

Midocean University

College of Management

Department of Risk management

**Establishment of a Governance Framework for Managing Technical Risks  
and Ensuring Business Continuity in government agencies and institutions  
within Saudi Arabia's Digital Government Realm**

إنشاء إطار حوكمة لإدارة المخاطر الفنية وضمان استمرارية الأعمال في الجهات  
والمؤسسات الحكومية في مجال الحكومة الرقمية في المملكة العربية السعودية

Prepared by:

Bader Alzahrani (221001860) Team Leader

Khalid Aldakhil (221001911)

Abdulaziz Aldakhil (221002030)

**Final Project – Proposal MGM697**

Supervised by:

Dr. Walid Suliman

Year:2023

## Introduction

Digital government is associated with various types of characteristics that enable it to cope with quite a number of digital inventions in this modern developed world. Moreover, the transformation digitally the entire Saudi government is something that is not a mere enabler but changed for the purposes of defining and reinventing the very pillar of what a government should be able to do (Al Mansoori, Sarabdeen & Tchantchane, 2018). Furthermore, this is very critical and imperative since technology is currently on the verge of developing into new horizons. Additionally, in relation to Vision 2030, the entire digital transformation that is linked to the Saudi Government is viewed to be a form of integral, conclusive together with a pragmatic kind of strategy that majorly aims towards enabling and even accelerating the transformation of the whole government in an efficient and effective manner. Interestingly, such kind of a transformation has also been implemented by quite a number of e-government programs and even projects, empowering and even supporting various forms of government organizations and authorities (Al-Mushayt, 2019). It majorly ranges from being able to have all reliable government services that are available from a digital perspective, accessed through the easiest ways possible by having different types of citizens as a consistent look and feel and at the same time be strategically centered within the boundaries of specific life events. Again, the entire digital transformation has been strategically designed for the purposes of maintaining a well-organized architecture alignment and being fit for this digital age that is adequately empowered by a vast range of digital skills and capabilities alongside a variety of fundamental tools (Alzahrani, Al-Karaghoulis & Weerakkody, 2018). Digital government, like the one that is linked to the Saudi government, is made up of quite a number of critical data that are managed and operated from a digital perspective. Due to this, the process of risk management has been very critical for such kind of a government since it helps in the

management of all its data from a range of perspectives and even goes ahead to prevent the occurrence of any form of future risks that might end up acting as a threat to the digital government.

### **Problem statement**

Risk management for a digital government majorly entails the government's ability to access, monitor, and even treat a variety of existing risks that might emerge from the entire process of digital transformation within the government boundaries. Different digital governments, like the Saudi government, have always been subjected to quite a number of threats and risks that are linked to the government's data. As a result, interference with such kinds of critical data for the government might end up subjecting it to serious impacts that might even go the extra mile to ruin its reputation. Due to this, the implementation of risk management for the digital government, therefore, plays a critical role in helping the government in relation to its departments to put much concentration on the existence of various threats and risks that are linked to its data together with the whole IT systems that are capable of processing the same data.

### **Justification of the study**

Risk management is a very important process that is known to be constituting quite a number of processes that are always taken into consideration with the intention of mitigating any risks that might be available within a specific context. As a result, when dealing with different forms of digital governments like the Saudi government, the context of risk management is majorly important when it comes to handling and managing various forms of data that are linked to the government by making sure that they are kept away from any type of existing risks or even threats. Due to this, one of the major purposes of implementing this research will therefore be to determine some of the major benefits that risk management has been able to bring on board to the digital government of Saudi Arabia. At the same time, it will also be carried out for the purposes of creating awareness on how risk

management processes can always be implemented across different types of digital governments for the purposes of addressing different types of goals and objectives.

### **Research objectives**

- To access different benefits of risk management to the Saudi Arabia digital government
- Analyze how Saudi Arabia has been able to embrace risk management strategies across different departments in order to address different goals and objectives.
- Create awareness of how risk management strategies create a critical role in making sure that various digital governments like Saudi Arabia are in a position to perform competitively in relation to their economies.

### **Research Questions**

- (1) What are some of the major benefits that risk management has been able to bring to digital governments like Saudi Arabia?
- (2) How has risk management played a critical role in protecting the critical data that are linked to Saudi Arabia's digital government?
- (3) What are the risk management strategies that Saudi Arabia's digital government has been able to implement the order to obtain competitive data protection?

