

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)

Supervised by:

Dr. Walid Suliman

Year:2023

Content index

<i>Introduction.....</i>	<i>3</i>
<i>Literature Review.....</i>	<i>6</i>
The digital government of Saudi Arabia	6
Professionals in the Digital Government of Saudi Arabia	8
Various risks faced by the digital government in Saudi Arabia	10
Risk Management frameworks that are used by the Saudi Arabia Digital Government	12
Identification of challenges and barriers to effective risk management in the digital government of Saudi Arabia.....	15
<i>Methodology.....</i>	<i>18</i>
Research design	18
Sample and population.....	18
Data Collection	18
Survey method	18
Controlled observations.....	19
Interviews	19
Data Analysis.....	19
<i>Findings</i>	<i>20</i>
<i>List Of figures :</i>	
<i>(Figure1: Online survey responses on the benefits of risk management to the digital government of Saudi Arabia).....</i>	<i>21</i>
<i>(Figure2: interview reponses on the benefits of risk management to the digital government of Saudi Arabia.....</i>	<i>21</i>
<i>Discussions.....</i>	<i>22</i>
<i>Limitations of Research</i>	<i>24</i>
<i>Ethical considerations.....</i>	<i>25</i>
<i>Conclusion.....</i>	<i>27</i>
<i>References.....</i>	<i>29</i>

Introduction

In this era that is marked by rapid technological advancements and a high rate of digitization, a lot of governments across different parts of the world are currently embracing the implementation of digital information within their respective boundaries in order to streamline their operations and even enhance the overall levels of public service delivery. Saudi Arabia is among the major governments that have gained popularity due to its ambitious vision 2020 agenda and is no exception in this particular situation (Alrubaiq & Alharbi, 2021). The entire digital government of Saudi Arabia is actively harnessing advanced modes of technologies that all aim towards harnessing the way it is able to interact with various citizens, businesses, and even stakeholders who are responsible for various roles within the boundaries of the government. As there is a rapid expansion in the digital landscape, this also expands the potential for various risks together with a series of different types of vulnerabilities. Due to this, the government must therefore navigate a complex web associated with cyber security threats, data breaches, and various concerns related to privacy alongside a wide range of technological disruptions. In order to navigate this kind of dynamic environment in an effective manner, the implementation of robust risk management practices becomes very critical. 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-Karaghoul & 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. This work, therefore, aims to carry out a deep exploration of some of the major benefits that are associated with risk management for the digital government of Saudi Arabia. Furthermore, it will clearly capture how the adoption of a more proactive and comprehensive approach to risk management can safeguard a wide range of sensitive information, ensure there is the continuity of advanced operations, and even foster higher levels of public trust. As a result of adequately managing various risks in an effective manner, the digital government is capable of unlocking quite a number of huge advantages that majorly range from improved decision-making and allocation of various resources to enhanced delivery of various services and long-term sustainability levels. In the following sections, the documentation will put much focus on specific benefits that are linked to risk management for the digital government of Saudi Arabia, addressing some of the major areas like cybersecurity, data protection, various forms of regulatory

compliance together with innovation. As a result of adequately examining all these aspects, it is much easier to gain a deeper understanding of why the implementation of risk management is crucial and imperative for the successful realization of the vision that is linked to the digital government of Saudi Arabia. Additionally, as Saudi Arabia continues to make some of the most remarkable strides within the boundaries of its digital transformation journey, the importance of risk management is a situation that cannot be overstated. As a result, by harnessing the power that is linked to risk management, the entire digital government can always foster a more reliable government that balances higher levels of innovation and security thereby ensuring that there is a sustainable and resilient mode of a digital ecosystem that is meant to benefit all the citizens. By managing these risks in an efficient manner, the digital government of Saudi Arabia can be able to optimize all its decision-making processes, allocate different types of resources in an efficient manner and even go as far as balancing innovation with security. Through this, the government can also be able to maintain one of the most robust and sustainable forms of digital infrastructure that fully supports all its goals of offering some of the most efficient digital services that are citizen-centric. Risk management is therefore one of the most critical components of the digital government's strategies. As a result of coming up with more comprehensive and organized risk management practices, the government can be able to proactively address some of the major potential risks, protection of crucial assets, and even ensure that there is a more successful implementation of all its digital transformation initiatives.

