BACKUP CONTROL MECHANISM AND ADMINISTRATIVE FINESSE OF PUBLIC SECTOR ORGANIZATIONS IN RIVERS STATE, NIGERIA

BRISTOL Marvellous and PROF. P. N**. NWINYOKPUGI**
Department of Office and Information Management, Faculty of Administration and Management, Rivers State University

ABSTRACT

This study examined the relationship between backup control mechanism and administrative finesse of public sector organizations in Rivers State, Nigeria. The study adopted the correlational research design taken cognizance of cross sectional survey approach. The population of the study comprised of Twenty-Two public sector organization in Rivers State, Nigeria. The study sampling elements comprised of 4 management staff of the 22 organizations resulted to a total of Eighty-Eight sampling elements. Due to the population of the study, the census approach was adopted and the entire population studied. The structured close ended 4 point Likert scale questionnaire was used for collection of the study data, and gathered data were analysed using the Spearman Rank Order Correlation Statistics and presented with the aid of Statistical Package for Social Sciences version 20.0. Findings from analysed data showed strong positive and significant relationship between backup control mechanism and the measures of administrative finesse of seamlessness and information security. Relying on the study findings, we concluded that, there is a strong positive and significant relationship between backup control mechanism and administrative finesse. We therefore, recommended that backup control mechanism be adopted in organizations as it's seen to have a strong positive and significant relationship with the measures of administrative finesse of seamlessness and information security.

Keywords: Backup Control Mechanism, Administrative Finesse, Seamlessness and Information Security

INTRODUCTION

Effective management of public sector organizations relies significantly on the integration of backup control mechanisms and administrative finesse. These two elements are essential for ensuring efficiency, accountability, and the achievement of organizational goals, especially in dynamic and complex environments such as the South-South region of Nigeria. Backup control refers to the implementation of checks and balances, contingency plans, and risk mitigation strategies that safeguard operations against disruptions or inefficiencies (Adewuyi & Oladimeji, 2020). Administrative finesse encompasses the leadership skills, decision-making capabilities, and strategic planning required to steer public institutions toward sustainable development (Eze & Okonkwo, 2021).

In the Rivers State of Nigeria, characterized by significant contributions to the national economy through oil production and a diversity of sociopolitical dynamics, public sector organizations often face unique challenges. These include corruption, bureaucratic inefficiencies, and inadequate resource management (Okeke & Nwankwo, 2019). As such, integrating robust backup control measures and leveraging administrative finesse becomes imperative for fostering transparency, improving service delivery, and addressing systemic issues that hinder organizational performance. This paper examines the relationship between backup control mechanism and administrative finesse in public sector organizations in Rivers State, Nigeria.

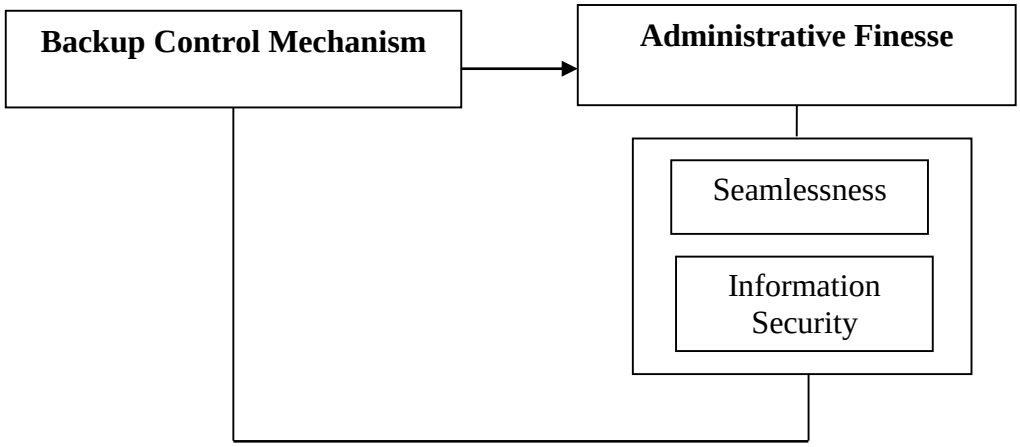

Fig. 1: Conceptual framework for Backup Control Mechanism and Administrative Finesse

THEORETICAL FOUNDATION

Contingency Theory: The contingency theory was propounded by Edward Fred Fiedler in 1960. Contingency theory is an approach to organizational structure and design that emphasizes the idea that there is no single, universally effective way to organize organization. Instead, the most appropriate organizational structure and management practices are contingent upon various internal and external factors unique to each organization. One of the earliest and influential contributions to contingency theory was the work of Burns and Stalker (1961) in their book "The Management of Innovation." They introduced the concepts of "mechanistic" and "organic" organizational structures and argued that the appropriate structure depends on the rate of environmental change. Mechanistic structures, characterized by high levels of formalization, centralization, and specialization, are better suited for stable environments, while organic structures, which are more flexible, decentralized, and adaptive, are more appropriate for dynamic, rapidly changing environments.