### **Literature Review**

According to Arias & Maçada (2018), in order to attain all its strategic objectives and even go as far as supporting all the achievements of the objectives that are linked to Vision 2030 for the purposes of enhancing reliability alongside the continuity of various forms of digital services that are offered by different types of government entities, the Digital Government Authority has been able to come up with an advanced mode of "Risk Management Guidelines for Digital Government" in order to focus on some

of the major importance of adopting risk management in relation to quite a number of variables and risk at the principle of different levels, that might negatively impact on the achievement of all vision and objectives of a government sector. Furthermore, the research conducted by Kumar, Sachan & Mukherjee (2018) clearly states that as digital transformation is being encountered at a faster rate across different parts of the world, a much clear and detailed risk management framework across different government entities is absolutely essential for the purposes of ensuring that different risks that are linked to global changes are adequately organized, new types of technologies are implemented, various types of procedures and communication channels are changed, evaluated and even managed in an appropriate manner. In Saudi Arabia, the Digital Government Authority plays a critical role when it comes to providing various Government Entities with advanced technical and advisory expertise together with fundamental criteria that the government can use in order to implement various forms of transformation models (Santa, MacDonald & Ferrer, 2019). In relation to Saudi Arabia's digital government policy, it has been able to set an overall direction for the purposes of attaining a more sustainable long-term digital transformation for the entire government (Sundberg, 2019). Furthermore, it also offers full support for all the strategic plans that are linked to the government entities, most so the ones that are fully aligned with the National Digital Government Strategy.

## **Methodology**

This research will be able to make good use of quantitative methodology as a critical method of data collection that will further ensure that all the documented goals and objectives of the research are properly addressed. The use of the quantitative methodology will help the research to be able to adequately measure the opinions of various types of participants in order to obtain the right combination of information from them to ensure that all the research questions are perfectly answered. By incorporating this type of methodology within the research, the following methods of data collection will have to be used;

**Surveys-** Through this method, data will be collected from a pool of different research respondents by asking them quite a number of survey questions in relation to the study topic. Furthermore, the surveys will be administered in form of questionnaires of different types of questions.

**Controlled observations-** This is also another critical quantitative data collection method that the research will also have to use. As a result, it will be used to keenly study the behaviors of different risk management experts within a carefully controlled and structured environment in order to come up with more accurate information for the purposes of analysis within the research.

**Interviews-** The use of quantitative interview as a method of data collection in this research will majorly be linked to the use of different types of closed-ended questions that will have to be appropriately delivered in the same format and in the same order to all the respondents who will be included within the research. Furthermore, the analysis of data for this quantitative interview will be done by assigning a numerical value to the responses that will be offered by the participants.

### **Fields of study**

The study majorly encompasses quite a number of key fields, amalgamating technology, governance together with risk management that exists within the real of digital government. Additionally, it navigates the intricate interplay of all these domains in order to forge a comprehensive understanding on how various types of technical risks can be adequately managed in order to ensure uninterrupted business continuity. Moreover, this interdisciplinary investigation draws upon various insights emerging from technology management, governance framework together with risk assessment methodologies, shading more light on the intricate landscape of various forms of digital government operations.

### Time Plan

| Activity          | Timeline |
|-------------------|----------|
| Introduction      | 1 Month  |
| Problem statement | 2 weeks  |
| Justification     | 2 weeks  |
| Literature review | 1 Month  |
| Methodology       | 3 Weeks  |

## **Conclusion**

Risk management for a digital government is a crucial process that needs to be understood by almost every type of digital government. Additionally, various digital governments like the ones in Saudi Arabia have been able to pave the way for quite a number of government agencies within the country to offer adequate and reliable digital services that end up contributing towards high investment returns to the extent of even raising the value of the entire national economy and even work towards measuring the performance levels and capabilities of all the government agencies that are known to be existing within the digital government. It is, therefore, important to understand the risk management of digital governments from a range of perspectives in order to develop a clear view of how various data-related risks within such governments can always be minimized.

## References

- Al Mansoori, K. A., Sarabdeen, J., & Tchantchane, A. L. (2018). Investigating Emirati citizens' adoption of e-government services in Abu Dhabi using modified UTAUT model. *Information Technology & People*, 31(2), 455-481.
- Al-Mushayt, O. S. (2019). Automating E-government services with artificial intelligence. *IEEE Access*, 7, 146821-146829.
- Alzahrani, L., Al-Karaghoul, W., & Weerakkody, V. (2018). Investigating the impact of citizens' trust toward the successful adoption of e-government: A multigroup analysis of gender, age, and internet experience. *Information Systems Management*, 35(2), 124-146.
- Arias, M. I., & Maçada, A. C. G. (2018). Digital government for e-government service quality: a literature review. In *Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance* (pp. 7-17).
- Kumar, R., Sachan, A., & Mukherjee, A. (2018). Direct vs indirect e-government adoption: an exploratory study. *Digital policy, regulation and governance*.
- Santa, R., MacDonald, J. B., & Ferrer, M. (2019). The role of trust in e-Government effectiveness, operational effectiveness and user satisfaction: Lessons from Saudi Arabia in e-G2B. *Government Information Quarterly*, 36(1), 39-50.
- Sundberg, L. (2019). Electronic government: Towards e-democracy or democracy at risk?. *Safety science*, 118, 22-32.