Literature Review

The digital government of Saudi Arabia

The digital government of Saudi Arabia clearly represents one of the most significant leaps forward when it comes to the leveraging of technology in order to enhance governance, improve higher levels of service delivery and even foster what is known as citizen engagement. The region has been able to set some of the most ambitious goals geared towards transforming its entire knowledge-based economy and even empowering all its citizens through the use of a wide range of digital solutions. The Saudi Arabia government clearly recognizes some of the major importance of robust digital infrastructure and connectivity as the major pillar for a thriving and advanced digital ecosystem. Moreover, the region has also made quite a number of substantial investments in relation to the expansion of its broadband networks, increasing the rates of internet penetration and even going the extra mile to offer more seamless connectivity to various citizens and businesses known to be situated across different parts of the country. This kind of infrastructure development, therefore, serves as a critical enabler for the successful implementation of advanced forms of digital government services. On the other hand, the digital government of Saudi Arabia has introduced a wide range of different government services aimed at streamlining various administrative processes, enhancing the overall level of efficiency, and even improving issues that are related to service delivery. Moreover, right from online portals for the registration of various businesses and licensing to digital platforms for healthcare, education, and even public services, the entire government has made one of the most significant strides in making sure that the services become more accessible and user-friendly. This mode of digitization of different services has contributed to reduced rates of bureaucratic procedures, and reduced levels of paperwork alongside expedited processes thus contributing to higher levels of citizen satisfaction and increased efficiency levels within the government. According to Nawafleh (2018), the engagement of various citizens majorly lies at the core of the entire digital government of Saudi Arabia. The

government has been able to fully support the implementation of various platforms and channels for the citizens to be able to interact, participate, and even offer their respective feedback on different types of policies and services. Through the implementation of a wide range of online portals, different types of mobile applications together with social media platforms, citizens find it much easier to gain access to information, be able to voice their respective opinions, and even go as far as actively contributing to various forms of decision-making processes. Moreover, this kind of inclusive approach not only strengthens the level of trust that exists between the government and its respective citizens but also empowers a variety of individuals for them to be in a position to actively shape the future of their respective communities.

The Saudi Arabian digital government has also undertaken some of the most significant digital transformation initiatives across different sectors of the country. A good example is in the healthcare sector where the implementation of electronic health records and telemedicine services has ended up improving access to quality healthcare most so in remote areas. Also, within the education sector, different types of digital platforms and e-learning solutions have greatly enhanced a wide range of educational opportunities, reaching a broader audience and even fostering a lifelong learning process. Such types of advancements clearly demonstrate the ability of the government's commitment to adequately utilize different types of technology with the intention of addressing a wide range of societal challenges and even going the extra mile to enhance the overall quality of life for its citizens. 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.

Professionals in the Digital Government of Saudi Arabia

The digital government of Saudi Arabia that is also recognized as the e-government program has been on the verge of actively working towards different aspects of digital transformation and innovation in order to enhance a vast range of government services and scale up the overall experience of different citizens (Batubara Ubacht & Janssen, 2018). Moreover, quite a number of professionals are always involved in different roles across the entire digital government of Saudi Arabia. The following are therefore some of the major professionals who have made it possible for the digital government to explore different goals and objectives in a more efficient manner;

- Chief information officer- The chief information officer is fully responsible for the overall information technology strategy together with implementation that is taking place within the boundaries of the digital government. Moreover, they are always in a position of overseeing quite a number of digital transformation activities and even ensure that there is a perfect alignment with all the government goals and objectives (Aljarallah & Lock, 2020).
- Chief digital officer- The chief digital officer is always in charge of driving a wide range of digital initiatives and strategies across the entire government. As a result, they always put much concentration on leveraging some of the most emerging technologies, fostering higher levels of innovation and even going as far as enhancing the overall level of citizen engagement across different digital platforms.
- Data Analysts- They always play a critical role within the boundaries of the digital government by trying as much as possible to carry out an analysis of a large combination of datasets in order to obtain some of the most reliable insights, identify a variety of different trends and even make proper data-driven decisions (Santa, MacDonald & Ferrer, 2019). Again, they help in the scaling up of different services within the digital government, optimizing the allocation of different resources and even enhancing different types of policy-making processes.
- Cybersecurity experts- in relation to the increased reliance on various digital systems together with some of the major potential risks that are known to be associated with cybersecurity, all those professionals known to be specializing in cybersecurity have always been critical in the digital government of Saudi Arabia. They are always on the verge of working in order to ensure that all government networks are perfectly secured (Verkijika & De Wet, 2018).
- User Experience designers- they are always focused on scaling up the overall level of usability and accessibility of a wide range of digital services that are being offered by the digital government of Saudi Arabia. As a result, they always come up with quite a number of intuitive

interfaces, conduct higher levels of user research and even collaborate with different types of stakeholders to ensure that all the government services are user-friendly to the extent of addressing all the needs of the citizens.

- Software developers-This group of professionals are fully responsible for designing, developing together with maintaining different types of digital platforms and applications that are always used by the government. Again, they also work on building various forms of robust systems, integrating different types of data sources, and also ensuring that there is a smooth functioning of various digital services.

