organisational scope of Optus consisted of different integrated processes and resources to ensure the successful completion of business projects by successfully address different organisational hazards.

It is observed that the corporate domain of Optus is committed to offering a comprehensive security assessment service to ensure successful exploration and assessment of ICT security risks. The central aim of this consideration is to offer secure evaluation outcomes to potential clients with the domain of minimal risk exposure (Barafort et al., 2017). The organisation of Optus focuses on successfully implement the approach of risk management by implementing Work Health and Safety (WHS) risk management procedures according to the organisation’s requirements. The overall scope Optus in the scenario of risk management appears as the proper application of minimum WHS requirements and the principles of the Commonwealth WHS Act 2011. The scope of work in the case of Optus ranges to different workplace activities such as excavation, electrical procedure, confined areas, telecommunication work, and other organisational practices. The overall organisation’s scope is closely linked to Optus’s main objectives and business considerations. The central objective of Optus appeared as the development of improved sustainability in organisation’s culture, values, decision-making, potential products, and services for the sake of developing a sustainable business environment with the proper handling of risks.

**External and Internal Contexts**

A detailed examination of external and internal contexts in the practical scenario of Optus is an important condition to determine the specific need and requirements of risk management. The comprehensive risk management framework comprised of both the prospects of external and internal environmental conditions for Optus. There are different external and internal parameters that help to illustrate the paradigm of risk management for the telecommunication organisation of Optus. A proper understanding of external and internal contexts is a necessary condition to examine the prevailing prospects in the case of Optus.

The practical perspective of the external context contains all the different external environment parameters that greatly impact the organisation’s approach during the process of risk management. External stakeholders for Optus can mainly be recognised as its local, national, and global business environment, its main corporate-driving domains, and the facet of organisational objectives. Moreover, various forms of stakeholders’ values, perception, and their connection with different social, cultural, political, legal, regulatory, technological, economic, and competitive environmental aspects also influence the company’s position under the paradigm of external context (Radack, 2011). The overall risk management approach of Optus greatly influenced by the political environment of the country. This specific scenario turned to the significant changes in changing rules and policies established by the Australian government. Additionally, the external business environment for Optus also closely linked with the practical spectrum of economic factors. The presence of economic instability naturally impacts the prospect of investment for the telecommunication company of Optus.

All the internal organisational parameters of Optus established under the spectrum of internal context. This domain explicitly describes the approach adopted by the organisation to successfully manage existing risk. All the available capabilities and skills of Optus identified under the spectrum of internal environmental context. The objective of sustainability closely linked with the internal parameters adopted by the organisation of Optus. The internal stakeholders of the organisation appeared as its internal operations to achieve the objectives of business enhancement and sustainability.

**Optus’s Risk Criteria and Accepted Risk Levels**

The practical approach of risk criteria is adopted to make better inferences in case of the existing level of risk within the organisational scenario. In other words, risk criteria comprised of various terms that can be assistive to determine the significance or importance of the overall organisation’s risk. The documented standard of risk within the organisational setting is the guiding principle for the management to decide whether the existing risk level is tolerable or not. In the context of the business functioning of Optus, WHS standards followed to meet the anticipated domain of compliance and risk management. The acceptable risk level recognised as the expected level of risk exposure for the organisation because the prospect of risk can never be fully eradicated as its probability can never be zero. The accepted risk level for Optus Australia appeared as the insignificant prospect of compliance and conflict of interest.

**Risk Identification**

Risk identification is illustrated as one of the most important approaches to successfully deal with different hazards at the organisational level. The phase of risk identification helps to explore the operating area that requires necessary and immediate fixation. The practical process of risk identification for the organisation of Optus is also useful to determine potential risk aspects and offer a better form of risk treatment accordingly. A comprehensive procedure of risk identification permits to successfully explore and analyse potential events in an organisational setting that can cause a great form of risk for the organisation. Proper adoption of the systematic procedure of risk identification also helps to examine the nature and specific levels of risks within the organisational domain (Chowdhury & Arefeen, 2011). Consideration of specific principles and guidelines is an essential condition to successfully identify potential risks that prevail for the telecommunication company of Optus in the competitive corporate setting.

**Improper Digital Development and Variation**

Extensive research of telecommunication competitive market explicitly revealed that the digital domain is dramatically growing. Telecommunication companies are competing when it comes to providing digital services to potential customers (Torabi et al., 2016). The growing prospect of diversification is one major risk for Optus to maximise profitability level by adopting required innovative business models according to the market’s opportunities. This type of risk eventually influences the organisational performance and value of the company.