The central focus of contingency theory is that organizations must adapt their structures, processes, and behaviours to align with the specific circumstances or contingencies they face. These contingencies can include environmental factors (e.g., market conditions, technological changes, industry dynamics), organizational characteristics (e.g., size, strategy, culture), and task or operational requirements (e.g., complexity, uncertainty, interdependence). According to contingency theory, organizations that achieve a proper fit between their internal design and the external environment are more likely to be effective and perform better than those that do not. Consequently, the theory suggests that there is no single, universally optimal organizational structure or management approach; rather, the most effective structure and practices depend on the specific contingencies (situations) faced by the organization. This submission correlates with the popular adage that no one size fit all. In the era of information as a critical organizational asset, and the consistent attack on organization information infrastructure, the backup control mechanism becomes a strategic approach that management must adopt to survive the wave of information attacked. This become imperative to adopt the contingency theory for this study as it pave way for leaders of the organization to adopt an appropriate management approach based on the situations under investigation as navigate accurately.

LITERATURE REVIEW

Backup Control Mechanism: Backup control refers to the implementation of checks and balances, contingency plans, and risk mitigation strategies that safeguard operations against disruptions or inefficiencies (Adewuyi & Oladimeji, 2020). It plays a crucial role in ensuring the availability and integrity of data within an organization's information technology (IT) infrastructure. It involves the implementation of policies, procedures, and technologies aimed at creating redundant copies of data to protect against data loss or corruption. The importance of backup control in IT cannot be overstated. As organizations increasingly rely on data for their operations, the risk of data loss due to hardware failures, human errors, or malicious attacks becomes more significant (Somasundaram & Shrivastava, 2009). Effective backup control helps organizations mitigate these risks by ensuring that critical data can be recovered in the event of an incident (Senthilkumar & Nedunchezhian, 2019).

Also, one common practice in backup control is the use of the 3-2-1 backup strategy, which recommends having at least three copies of data, stored on two different types of media, with one copy located off-site (Venkatesan & Varadharajan, 2019). This approach helps protect against various scenarios, such as hardware failures, natural disasters, and cyber threats (Soni et al., 2020). Another important aspect of backup control is the selection of appropriate backup types, such as full backups, incremental backups, or differential backups (Rajasekar et al., 2018). Full backups create a complete copy of the data, while incremental and differential backups capture only the changes since the last backup, reducing the storage requirements and backup window (Babu & Ravi, 2019). Furthermore, today, cloud-based backup solutions have gained popularity in recent years, offering scalability, accessibility, and potential cost savings (Gupta & Sinhal, 2020). However, organizations must carefully consider factors such as data security, compliance requirements, and vendor reliability when adopting cloud-based backup solutions (Dutta & Saxena, 2021).

Despite the widespread recognition of the importance of backup control, organizations often face challenges in implementing and maintaining effective backup strategies. These challenges may include limited budget and resources, lack of employee awareness and training, and the complexity of managing backups across diverse IT environments (Senthilkumar & Nedunchezhian, 2019; Venkatesan & Varadharajan, 2019). Hu et al. (2016) define backup control as the set of policies, procedures, and technologies that an organization employs to create and manage redundant copies of data to protect against data loss or corruption. According to Sengupta and Annachhatre (2018), backup control refers to the process of creating and managing duplicate copies of data, configurations, and system information to enable the recovery of information systems in the event of a disruption or failure. Similarly, Venkatesan and Varadharajan (2019) describe backup control as "the systematic process of duplicating data, configurations, and other essential information to facilitate the restoration of systems, applications, and data in the event of a hardware or software failure, human error, or natural disaster." Furthermore, in their book on information storage and management, Somasundaram and Shrivastava (2009) define backup control as "the policies, procedures, and technologies employed by an organization to create and maintain copies of data and system information for the purpose of recovery in the event of data loss or corruption. According to Rajasekar et al. (2018), backup control is the process of creating and maintaining redundant copies of data and system configurations to enable the recovery of information resources in the event of a failure, disaster, or other incident that compromises the integrity or availability of the original data.