Various risks faced by the digital government in Saudi Arabia

While the digital government brings on board some of the most immense benefits, it is also subjected to quite a number of critical challenges. Moreover, the digital government just like any other form of a digital entity is always subjected to these risks and challenges hence bringing on board some of the most significant implications for various operations known to be taking place within the government boundaries, service delivery alongside the security and privacy of the citizens' data. The following are therefore some of the major risks that are known to be encountered by the digital government;

- Cyber security threats- One of the most significant risks has always been the threat of cyberattacks. As the government heavily depends on a wide range of digital systems and data, it emerges to be a prime target most so to various types of malicious actors who are seeking to disrupt various operations, steal quite a number of sensitive information or even cause some sort of reputational damage. Some of the major cyber security threats include ransomware, hacking attempts alongside a distributed denial of service attack.

- Data breaches and privacy concerns- The digital government handles different amounts of personal and sensitive data that are linked to the citizens, businesses, and even a wide range of government operations. As a result, a breach of this data can bring on board some of the most severe consequences that entail things like identity theft, fraud, or even loss of trust across different government services. Making sure that there is a more robust data protection measures and compliance with a wide range of privacy regulations is more critical most so when it comes to the mitigation of this kind of risk.
- Technological obsolescence- The rapid development of different types of technological advancements is a clear indication that the digital government might encounter challenges when it comes to keeping up with some of the most evolving technologies. Different outdated systems and infrastructures can also become vulnerable to different security breaches to the extent of preventing the delivery of more efficient and effective services.
- Insider threats- The Saudi Arabia digital government must also be very mindful of quite a number of internal threats that are known to be imposed by employees, contractors, or even some of the third-party service providers. Moreover, issues related to insider threats can majorly entail unauthorized access to different systems, data theft, or even sabotage.
- Service disruptions and operational challenges- A full dependence on different digital systems and infrastructure is a situation that makes the digital government to be susceptible to issues associated with service disruptions that are majorly caused by occurrences like power outages, natural disasters, or even technical failures. Such kinds of disruptions can always contribute to the disruption of various services, delays when it comes to the delivery of different services, and also the loss of public trust.
- Regulatory compliance- The digital government of Saudi Arabia is expected to fully adhere to different types of regulatory frameworks together with standards that are majorly concerning

issues related to data protection, privacy, and also cybersecurity. Moreover, failure to fully comply with such types of regulations can contribute to legal and financial consequences to the extent of damaging the overall reputation of the government

- **Social Engineering Attacks-** Different types of social engineering attacks that entail things like impersonation or even manipulation pose some of the most significant risks to the entire digital government. Moreover, these kinds of attacks exploit a wide range of human vulnerabilities for the purpose of gaining unauthorized access to different systems of even sensitive information.
- **Digital Divide and Inclusivity-** The entire digital government must be in a position of addressing some of the major risks that are associated with the creation of a digital divide where certain population segments are always excluded from getting access and benefits from digital services.

In order to ensure that these risks are managed in an effective manner, the entire digital government of Saudi Arabia should be in a position to fully adopt some of the most comprehensive risk management strategies that will play critical roles when it comes to the performance of different tasks.

Risk Management frameworks that are used by the Saudi Arabia Digital Government

The Saudi Arabia digital government clearly has been able to employ a wide range of risk management frameworks in order to adequately identify, assess and even mitigate a wide range of risks. These types of frameworks offer some of the most structured approaches together with guidelines that aim towards managing different risks in a more systematic and proactive way. the following are therefore some of the major risk management frameworks that the government has been able to put into consideration as far as its operations are concerned.

- ISO 31000- This is a critical framework that is globally recognized due to its capability of providing different principles, frameworks, and even process guidelines that are all associated with risk management. Additionally, it majorly emphasizes some of the major holistic and systematic approaches that are linked to risk management thus focusing on the ability to establish the context, identify different risks, and even assess all their respective impacts and likelihood thus going as far as implementing some of the most appropriate risk management measures (Makki & Alqahtani, 2022). Moreover, the digital government of Saudi Arabia normally refers to ISO 31000 as a critical foundation for all its risk management practices.
- COSO Enterprise Risk Management (ERM) Framework- This is also another form of commonly used risk management framework. It offers one of the most comprehensive approaches to issues associated with enterprise risk management majorly including the ability to offer a clear definition to risk appetite, identification of different risks, assessment of their potential impacts, and even design of more organized risk response strategies. Moreover, it is normally adapted to the specific needs and requirements that are in line with Saudi Arabia's digital government (Alzahrani, Al-Karaghoulis & Weerakkody, 2018).
- NIST Cybersecurity Framework- The National Institute of Standards and Technology Framework is majorly focused on the management of different types of cybersecurity risks. Again, it also offers a well-structured approach for different types of organizations to adequately assess and even enhance their respective cyber security postures. The digital government of Saudi Arabia is capable of implementing this type of framework with the intention of identifying and prioritizing a wide range of cyber security risks, implementing various forms of cyber security controls, and even establishing various incident responses alongside recovery capabilities (Dobrolyubova, 2022).