**Insufficient Application of Changing Requirements in Privacy, Security, and Trust**

Today, ensuring the desired form of privacy, security, and trust of potential customers and workers is one of the most challenging business aspects for the telecommunication organisation. There are plenty of cases on record where companies faced the allegation of a data breach or information theft. Telecommunication companies are continuously facing the consumers’ concerns when it comes to their security and privacy in case of online data (Frigo & Anderson, 2011). Undoubtedly, it is a critical approach for telecommunication companies to build the desired domain of trust between organisations and potential consumers. The hazard of data breaches immensely faced by the organisation of Optus that ultimately affects the overall credibility of this company. It is complained by many customers that they faced the issue of privacy breaches in case of personal information such as their names, addressed, and other related details. The phenomenon of cybersecurity was greatly at risk under the business perspective of Optus as the telecommunication company.

**Incapability to Successfully Adopt Internal Digitization Initiatives**

The current competitive business environment requires successfully transforming customers’ experiences when it comes to offering digital initiatives to them. There is a number of organisations that are focused on delivering multilayer digital transformation domains for the customers effectively and efficiently (Saleh & Alfantookh, 2011). This changing digital perspective is characterised as a major business risk for the company to ensure its value by adopting modified forms of digital skills.

**Failure to Properly Arrange Workforce Planning and Design**

It is a challenging aspect for the telecom companies to maintain workforce environment according to a rapidly changing competitive environment. It is one great risk under the domain of risk management principles that organisations need to face when it comes to workforce planning and design. Attainment of digital skills is one major hazard for the company considering the objective of digital transformation. Development of workforce design according to the new business requirement is one of the central risks for the organisation that requires necessary attention. Provision of greater customer experience with the utilisation of workforce engagement is a major practical task for the telecom company.

**Failure to Appropriately Direct Interruption Scenarios**

Proper fixation of any disruption in the form of digital service is one of the greatest risks for the organisations when it comes to achieving the objective of performance enhancement. Market demands are constantly changing due to the prospect of innovation that requires drastic policy alterations. This sort of challenge can be examined specifically through the example of 5G momentum. The growing trend of technology advancement in the field of telecom made it challenging and necessary for Optus to enhance its performance competitiveness and successfully address potential disruptive hazards. The changing business scenario is a growing risk for the organisation that requires an immediate plan of action on practical grounds.

**Inadequate Portfolio Management Procedures**

The growing business environment demands organisations to successfully implement the idea of better management processes. It is one great challenge that requires proper risk management and treatment plan considering the importance of different management processes (Racz et al., 2010). Convergence is a necessary condition that requires the adoption of proper management procedure according to the changing administrative requirements.

**Failure to Acclimate to Changing Governing Contexts**

The intervention of appropriate governance can never be ignored as it appeared as one great risk factor for the organisations. The changing perspective of governing contexts requires immediate and flexible changes to successfully evaluate and deals with this form of risk. Consideration of regulatory frameworks is a challenging condition for the company that eventually appeared as development in innovative strategies.

**Lacking Engagement with Industry and Public Sector Setting**

Insufficient form of work engagement within an industrial setting is one of the greatest risk factors that influence the final outcomes in the form of organisational performance. It is one of the primary standards for the telecom organisation to establish a balanced operating domain with the overall functioning of industry and public sector setting (Tupa et al., 2017). The growing form of digital transformation is a challenging condition for the telecom company to successfully apprehends the prospect of the desired level of market engagement and public sector involvement.

**Risk Analysis and Evaluation**

A successful application of phase of risk identification eventually leads to the stages of risk analysis and assessment. It requires understanding the overall nature and scope of the risk under the comprehensive prospect of risk analysis and evaluation. Consideration of specific standards is an obligatory condition to successfully apprehends the two major stages of risk analysis and evaluation during the entire domain of risk management plan according to the requirements of the organisation. The insufficient paradigm of privacy, security, and trust, improper management procedures, and failure to successfully arrange workforce planning and design are characterised as three major risk aspects appeared in case of corporate functioning of Optus as leading telecommunication organisation. It is important to analyse and evaluate the entire spectrum of risk in case of these challenges or hazards to successfully examine the entire domain of risk management (Gjerdrum & Peter, 2011). The broader prospect of risk assessment comprised of two main conditions or requirements identified as risk analysis and risk evaluation. A proper establishment of both these domains is an essential condition to figure out the intensity of the risk and propose better solutions to successfully deals with potential hazards.