Druva (2021) discusses the evolution of backup and recovery solutions, highlighting the shift from traditional on-premises backup systems to modern cloud-based solutions. They

emphasize the importance of addressing data growth, compliance requirements, and the need for seamless data protection across hybrid IT environments. Gartner (2020) recommends organizations adopt a "backup and recovery modernization" approach, which involves leveraging cloud services, automation, and analytics to improve backup efficiency, reduce costs, and enhance data visibility. They also highlight the need for organizations to align their backup strategies with their overall data management and governance frameworks. Veritas (2019) emphasizes the role of backup control in enabling effective disaster recovery and business continuity. They highlight the importance of regular testing and validation of backup processes, as well as the need for robust data protection policies and procedures. Also IBM (2018) discusses the challenges of managing backups in distributed and virtualized environments, highlighting the need for unified backup solutions that can streamline backup operations and reduce complexity. They also emphasize the importance of data deduplication and compression technologies to optimize storage and network usage.

Veeam (2021) focuses on the importance of backup control in the context of ransomware and other cyber threats. They emphasize the need for immutable backups, air-gapped storage, and robust recovery capabilities to ensure data can be restored in the event of a successful attack. Commvault (2020) highlights the challenges of managing backups across multiple cloud platforms and the need for a comprehensive data protection strategy that encompasses both on-premises and cloud environments. They also discuss the importance of data lifecycle management and the role of backup in enabling data archiving and compliance success of organization information.

Administrative Finesse: In the realm of organizational management, the concept of "administrative finesse" has emerged as a critical factor influencing the success and efficiency of administrative processes. Administrative finesse encompasses the skills, qualities, and strategies employed by administrative professionals to navigate the complexities of their roles effectively. Administrative finesse encompasses the leadership skills, decision-making capabilities, and strategic planning required to steer public institutions toward sustainable development (Eze & Okonkwo, 2021). Administrative finesse can be defined as the ability to navigate and manage administrative tasks with dexterity, efficiency, and finesse (Brown & Duguid, 1991). It involves a deep understanding of organizational processes, policies, and procedures, as well as the ability to anticipate and proactively address potential challenges or bottlenecks (Mintzberg, 1975). Individuals with administrative finesse possess a unique combination of technical skills, interpersonal abilities, and strategic thinking. Furthermore, administrative professionals with finesse possess a comprehensive understanding of the organization's goals, strategies, and internal dynamics (Strati, 1999). They can anticipate potential challenges, identify opportunities for improvement, and align administrative tasks with broader organizational objectives (Mintzberg, 1975). This strategic mindset enables them to prioritize effectively, allocate resources efficiently, and contribute to the overall success of the organization. Administrative finesse involves the ability to communicate clearly, concisely, and persuasively with individuals at all levels of the organization (Strati, 1999). Strong interpersonal skills facilitate collaboration, problem-solving, and conflict resolution, enabling administrative professionals to build and maintain positive working relationships (Brown & Duguid, 1991). Administrative finesse requires adaptability and resilience to navigate these demands effectively (Mintzberg, 1975). Individuals with finesse can quickly adjust to changing circumstances, remain composed under pressure, and maintain a solutions-oriented approach to problem-solving (Strati, 1999). This adaptability and resilience contribute to the overall efficiency and effectiveness of administrative processes.

In today's rapidly evolving technological landscape, administrative finesse encompasses the ability to leverage technology effectively and optimize processes (Brown & Duguid, 1991). Administrative professionals with finesse are adept at adopting and utilizing various software, tools, and platforms to streamline administrative tasks, improve productivity, and enhance collaboration (Strati, 1999). They continuously seek opportunities to refine and improve existing processes, ensuring efficiency and alignment with organizational objectives. Administrative finesse is not a static attribute but rather a continuous journey of growth and development. Individuals with finesse recognize the importance of professional development and continuous learning (Brown & Duguid, 1991). They actively seek opportunities to enhance their skills, stay updated with industry trends, and expand their knowledge base (Strati, 1999). This commitment to lifelong learning ensures that administrative professionals maintain their finesse and remain valuable assets to their organizations. It has a profound impact on organizational performance. Individuals with finesse contribute to improved operational efficiency, enhanced communication and collaboration, and increased productivity (Mintzberg, 1975). Their strategic mindset and ability to anticipate and address challenges proactively can lead to cost savings and improved resource allocation (Strati, 1999). Furthermore, administrative professionals with finesse often serve as valuable partners to decision-makers, providing insights and recommendations that support informed decision-making processes (Brown & Duguid, 1991).