- ITIL (Information Technology Infrastructure Library)- This is a combination of various best practices that are linked to the IT service and management where it is widely used within the digital government of Saudi Arabia. Moreover, while ITIL is not a risk management per se, it entails a wide range of guidelines for managing a variety of different risks that are known to be associated with IT service delivery that entails things like ensuring availability, higher levels of integrity together with the confidentiality of different digital systems and data.
- COBIT (Control Objectives for Information and Related Technologies)- This type of framework is majorly focused on the overall governance and control of IT where it offers some of the most reliable guidelines that are specifically meant for managing different IT risks, aligning IT with a wide range of business objectives and even going as far as ensuring that there is a more effective IT governance. Moreover, the digital government of Saudi Arabia is in a position to fully utilize COBIT in order to adequately access and manage quite a number of IT-related risks that are existing within the context of different types of digital transformation initiatives.

It is therefore essential to note that quite a number of digital government entities existing within the boundaries of Saudi Arabia might also be in a position of developing their personal risk management frameworks that are fully customized, aligning them with all the available international standards and best practices while at the same time considering some of the most unique challenges and different requirements that are associated with the entire context of digital government. As a result of implementing a risk management framework that is well-defined, the digital government of Saudi Arabia has been in a position to effectively evaluate and prioritize quite a number of existing risks, develop some of the most reliable risk response strategies and even carry out the allocation of a wide range of resources. Additionally, these frameworks also facilitate compliance with different types of regulatory requirements and even go as far as helping different types of organizations to create resilience in the face of uncertainty and also under different dynamic situations. The use of risk

management within Saudi Arabia's digital government has been reported to have brought on board some of the most significant changes thereby allowing the government to always be at the forefront of dealing with a lot of digital information in an appropriate manner that is full of a lot of positive results. On the other hand, the government has also made good use of different types of well-trained and experienced individuals who have got a deeper understanding of some of the best ways in which the frameworks can always be implemented just to ensure that the right outcome is attained.

Identification of challenges and barriers to effective risk management in the digital government of Saudi Arabia.

Effective risk management practices within the boundaries of the Saudi Arabian digital government encounter quite a number of challenges and barriers that mainly entail the following;

- Lack of Awareness and Education- There might be a lack of awareness and a proper understanding of some of the major importance associated with risk management across different types of government officials and employees. Moreover, insufficient knowledge regarding cybersecurity practices alongside various risk mitigation strategies can prevent the implementation of more effective risk management efforts (Aljarallah & Lock, 2018).
- Existence of limited resources- quite a number of critical resources including funding, skilled personnel together with advanced levels of infrastructure are very critical when it comes to the implementation of more effective risk management. As a result, the existence of limited resources can end up impeding the overall implementation of robust risk management practices within the boundaries of the digital government.
- Regulatory Compliance- The ability to comply with different regulations and standards associated with data protection and privacy can end up being among the major challenges for digital governments. Again, ensuring that there is an alignment with various types of

international standards such as the General Data Protection Regulation might end up being complex and time-consuming (Alkhwaldi, Kamala & Qahwaji, 2018).

Interagency Coordination-The digital government entails a wide range of multiple agencies together with departments that are always working together to attain common goals and objectives. Moreover, coordinating different types of risk management efforts across different entities can always be challenging as a result of the existence of differences in priorities, and organizational structures alongside various forms of communication gaps (Al Mudawi, Beloff, & White, 2020).

Rapid technological advancements-The fast pace at which different technological advancements are moving is capable of outdoing the ability of the government to adequately manage various associated risks. Keeping up with some of these emerging technologies and identifying some of the major existing potential risks at an early stage is always very demanding.

Resistance to change- Resistance to change and the implementation of new forms of technologies can prevent effective risk management. There are some government employees who might be hesitant when it comes to embracing different forms of digitization thereby contributing towards delays when it comes to the implementation of some of the necessary risk management measures.

Cultural and social factors- A wide range of cultural and social factors can always end up impacting risk management across the entire digital government of Saudi Arabia. Moreover, the existence of different factors like attitudes towards issues related to cyber security, various privacy concerns together with societal norms within the boundaries of information sharing can end up influencing the overall effectiveness of risk management practices.