**Risk Analysis**

After the first phase of risk identification, the next crucial stage under the spectrum of risk analysis has appeared as risk analysis. This practical approach is adopted in case of potential hazards facing by the organisation of Optus in the telecommunication industry. These risks are mainly identified in the form of inadequate approach to privacy, security, and trust, failure in the form of management processes, and proper development of workforce planning and designing according to organisational requirements. The stage of risk analysis is helpful to successfully anticipate the likelihood that these risks or threats can be materialised in case of the functioning of Optus in the market. It is a systematic procedure to evaluate the intensity of possible risks in the scenario of organisational operations. Additionally, risk analysis is illustrated as the proven form of action to successfully identify and assess all the features that can negatively affect the business functioning of Optus. The outcomes of this specific stage are also viable to make better inferences whether the company needs to move forward with a decision or establish some other operating prospect.

           The perspective of risk analysis can never be considered complete without focusing on the influences of different assumptions, and consequences of different interrelated events or the company. This form of consideration is a suitable instrument to determine the intensity of hazard that prevails for Optus in case of all three major risks. Routine monitoring of everyday business activities in the scenario of Optus revealed that there is high risk involves when it comes to the privacy of customers’ personal information. The potential of hazard is also intense concerning to successful application of workforce planning and designing according to the need of the situation. Risk estimation is a mandatory condition that needs to be followed under the broader spectrum of risk analysis. The possible impact and likelihood of occurrence of these potential risks in future can only determine by adopting the standard of risk estimation. Consideration of possible controls in the organisational scenario is a suitable practical condition to make better inferences about the existing organisational operations. A critical examination of past events in the organisation’s history is also a necessary condition to successfully examine the entire scenario of risk for the organisation (Cagliano et al., 2015). Referring to the case of Optus as a telecommunication company operating in the Australian market, it is examined that in past, this organisation faced the challenge of a privacy breach at an extensive level. This form of fact identification ultimately explained the likelihood of the appearance of risks in future.

**Risk Evaluation**

           The primary objective of applying the process of risk evaluation is to assist the required form of decisions in case of potential risks and possible outcomes. The standard of risk evaluation is helpful to make a vital decision that which form of risk treatment is required in the organisational scenario of Optus by focusing its potential threats or managerial challenges. The practical phase of risk analysis revealed that there are high chances of risk in case of the issue of security, privacy, and trust for the potential customers. Moreover, the intensity of risk is also high when the organisation is keen to develop and design a competitive workforce according to the changing requirements of the market. The primary focus of criteria of risk evaluation is to ensure the provision of effective input in the scenario of prioritising risk treatments according to the need of specific organisational situation.

           It is established that continuous exposure to a specific form of risk can cause great damage for the company referring the approach of proper organisational management. The stage of risk evaluation is a practical foundation to compare the outcomes of risk analysis with the specific standard of risk evaluation (McNutt et al., 2010). The results of this prospect explicitly indicate whether the existing level of risks is acceptable for the company or not. The practical scenario of risk evaluation is a good approach to examine the intensity of risk exists for Optus mainly in case of hazards of a data breach and data theft. Consequences and probability of each major risk for the company assist to successfully implement the practical idea of risk evaluation.

**Risk Treatment**

Risk treatment is defined as a practical stage to adopt specific strategies to address potential risks appears for the project or the organisation. The procedure of risk treatment involves the adoption of different interconnected domains of consideration. The first phase of the approach of risk treatment is to critically evaluate the effectiveness of risk treatment. The next step is to make a rational decision on whether residual risk levels are acceptable for the company or not. The next facet of consideration in case of high risk is to create a feasible form of new risk treatment according to the need of changing situation. It is also important to critically examine the overall suitability of the risk treatment (Hoffmann et al., 2013). It is noteworthy to mention that all the selected options of risk treatment need to successfully aligned with the requirements of the specific operating situation.