Seamlessness: The concept of the seamlessness in the workplace has garnered significant attention in recent years as organizations strive to adapt to the rapidly evolving digital landscape and changing workforce dynamics. This paradigm shift challenges traditional organizational boundaries and hierarchies, fostering a more fluid, collaborative, and technology-enabled work environment. The seamlessness in the workplace is characterized by a blurring of boundaries between physical and virtual spaces, enabling employees to work seamlessly across different locations, devices, and platforms (Millard & Ross, 2006). It represents a shift from the traditional office-centric model to a more flexible and distributed approach to work (Gratton, 2011). According to Khanna and New (2008), the seamless workplace is an environment where people can work together effectively, regardless of their physical location, using whatever tools and processes are most appropriate for the task at hand. Also the emergence of the seamlessness in the workplace is primarily driven by advancements in digital technologies and communication tools. Cloud computing, virtual collaboration platforms, and mobile devices have enabled employees to access information, collaborate, and work remotely with relative ease (Landers, 2015). As Millar et al. (2018) argue, the proliferation of new technologies has enabled the development of new forms of distributed and remote working, allowing for greater flexibility and mobility in where and when work is carried out.

Furthermore, the seamlessness in the workplace is also shaped by changing employee expectations and organizational cultures. Younger generations, such as millennials and Generation Z, have grown up with digital technologies and value flexibility, work-life integration, and collaboration (Gratton, 2011; Meister & Willyerd, 2010). Organizations are responding to these shifting expectations by adopting more flexible and seamless work arrangements to attract and retain top talent (Cisco, 2011). Tools such as video conferencing, instant messaging, and collaborative document editing enable teams to work together seamlessly across geographical boundaries (Landers, 2015; Malhotra et al., 2007). However, as Intindola et al. (2021) highlight, successful virtual collaboration requires developing norms, routines, and technologies that facilitate communication, coordination, and cooperation among distributed teams. Moreover, a seamless workplace often requires a significant cultural shift

within organizations. Leaders play a crucial role in fostering a culture of trust, empowerment, and accountability (Gratton, 2011; Landers, 2015). As Millar et al. (2018) suggest successful implementation of the seamless workplace requires a change in mind-sets and culture, with a focus on outcomes rather than physical presence. The physical workspace is also evolving to support the seamless workplace paradigm. Open floor plans, huddle rooms, and activity-based working arrangements are designed to facilitate collaboration, focused work, and seamless transitions between physical and virtual environments (Gratton, 2011; Waber et al., 2014).

Additionally, the integration of smart technologies, such as sensors and internet of things (IoT) devices, is enabling the creation of intelligent workspaces that adapt to user needs and preferences (Cisco, 2011; Millar et al., 2018). Seamlessness in workplace offers increased flexibility and autonomy; it also presents challenges related to work-life balance and employee well-being. As boundaries between work and personal life blur, employees may experience increased stress, burnout, and difficulty disconnecting from work (Landers, 2015; Millar et al., 2018). Organizations must proactively address these concerns by implementing policies, training, and support systems to foster healthy work-life integration (Gratton, 2011; Intindola et al., 2021). The seamless workplace has implications for talent management and workforce mobility. With the ability to work from anywhere, organizations can access a global talent pool and leverage remote workers or virtual teams (Khanna & New, 2008; Landers, 2015). However, this also requires adapting recruitment, on boarding, and performance management processes to accommodate distributed and mobile workforces (Gratton, 2011; Millar et al., 2018).

Information Security: Information security means protecting information (data) and information systems from unconstitutional access, use, disclosure, disruption, modification, or destruction. Information security defends information (and the facilities and systems that store, use and transmit it) from a wide range of threats, in order to preserve its value to an organization. This definition of information security is adapted from that of the American National Security Telecommunications and Information Systems Security Committee (NSTISSC). There are two important characteristics of information that determine its value to an organization: the scarcity of the information outside the organization; the share ability of the information within the organization, or some part of it. Simplifying somewhat, these characteristics state that information is only valuable if it provides advantage or utility to those who have it, compared with those who don't. Thus the value of any piece of information relates to its levels of share ability and scarcity. The aim of information security is to preserve the value of information by ensuring that these levels are correctly identified and preserved. Threats to information influence the organization's ability to share it within, or to preserve its scarcity outside. And threats that are carried out can cost millions in compensation and reputation, and may even jeopardize an institution's ability to survive. According to Whitman and Mattord (2005) information security is the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information against unauthorised users. Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure.