Vendor management- Being in a position of engaging different types of third-party vendors together with various service providers has always introduced additional risk factors. Again, ensuring that different vendors are able to comply with all the available security requirements to the extent of even

managing their access to a wide range of sensitive government data can always emerge to be quite challenging (Pinto & Allui, 2020).

International collaboration- Collaboration with different types of international entities, sharing of threat intelligence, and addressing some of the major global cybersecurity challenges have always required one of the most effective forms of coordination and cooperation. Moreover, overcoming quite a number of geopolitical barriers and establishing higher trust levels among various nations has always ended up being one of the most significant challenges.

Being able to address these challenges and barriers majorly requires one of the most comprehensive approaches that will further ensure the government is able to effectively deal with quite a number of risks within its digital boundaries and further ensure that a more competitive level of performance and sustainability is embraced at all times.

Methodology

Research design

The research was much focused on the collection of relevant types of data and to ensure that this took place effectively, the research decided to fully concentrate on a qualitative research design that offered one of the best opportunities for the researcher to be able to carry out the exploration of a wide range of insights that were related to the topic of study.

Sample and populating

The research was also keen on embracing the right sampling technique where which entailed the random sampling of different types of research participants. Furthermore, this mode of sampling played a critical role in making sure that every member of the research was subjected to an equal chance of being chosen. Again, a total of 50 participants were also chosen for the research where most of them were in a position of having a clear understanding of the implementation of risk management within the boundaries of Saudi Arabia's digital government and had even worked for the government for a period of more than five years.

Data collection

Some of the major data collection techniques that this research decided to incorporate mainly entail the following;

Survey method- This data collection method offered the researcher an opportunity to collect a wide range of data across different types of research participants. The survey questions were all administered online since it was one of the cheapest and most time-consuming methods that could be used to obtain the right combination of information from all the participants within the shortest time possible.

Controlled observations- Through the implementation of this technique, it helped the research to study and observe how the digital government of Saudi Arabia has been able to respond to risk management practices within its boundaries where the observation was subjected to a controlled environment just to ensure that more accurate and reliable information was collected for a more efficient analysis to be carried out.

Interviews- The interview made good use of a wide range of close-ended questions that were all delivered in the same format to all the research respondents who were incorporated with the research. There were quite a number of reasons why this research had to use interviews as a method of collecting data from its participants. One of the major reasons was that this method offered one of the best information for extra information extraction. Again, it also offered increased knowledge in relation to the study topic.

Data Analysis

The research was also keen on data analysis of the obtained information. Due to this, a qualitative analysis approach was incorporated into this research. It further offered one of the best opportunities for analyzing all the non-numerical data that were collected in the research most so the ones that were obtained from the closed-ended questions that were linked to the interview. This analysis, therefore, created one of the most conducive environments to understand the research in deeper detail based on a wide range of information.

Findings

All the data collection methods that were used in this research made it much easier to come up with a wide range of findings most so from different types of information that were offered by the research participants. Again, the research findings were strictly based on the benefits that are associated with risk management after having been implemented within the boundaries of the Saudi Arabian government. Again, the findings also indicated how critical risk management has been to the digital government of Saudi Arabia. The risk management of experts who were subjected to the research was able to offer a wide range of opinions pertaining to the topic. 25% of the risk management experts who were subjected to the online survey responded that the ability to implement risk management within the digital government of Saudi Arabia has been able to come up with an enhanced level of security. On the other hand, another 25% of these participants were also able to admit the implementation of higher levels of risk management within the organizational boundaries of Saudi Arabia has also propelled an efficient allocation of different types of resources. According to their point of view, the ability to implement risk management has enabled the entire digital government to allocate a good number of its resources in an effective and efficient way. Again, there were different senior government employees within the digital government who also acted as some of the major participants in this research. When they were interviewed about some of the major benefits that are associated with risk management within their digital government, 20% of this population said that it has greatly helped in the enhancement of a variety of continuity services. Through some of the major and critical risk management practices that they have been able to implement, the digital government has found one of the best opportunities to identify a lot of potential disruptions to most of its services to the extent of even developing certain modes of contingency development plans to trigger higher continuity levels. Again, another 20% of this group of participants fully admitted that the use of risk management in the Saudi Arabian digital government has greatly helped in compliance with different types of regulations

hence this has created an opportunity to comply with different laws, regulations, and also industry standards. The final 10% of the participants also pointed out the fact that risk management practices within the digital government have been among the most critical factors that have greatly enhanced strategic decision-making that has been taking place within the internal environment in relation to various perceptions provided by various individuals.