           The first phase of risk treatment explicitly indicates that the organisation of Optus have different options in case of a proper form of risk treatment. The first option for the company in the form of risk treatment is to adopt the option of avoiding the risk by rejecting the idea of a new start or continue with the practice that ultimately enhances the level of risk. The second available option in the form of risk treatment is to increase the existing level of risk to further enhance the potential of opportunity for the sake of advanced benefit. The third available option for the company is to completely eradicate the possible risk source. Changing the spectrum of likelihood is another available option under the spectrum of risk treatment. Adoption of a contingency plan to change consequences is another prominent option for the company to successfully deal with an existing form of risk. Shifting the magnitude of risk to any other party is another practical way to minimise the negative consequences of any potential risk. Retaining the paradigm of risk in the form of informed decision is another prominent option to successfully handle the problem of potential organisational risks.

           A critical assessment of treatment options is a mandatory condition to propose the most suitable approach considering the practical scenario of the organisation. This form of information is also helpful to formulate a treatment plan according to the requirements of the situation. Balancing the available forms of costs and efforts of application is basic criteria when it comes to selecting the most suitable risk treatment option. It is viable for the company of Optus to adopt the combination of different risk treatment options to successfully deal with different existing hazards in a successful manner. The next step is to develop a treatment plan that describes the level of priority in the form of offering different risk treatment options with the focus of successful implementation (Fernández-Muñiz et al., 2012). Application of specific assumptions helps to determine that the combination of retaining the risk by the informed decision and successful pursuit of priority are significant forms under the domain of risk treatment plan.

**Organisational Risk Management Strategies**

The management of the company needs to be vigilant when it comes to adopting specific risk management strategies according to the requirements of the situation. The successful spectrum of risk management has appeared in four major forms of possibly avoiding the risk, reducing it, transfer it, and accept it to gain better outcomes from the situation (Chapman, 2011). Development of the appropriate plan is a central risk management strategy to successfully handle the existing domain of risk.

           Forming a rational decision to handle different forms of risk is another critical risk management strategy to achieve desired outcomes. All the four strategies of avoiding, reducing, transferring, and accepting risks have some potential advantages and limitations. It is important for the company’s management to select the most suitable option according to the company’s need. Reducing the existing form of risk is the strategic option selected for the organisation to obtain better results from the existing situation. The central limitation of this risk management strategy is that might lead to an ineffective form of controls for the company.

**Conclusion**

To conclude the discussion on the approach of risk management specifically in the scenario of the organisational setting of Optus, it is vital to indicate that complete avoidance of risk is not possible. Business organisations have to deal with the issue of risk in case of diverse forms that impact existing approaches of business in different forms. Reducing the existing form of risk is a suitable condition that can only achieve by implementing a comprehensive risk management plan according to the need of the organisation.

**References**

Barafort, B., Mesquida, A.-L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, *54*, 176–185.

Cagliano, A. C., Grimaldi, S., & Rafele, C. (2015). Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research*, *18*(2), 232–248.

Chapman, R. J. (2011). *Simple tools and techniques for enterprise risk management* (Vol. 553). John Wiley & Sons.

Chowdhury, A. A. M., & Arefeen, S. (2011). Software risk management: Importance and practices. *IJCIT, ISSN*, 2078–5828.

Fernández-Muñiz, B., Montes-Peón, J. M., & Vázquez-Ordás, C. J. (2012). Occupational risk management under the OHSAS 18001 standard: Analysis of perceptions and attitudes of certified firms. *Journal of Cleaner Production*, *24*, 36–47.

Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting & Finance*, *22*(3), 81–88.

Gjerdrum, D., & Peter, M. (2011). The new international standard on the practice of risk management–A comparison of ISO 31000: 2009 and the COSO ERM framework. *Risk Management*, *31*(21), 8–12.

Hoffmann, P., Schiele, H., & Krabbendam, K. (2013). Uncertainty, supply risk management and their impact on performance. *Journal of Purchasing and Supply Management*, *19*(3), 199–211.

McNutt, P. A., Demidenko, E., & McNutt, P. (2010). The ethics of enterprise risk management as a key component of corporate governance. *International Journal of Social Economics*.

Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play? *International Journal of Project Management*, *34*(8), 1568–1578.

Racz, N., Weippl, E., & Seufert, A. (2010). A process model for integrated IT governance, risk, and compliance management. *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)*, 155–170.

Radack, S. (2011). *Managing information security risk: Organization, mission and information system view*. National Institute of Standards and Technology.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, *9*(2), 107–118.

Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, *89*, 201–218.

Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of risk management implementation for Industry 4.0. *Procedia Manufacturing*, *11*, 1223–1230.