According to Baskerville and Siponen, (2002) the domain of information security requires a multidisciplinary knowledge of a large amount of information, experience, and skill. In consequence, not having this multidisciplinary knowledge makes the fight of companies against risks, vulnerabilities, and threats more difficult. Also, it should not be forgotten that, with the growing popularity of the Internet and its services, there is an increase in information security threats, such as social engineering, malware, and hacking, of which some users may

not be aware. Additionally, while many different security methods, such as intrusion detection systems and antivirus software, are used to protect IT systems from different attacks, the information security threat landscape continues to rapidly evolve and attackers are putting more effort into developing sophisticated and advanced malware and hacking methods. Therefore, it is evident that there is urgency on the part of companies to take new measures to face the wide variety of forms that cyberattacks are adopting. In another line, there is little evidence that users are aware of the threats and forms of protection that revolve around information security, as well as that they practice mechanisms to deal with this problem. In addition, there is evidence that users have difficulty understanding information security threats, as well as not knowing what to use and how to react to them.

METHODOLOGY

This study adopted the correlational research approach, taken cognizance of cross sectional survey. The population of the study consists of 22 public sector organizations in Rivers State, Nigeria. Owing to the size of the study population, the entire population was sampled using the census approach. However, sampling elements from the study population comprised of 88 management staff of the 22 public organizations in Rivers State, Nigeria based on 4 representatives of the 22 organizations. The primary data source was adopted through the use of structured closed ended questionnaire with collected data analysed with descriptive and inferential statistics. The descriptive was used to analyse the biodata of the study respondents, why the inferential statistic used for the study hypotheses. The study hypotheses tested using Spearman Rank Order Correlation statistics and presented with the aid of the Statistical Package for Social Science (SPSS) version 20.0. Below is the Spearman Rank Order Correlation formula.

$$r_s = 1 - \frac{6\sum d_1^2}{n(n^2-1)}$$

Table 1. Age of Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	30 – 35years	15	21.4	21.4	21.4
	35 – 40years	23	32.9	32.9	54.3
	40 – 45years	25	35.7	35.7	90.0
	50years and Above	7	10.0	10.0	100.0
	Total	70	100.0	100.0	

Source: SPSS Output, Version 20.0 2024

Table 1. showed the response rate for respondents' age distribution and the corresponding pie-chart in the study base on the total numbers of retrieve questionnaires. Out of the 70(100%) used for analysis, age 30-35years in term of frequency, account for 15(21.4%), 33-40years, account for 23(32.9%), 40-45years, account for 25(35.7%) and 50years and above account for 7(10.0%). It showed that majority of the workers are between 33-40years and 40-45years. This showed that the respondents' have the requisite knowledge about the organization to provide answer to the research questionnaire.

Table 2: Gender of Respondents'

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	43	61.4	61.4	61.4
	Female	27	38.6	38.6	100.0
	Total	70	100.0	100.0	

Source: SPSS Output, Version 20.0 2024

Table 2 showed the response rate for respondents gender distribution and the corresponding pie-chart base on the total numbers of retrieve questionnaires. Out of the 70(100%) used for analysis, 43 respondents are male, representing 61.4% of the respondents and 27 respondents are female, representing 38.6%. It showed that majority of the respondents in the study are male.

Table 3: Educational Qualification of Respondents'

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	B.sc	41	58.6	58.6	58.6
	M.sc	14	20.0	20.0	78.6
	HND	15	21.4	21.4	100.0
	Total	70	100.0	100.0	

Source: SPSS Output, Version 20.0 2024

Table 3 showed the respondents educational background and the corresponding pie-chart in figure 3.1. It indicates that out of the 70(100%) copies of questionnaire retrieved for analysis, 41(58.6%) of the respondents are bachelor degree, 14(20.0%) of the respondents are master degree holders, and finally, 15(21.4%) of the respondents are HND degree holders. It observed that majority of the respondents has bachelor degrees; this was observed that all respondents in the filled questionnaire are educated. This showed that majority of the respondents had the expected knowledge to answer the research questionnaire.

Table 4: Marital Status

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Married	56	80.0	80.0	80.0
	Single	9	12.9	12.9	92.9
	Divorced	5	7.1	7.1	100.0
	Total	70	100.0	100.0	

Source: SPSS Output, Version 20.0 2024

Table 4 showed the respondents marital status and the corresponding pie-chart in figure 4.4. It indicates that out of the 70(100%) copies of questionnaire retrieved for analysis, 56(80.0%) of the respondents are married, 9(12.9%) of the respondents are single, and finally, 5(7.1%) of the respondents are divorced. It observed that majority of the respondents are married respondents'. This showed that majority of the respondents had the expected knowledge to answer the research questionnaire.