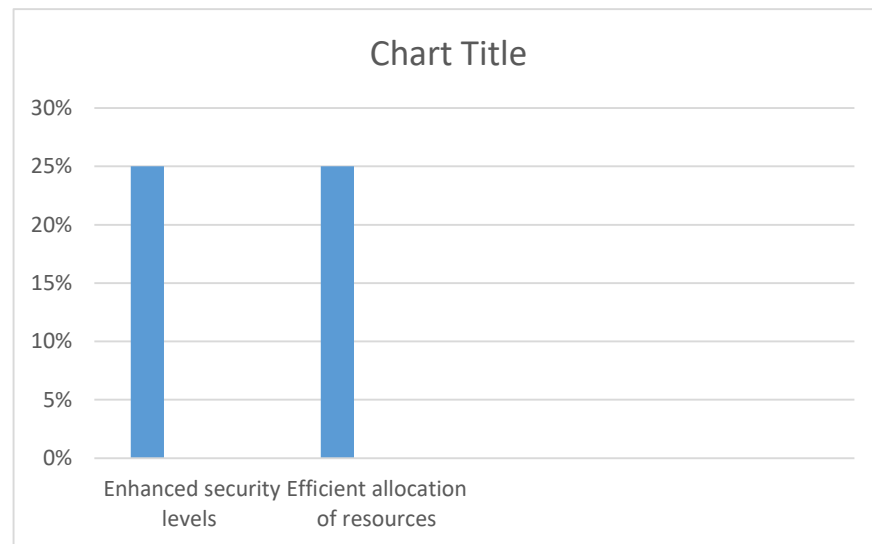


Figure 1: Online survey responses on the benefits of risk management to the digital government of Saudi Arabia

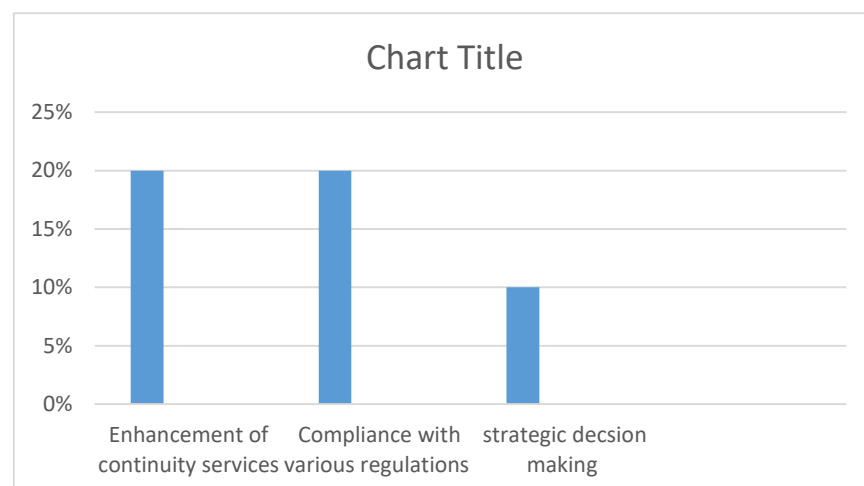


Figure 2: Interview responses on the benefits of risk management to the digital government of Saudi Arabia

Based on the controlled observation methods that were employed by the research, it was observed that making good use of a wide range of risk management strategies in the digital government has helped Saudi Arabia to improve its service quality. As a result of managing different risks through appropriate risk identification and mitigation, the government has found one of the best opportunities to address a lot of vulnerabilities and weaknesses across its systems, processes, and infrastructure. Finally, another observation that was found was that risk management practices have greatly helped the Saudi Arabian government to greatly enhance its reputation across different parts of the world. Through the consideration of a more robust risk management framework, this has been able to fully protect the reputation and brand image of the entire digital government.

Discussions

The implementation of risk management clearly allows the identification, and assessment alongside the mitigation of some of the major potential security risks. As a result, it greatly helps in the safeguarding of sensitive data and critical infrastructure thus offering full protection to all the systems of the digital government right from cyber threats to any modes of unauthorized access. Also, through the implementation of some of the most robust security measures, the digital government of Saudi Arabia has found itself in a situation of building trust among all its citizens to the extent of ensuring confidentiality, integrity levels together with the availability of all its digital services. Again risk management has also enabled the digital government to easily allocate its resources in a more efficient manner. Through the identification and prioritization of various risks, the digital government has been able to channel most of its efforts and resources with the intention of addressing some of the most significant threats. This mode of approach has greatly helped in the optimization of resource allocation thereby scaling down any unnecessary costs and maximizing the whole value that has been derived from various investments in digital technologies and infrastructure. Through a variety of risk management practices, the Saudi Arabian digital government has found it much easier to identify a lot

of potential disruptions to its services and even develop a wide range of contingency plans for the purposes of continuity. By addressing a variety of risks in a proactive manner that entails things like system failure or even natural disasters, the government has been able to adequately minimize the overall impact of issues associated with service delivery and even the maintenance of more seamless operations. This kind of approach is therefore critical when it comes to ensuring uninterrupted access to various digital services most so for its citizens and businesses.