Table 5: Position of Respondents' in Organization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Director ITC	20	28.6	28.6	28.6
	Director Administration	27	38.6	38.6	67.1
	Director Finance	12	17.1	17.1	84.3
	Director Procurement	11	15.7	15.7	100.0
	Total	70	100.0	100.0	

Source: SPSS Output, Version 20.0 2024

Table 5 showed the respondents position in the organization and the corresponding pie-chart in figure 4.5. It indicates that out of the 70(100%) copies of questionnaire retrieved for analysis, 20(28.6%) of the respondents are ICT directors, 27(38.6%) of the respondents are administrators, 12(17.1%) of the respondents are director finance and finally, 11(15.7%) are directors of procurements. It observed that majority of the respondents are senior management staff of the respective organizations. This showed that majority of the respondents had the expected knowledge to provide answer to the research questionnaire.

Backup Control Mechanism

Table 6: Descriptive Statistics For Backup Control Mechanism

	N	Mean	Std. Deviation
Backup control plays a crucial role in ensuring the availability and integrity of data within an organization's information technology (IT) infrastructure.	70	3.54	.846
As organizations increasingly rely on data for their operations, the risk of data loss due to hardware failures, human errors, or malicious attacks becomes more significant.	70	3.76	.550
Backup control approach helps protect against various scenarios, such as hardware failures, natural disasters, and cyber threats.	70	3.31	1.029
Effective backup control enhances business continuity.	70	3.60	.824
Valid N (listwise)	70		

Source: SPSS Field Result, Version 20.0 2024

Table 6 above showed the response rate for backup control mechanism using mean and standard deviation and measured with 4-items. The first research item with a high mean value of (x=3.54 and std.dev. =0.846). The second research item with a high mean value of (x= 3.76 and Std.dev. =0.550). Third research item with a moderate mean value of (x=3.31 and Std.dev. =1.029). Fourth research item with high mean value of (x=3.60 and Std.dev. =0.824). The majority of the responses showed that there is a high rate of backup control and observed as a strong phenomenon to the study of information architecture in the public sector organization in Rivers State, Nigeria.

Seamlessness

Table 7: Descriptive Statistics For Seamlessness

	N	Mean	Std. Deviation
The adoption of information technology in organization enhances seamless workplace.	70	3.61	.839
The ability of organization employee to work from home reduces organizational expenses.	70	3.86	.460
Workplace collaborations are easily done in a seamless work environment.	70	3.64	.762
Physical location is not a barrier to effective organizational performance.	70	3.54	.928
Valid N (listwise)	70		

Source: SPSS Output 2024 version 20.0

Table 7 above showed the response rate for seamlessness using mean and standard deviation and measured with 4-items. The first research item with a high mean value of (x=3.61 and std.dev. =0.839). The second research item with a high mean value of (x= 3.86 and Std.dev. =0.460). Third research item with a high mean value of (x=3.64 and Std.dev. =0. 762). Fourth research item with high mean value of (x=3.54 and Std.dev. =.928). The majority of the responses showed that there is a high rate of seamless workplace and observed as a strong

phenomenon to the study of administrative finesse in public sector organization in Rivers State, Nigeria.

Information Security

Table 8: Descriptive Statistics For Information Security

	N	Mean	Std. Deviation
Backup control is a measure for effective organization information security.	70	3.64	.799
Organization that fail to provide backup control plan, fail to secure its information environment.	70	3.37	1.038
Disaster control is a good plan to mitigate security threat of organizational information life.	70	3.44	.973
Human and technological aspects play a central integrating role in the security of organization important asset.	70	3.73	.700
Valid N (listwise)	70		

Source: SPSS Output 2024 version 20.0

Table 8 above showed the response rate for information security using mean and standard deviation and measured with 4-items. The first research item with a high mean value of (x=3.64 and std.dev. =0.799). The second research item with a moderate mean value of (x= 3.37 and Std.dev. =1.038). Third research item with a moderate mean value of (x=3.44 and Std.dev. =0. 973). Fourth research item with high mean value of (x=3.73 and Std.dev. =0.700). The majority of the responses showed that there is a high rate of information security and observed as a strong phenomenon to the study of administrative finesse in public sector organization in Rivers State, Nigeria.