Embracing risk management has helped the digital government of Saudi Arabia to fully ensure that there is compliance with a lot of relevant laws and regulations together with a variety of industry standards. By clearly identifying and mitigating all the available risks that could end up contributing to non-compliance, the government has been able to eradicate some of the legal and financial penalties, reputational damage, and also loss of public trust. Furthermore, the digital government has been able to establish a more robust control and governance framework thereby scaling up higher levels of transparency and accountability when dealing with a lot of digital operations. Effective risk management offers a lot of valuable insights that have greatly helped the digital government to adequately support a lot of strategic decision-making processes. As a result of assessing different risks that are linked to new initiatives, it has been much easier for the government to make a lot of informed choices related to the allocation of different resources, timelines, and also implementation strategies. Again, it has greatly helped in the identification of a lot of potential challenges at an early stage allowing space for proactive mitigation measures to be considered together with a much better decision making.

As a result of adequately managing a variety of existing risks, the entire digital government of Saudi Arabia has been able to enhance the quality levels of all its services. By embracing both risk identification and mitigation, the government has been able to find one of the best opportunities to address a lot of vulnerabilities and weaknesses existing in its systems, and processes together with its infrastructure. As a result, this kind of proactive approach has played one of the most significant roles in

the delivery of reliable, efficient, and user-friendly forms of digital services that have been fairly distributed across all its citizens to the extent of fostering both public satisfaction and trust. Finally, a more robust type of risk management framework within the government has fully protected the reputation and brand image of the whole digital government. As a result of mitigating a variety of risks that are associated with data breaches, failure of various systems, and interruptions of different services, the digital government has been able to highly maintain its public confidence and trust levels within the boundaries of all its digital initiatives. The creation of a positive reputation strengthens the overall position of the government, attracting high levels of investments, fostering reasonable levels of collaboration, and even going further to encourage full participation in different types of digital transformation efforts. Risk management, therefore, plays some of the most critical roles in the digital government of Saudi Arabia. As a result of the implementation of some of the most effective risk management practices, the government has found it much easier to mitigate different types of potential risks in order to attain its digital transformation objectives in a more efficient and effective manner.

Limitations of the Research

The implementation of the research was able to encounter certain limitations that created some barriers in terms of effectively exploring the goals and objectives of the research. The first research limitation that was encountered was time and resource constraints. Since the research was conducted within a specific time frame alongside a limited amount of resources, these constraints ended up impacting both the depth and breadth of the whole research. Since there was a short research duration, this made it very difficult to capture some of the long-term results in relation to the study topic. At the same time, having limited financial resources also restricted the entire scope of data collection and analysis of the research. The second limitation was sample size selection; the existence of a small sample size of the research was able to scale down the generalizability of all the findings.

Ethical considerations

A wide range of ethical considerations were incorporated within this research. Moreover, they were very essential since they ensured that the conducted study was carried out in a manner that was able to uphold, the rights, welfare, and dignity of different types of participants. This also went ahead to promote the overall integrity alongside the credibility of the entire research process. As a result, the following types of ethical considerations had to be implemented;

Informed consent- The researcher was able to obtain voluntary, informed, and well-documented consent from different types of participants before they were able to take part in the study. Again, the participants were fully informed before the entire purpose, and procedures alongside all the risks and benefits that were linked to the research. Again, they were also given an opportunity to opt out of the research at any given time.

Privacy and confidentiality- The research was able to fully protect the privacy and confidentiality of all the involved participants. This procedure entailed different actions like handling a variety of personal data in a more secure way, using different types of anonymous identifiers, and also ensuring that all the participant information was not disclosed without their consent except in specific cases where there was some form of legal or ethical obligations.

The integrity of the research- The research was able to fully adhere to high standards of research integrity that majorly entailed different aspects like honesty, objectivity together with transparency levels. As a result, the researcher was therefore in a position to accurately report different, methods, findings, and conclusions to the extent of even avoiding the fabrication and falsifying of data.

Moreover, the research was also carried out in an unbiased manner.

Respect for the research participants- The research was also able to fully respect the overall dignity, rights, and even autonomy of different participants. This entailed the ability to treat the participants

with fairness to the extent of avoiding any act of discrimination or even exploitation and even went ahead to consider their cultural, religious, and social backgrounds during the designing of the research protocols. The research was also mindful of the power dynamics that were inherent in the research-participant relationship.

Transparency and accountability- The whole research was able to strive for higher levels of transparency in all the involved practices that entailed the disclosure of the funding sources, different types of existing conflicts of interest, and also the limitations in different types of findings. Again, the research was also open to scrutiny to the extent of making the researcher willing to share different types of data, data, and materials with other existing researchers.

Conclusion

The implementation of robust risk management practices within the boundaries of Saudi Arabia's digital government brings the onboard a significant advantage and also contributes to the overall success of all its digital initiatives. Moreover, as a result of prioritizing security, resilience, and even stakeholder trust, the government can be able to fully protect its sensitive data, ensure uninterrupted service delivery and even foster one of the most conducive environments that are capable of supporting digital transformation., moreover, risk management also offers the government to come up with a lot of informed decisions, allocate different resources in an effective manner and even comply with a wide range of different regulations thereby bolstering its credibility levels both at the national and international platform. Through the implementation of more effective risk management, the digital government of Saudi Arabia is also in a position of navigating the ever-evolving digital landscape with higher levels of confidence. By being in a position of proactively identifying and mitigating a wide range of risks, the government clearly demonstrates its level of commitment to safeguarding all the interests and privacy of all its citizens, fostering the overall level of public trust, and also going an extra mile to attract different investments and partnerships. Again, by focusing on risk management as a fundamental aspect that is associated with its risk management, the entire government of Saudi Arabia can be able to find one of the best opportunities to create one of the most robust and resilient digital governments capable of delivering more secure and efficient services that are citizen centric in this digital era. Both stakeholder trust and confidence are very critical for the digital government, and risk management also plays a vital role in clearly establishing and maintaining this level of trust. Moreover, by actively managing a variety of different risks, the entire digital government has been able to clearly demonstrate its commitment to protecting different types of interests of the citizens together with complying with all the relevant regulations and standards. This further fosters trust across different citizens, businesses, and also international partners thereby

encouraging their respective active participation within the digital ecosystem. Additionally, stakeholder collaboration is a situation that is also promoted through a variety of risk management practices, as involving a wide range of stakeholders in the entire risk assessment and mitigation processes create an opportunity for different types of diverse perspectives and knowledge sharing in promoting higher levels of digital security and governance.

References

- 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).
- 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.
- Al Mansoori, K. A., Sarabdeen, J., & Tchantchane, A. L. (2018). Investigating Emirati citizens' adoption of e-government services in Abu Dhabi using a modified UTAUT model. *Information Technology & People*, 31(2), 455-481.
- Alrubaiq, A., & Alharbi, T. (2021). Developing a cybersecurity framework for e-government project in the Kingdom of Saudi Arabia. *Journal of Cybersecurity and Privacy*, 1(2), 302-318.
- Al Mudawi, N., Beloff, N., & White, M. (2020). Issues and challenges: Cloud computing e-government in developing countries. *International Journal of Advanced Computer Science and Applications*, 11(4), 7-11.
- Aljarallah, S., & Lock, R. (2020). An Investigation into Sustainable e-Government in Saudi Arabia. *Electronic Journal of e-Government*, 18(1), pp1-16.
- Alkhwaldi, A. F. A., Kamala, M. A., & Qahwaji, R. S. (2018). Analysis of cloud-based e-government services acceptance in Jordan: challenges and barriers.

- 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.
- Batubara, F. R., Ubacht, J., & Janssen, M. (2018, May). Challenges of blockchain technology adoption for e-government: a systematic literature review. In *Proceedings of the 19th annual international conference on digital government research: governance in the data age* (pp. 1-9).
- Dobrolyubova, E. I. (2022). Evaluating digital government performance using surveys: international literature review and prospects for the future research. *Public Administration Issues*, 5, 152-181.
- Kumar, R., Sachan, A., & Mukherjee, A. (2018). Direct vs indirect e-government adoption: an exploratory study. *Digital policy, regulation and governance*.
- Makki, A. A., & Alqahtani, A. Y. (2022). Modeling the Barriers Surrounding Digital Government Implementation: Revealing Prospect Opportunities in Saudi Arabia. *Sustainability*, 14(23), 15780.
- Nawafleh, S. (2018). Factors affecting the continued use of e-government websites by citizens: An exploratory study in the Jordanian public sector. *Transforming Government: People, Process and Policy*, 12(3/4), 244-264.
- Pinto, L., & Allui, A. (2020). Critical drivers and barriers of corporate social responsibility in Saudi Arabia organizations. *The Journal of Asian Finance, Economics and Business (JAFEB)*, 7(11), 259-268.
- 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.
- 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.

Verkijika, S. F., & De Wet, L. (2018). A usability assessment of e-government websites in Sub-Saharan Africa. *International Journal of Information Management*, 39, 20-29.1

Aljarallah, S., & Lock, R. (2018, October). An empirical study of sustainable e-government characteristics in Saudi Arabia. In *18th European Conference on Digital Government* (pp. 8-15).