HYPOTHESES TESTING

Table 9: Correlations Matrix For Backup Control Mechanism

			Backup Control Mechanism	Seamlessness	Information Security
Spearman's rho	Backup Control Mechanism	Correlation Coefficient	1.000	.854**	.943**
		Sig. (2-tailed)	.	.000	.000
		N	70	70	70
	Seamlessness	Correlation Coefficient	.854**	1.000	.879**
		Sig. (2-tailed)	.000	.	.000
		N	70	70	70
	Information Security	Correlation Coefficient	.943**	.879**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	70	70	70

**. Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS Version 20.0 Result, 2024

Research Question 1: How does backup control mechanism relate with administrative finesse of public sector organizations in Rivers State, Nigeria?

The results presented in table 9 where (*rho*) = .854**, indicates that there is strong positive relationship between backup control mechanism and seamlessness. Thus, backup control mechanism has a very strong positive relationship with seamlessness in the workplace. That is to say, the more the backup control mechanism is applied the more the seamlessness in the workplace becomes sustainable in the public sector organization in Rivers State, Nigeria.
The results presented in table 9 where (*rho*) = .943**, indicates that there is strong relationship between backup control mechanism and information security. Thus, backup control mechanism has a very strong positive relationship with information security. That is to say, the more the backup control mechanism is applied the more the information security of the organization becomes sustainable.
The result for the test of hypotheses on the relationship between backup control mechanism and the measures of administrative finesse is stated as follows:

Hypothesis 1: There is no significant relationship between backup control mechanism and seamlessness of public sector organizations in Nigeria. The results with (*rho* = 0.854; and *P*-v=0.000<0.05%) level of significance indicates that backup control mechanism has a very strong positive and significant relationship with seamlessness in the workplace in the public sector organizations in Rivers State, Nigeria. Therefore, on the basis of the findings the null hypothesis is rejected. Thus, the alternate upheld, hence, there is a strong positive significance relationship between backup control mechanism and seamlessness in public organizations in Rivers State, Nigeria.

Hypothesis 2: There is no significant relationship between backup control mechanism and information security of public sector organization in Rivers State, Nigeria. The results with (*rho* = 0.943; and *P*-v=0.000<0.05%) level of significance indicates that backup control mechanism has a very strong positive and significant relationship with information security of public sector organizations in Rivers State, Nigeria. Therefore, on the basis of the findings the null hypothesis is rejected. Thus, alternate upheld, hence, there is a strong positive significance relationship between backup control mechanism and information security of public organizations in Rivers State, Nigeria.

DISCUSSION OF FINDINGS

The findings showed that there is a strong positive and significant relationship in both instances. The result showed that backup control mechanism has a very strong positive and significant relationship with seamlessness in the workplace. The result showed that backup control mechanism has a very strong positive and significant relationship with information security. The result is in agreement with Lam (2019) examines the impact of regulatory frameworks and compliance requirements on backup control strategies in public sector organizations. The author notes that public sector organizations must ensure that their backup control practices align with relevant regulations and industry standards, such as data protection laws and cybersecurity guidelines. Also, Alhawari et al. (2012) investigate the impact of employee training and awareness on backup control practices in public sector organizations. The authors argue that "organizations must invest in developing a culture of data protection and backup awareness among their employees, as well as providing adequate training and resources to support backup control efforts. Similarly, Shivraj and Venkateshan (2020) explore the impact of leadership styles on backup control outcomes in public sector organizations, highlighting the importance of effective communication, collaboration, and adaptability. The authors suggest that transformational leadership approaches are particularly well-suited for

backup control initiatives, as they emphasize inspiration, motivation, and a shared vision among team members.

CONCLUSION

The findings of this study has proved that backup control mechanism within the public sector organizations in Rivers State, Nigeria, established a positive correlation with administrative finesse measures of seamlessness and information security in public sector organizations. Moreover, effective adoption of backup control mechanism in the protection of information in organizations enhances administrative finesse by achieving seamlessness in the workplace and information security. Therefore, the study concluded that, there is a strong positive and significant relationship between backup control mechanism and seamlessness and information security, the measures of administrative finesse in public sector organizations in Rivers State, Nigeria.

RECOMMENDATIONS

Based on the findings of this study, the following recommendations are made:

i. Government should increase their information backup control mechanism as it is seen to have significant relationship with seamlessness in the workplace.
ii. Government agencies and other organizations leadership should prioritize backup control mechanism as it enhances effective organization information security.

REFERENCES

Adewuyi, T. O., & Oladimeji, A. A. (2020). The role of internal control systems in public sector organizations: A case study approach. *Journal of Management Studies*, *15*(4), 45-59.

Baskerville, R. and Siponen, M. (2002). An information security meta-policy for emergent organizations, *logistics information management, 15*(5/6), 337- 346.

Cisco. (2011). *The seamless workplace: Future of work.* Cisco Internet Business Solutions Group.

Commvault. (2020). The challenges of backup and recovery in a multi-cloud world. *https://www.commvault.com/resources/the-challenges-of-backup-and-recovery-in-a-multi-cloud-world*

Druva. (2021). The state of ransomware, data resiliency and backup modernization. *https://www.druva.com/resources/reports/the-state-of-ransomware-data-resiliency-and-backup-modernization/*

Dutta, A., & Saxena, V. (2021). Cloud backup: A review on techniques, security issues, and future directions. *International Journal of Information Technology, 13*(1), 313-323.

Eze, C. U., & Okonkwo, O. I. (2021). Administrative competence and public sector performance in Nigeria: Lessons from sub-national administrations. *African Journal of Public Administration, 17*(3), 112-129.

Gratton, L. (2011). *The shift: The future of work is already here.* Harper Collins.

Gartner. (2020). Backup and recovery modernization is the next frontier for data protection. *https://www.gartner.com/en/documents/3989877/backup-and-recovery-modernization-is-the-next-frontier-f*

Gupta, R., & Sinhal, A. (2020). Backup and disaster recovery: Cloud integrated solution. *International Journal of Advanced Science and Technology, 29*(5), 1373-1384.

Hu, V. C., Ferraiolo, D. F., & Kuhn, D. R. (2016). *Assessment of access control systems.* National Institute of Standards and Technology.

Intindola, M. L., Jacobsberg, L. B., & Mathwick, C. (2021). Virtuality in the workplace: A systematic literature review. *International Journal of Management Reviews, 23*(3), 325-348.

IBM. (2018). Unified data protection for virtual environments. *https://www.ibm.com/downloads/cas/ZYLJ7YOX*

Khanna, P., & New, J. (2008). *Removing the boundaries: The seamless workplace*. Cisco Internet Business Solutions Group.

Landers, R. N. (2015). Computing intra-individual processes: Introduction to the special issue, *Journal of Management, 41*(4), 855-857.

Mintzberg, H. (1975). The manager's job: Folklore and fact. *Harvard business review, 53*(4), 45 – 59.

Millard, D., & Ross, M. (2006). Web 2.0: Hypertext by any other name? *In Proceedings of the Seventeenth Conference on Hypertext and Hypermedia (27-30). ACM.*

Meister, J. C., & Willyerd, K. (2010). *The 2020 workplace: How innovative companies attract, develop, and keep tomorrow's employees today.* HarperCollins.

Malhotra, A., Majchrzak, A., & Rosen, B. (2007). Leading virtual teams. *Academy of Management Perspectives, 21*(1), 60-70.

Okeke, J. N., & Nwankwo, I. C. (2019). Challenges of governance in the Niger Delta: Implications for development planning. *International Journal of Development and Policy Studies, 11*(2), 84-97.

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2018). *Research methodology*. arXiv preprint arXiv:1803.08407.

Somasundaram, G., & Shrivastava, A. (2009). *Information storage and management: Storing, managing, and protecting digital information.* John Wiley & Sons.

Strati, A. (1999). Putting people in the picture: Art and aesthetics in photography and in understanding organizational life. *Organization Studies, 20*(7), 53-69.

Senthilkumar, G., & Nedunchezhian, R. (2019). A study on backup and recovery systems in cloud computing environment. *International Journal of Advanced Science and Technology, 28*(16), 1257-1264.

Soni, D., Makwana, A., Barot, A., & Saravaiya, J. (2020). Review on backup strategies in cloud computing. *International Journal of Engineering Research and Applications, 10*(3), 26-34.

Sengupta, S., & Annachhatre, C. (2018). *Backup and recovery: Concepts, strategies and techniques.* CRC Press.

Venkatesan, S., & Varadharajan, V. (2019). Backup and disaster recovery for cloud computing resources. *International Journal of Intelligent Engineering and Systems, 12*(2), 124-132.

Veritas. (2019). The role of backup and recovery in business continuity and resiliency. *https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_SP_Backup-Recovery-Role-in-Business-Continuity-V0834-1.pdf*

Veeam. (2021). Ransomware protection: Immutable backups and recovery. *https://www.veeam.com/blog/ransomware-protection-immutable-backups-recovery.html*

Waber, B., Magnolfi, J., & Lindsay, G. (2014). Workspaces that move people. *Harvard Business Review, 92*(10), 68-77.