National College of Ireland

Student Name: OLIVER ANI

Student ID: x22178643@student.ncirl.ie

Programme: MSCCYBE **Year:** JANO23_O

Module: Masters Project (MSCCYBE_JANO23_O)

Supervisor: Michael Pantridge

Submission Due Date: 12/08/2024

Project Title Multi-Cloud: Assessing Resilience Amid Threats

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Oliver Ani

Date: 10/08/2024

Multi-Cloud: Assessing Resilience Amid Threats

Abstract

Resilience has become a priority for organisations seeking to navigate an increasingly complex and unpredictable digital landscape. This thesis investigates the impact of multi-cloud strategies on enterprise resilience by examining factors such as the number of cloud providers, percentage of services distributed, annual IT budget, downtime, incident response time, and redundancy measures. Through a comprehensive literature review and a data-driven approach, this research explores how these variables contribute to the resilience of organisations' IT infrastructure in the face of disruptions. A multiple linear regression analysis was conducted using data from 1000 enterprises, revealing significant relationships between the independent variables and organisational resilience.

While also incorporating comparative analysis, the study further proposes a framework for increasing enterprise resilience based on the empirical results. This framework emphasises the need for risk management strategies informed by quantifiable data, tailored allocation of resources, effective governance across multiple clouds, and the implementation of redundancy measures to mitigate risks. By providing quantifiable metrics and insights, this research aims to assist organisations in making informed decisions about multi-cloud adoption, to enhance the resilience of their deployments to withstand and recover from disruptions.

Keywords: Multi-cloud, Resilience, CSPs, Risk Management, Governance, Metrics, APIs, Disaster Recovery, IaCs

Contents

1.0 Introduction

The multi-cloud computing model, which integrates resources from multiple cloud service providers (CSPs) like AWS, Google, Microsoft Azure, Oracle, Digital Ocean and many more, has gained traction among organisations due to its potential for scalability, flexibility and redundancy. The use of multi-cloud strategies is growing in bounds, with more than 50% of public cloud users now engaging the services of two or more providers[1]. This shift highlights the increasing awareness of the benefits that diversified cloud strategies offer, particularly in terms of enhanced security and flexibility. Valued at USD 8.03 billion in 2022, the multi-cloud management global market share is estimated to rise at a compound annual growth rate of 28.0% by 2030 (Grand View Research, 2023)[2]. This surge is partly driven by the necessity to avoid vendor lock-in, boost agility and ensure compliance with diverse regional regulatory requirements. However, security and interoperability issues inherent in multi-cloud environments pose significant challenges towards organisational resilience - the ability of organisations to minimise downtime in the face of unexpected incidents.

This study investigates the existing research in the field of multi-cloud to assess how these environments can enhance or undermine resilience within organisations. By examining various frameworks, provisioning methods, and interoperability solutions, this review aims to identify the gaps in current research and explore a data driven approach to how effectively managed multi-cloud environments can contribute to the resilience of organisations in the face of service and operational disruptions.

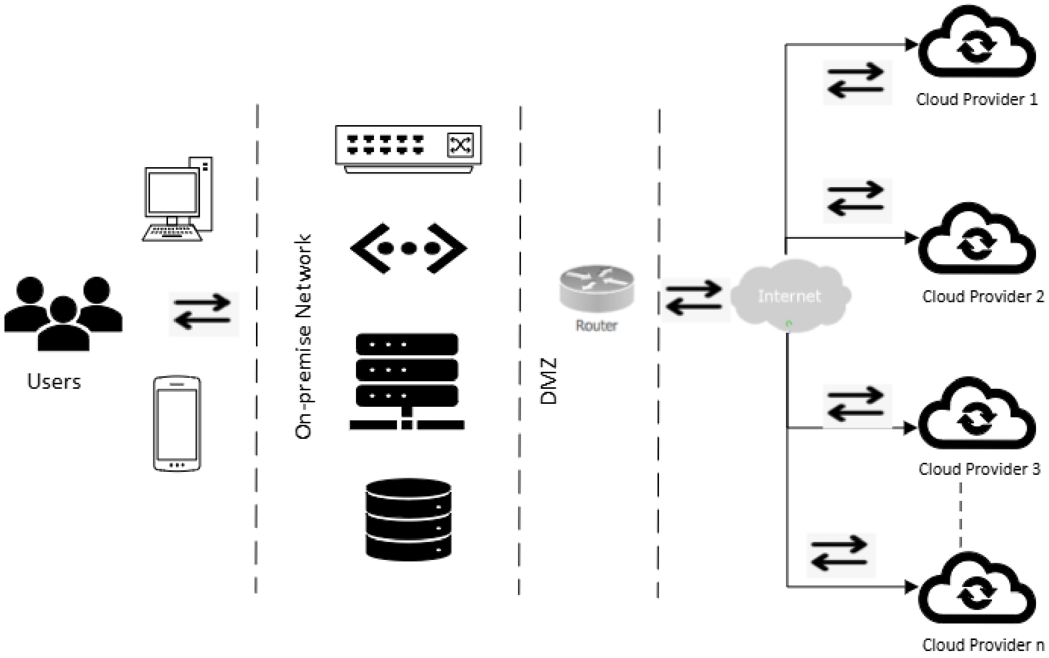


Figure 1 - Typical Multi-Cloud Architecture

1.1. Justification of the Research Topic

The transition to multi-cloud strategies is a significant advancement in IT resource deployment, driven by the need for greater scalability, flexibility, and redundancy. Given the complexities of setting up such deployments, this shift requires thorough investigation into how such environments impact organisational resilience and security. As cyber-attacks become common and severe, understanding the durability of multi-cloud configurations is crucial for protecting critical organisational assets. According to "The State of Multi-Cloud" (Custer, 2024), utilising multiple cloud providers can enhance high availability, disaster recovery efforts, and also brings about substantial challenges in managing security across various platforms. This highlights the necessity of evaluating how multi-cloud environments influence organisational resilience, either for or against it.

1.2. Research Question

How do multi-cloud strategies impact organisational resilience?

1.3. Research Question Potential Benefits

Exploring the impact of multi-cloud environments on organisational resilience and security provides several advantages. This research can shed light on how distributed cloud resources influence an organisation's capability to withstand and respond to cyber incidents. Adopting a multi-cloud architecture allows businesses to select the most suitable services for their specific workload requirements in terms of performance, security, and cost-effectiveness. Additionally, multi-cloud setups can significantly bolster disaster recovery (DR) capabilities and business continuity plans (BCPs). By distributing backups across multiple clouds in different geographical locations, organisations can achieve faster recovery times and minimise data loss during disasters. This geographic and vendor diversification mitigates risks related to natural disasters, ransomware, regional power outages, DDoS or other targeted attacks on a single cloud service provider.

Furthermore, this research intends to contribute to the development of frameworks that can guide organisations on effective allocations of resources in achieving resilience. In summary, while multi-cloud environments represent a crucial advancement in digital transformation, their impact on organisational resilience and security amidst emerging cyber threats needs comprehensive understanding and management. This research underscores the importance of exploring multi-cloud environments with a focus on sustaining and improving organisational resilience.

2.0 Literature Review

Binu C T. and Dr. S. Mohan Kumar (2023) identify a range of prevalent security issues in multi-cloud environments, including cloud service abuse, broken authentication, data breaches, API hacking, system vulnerabilities, DoS attacks, account hijacking, and others [3]. These threats expose critical areas that could negatively impact an organisation's resilience if not properly managed. The authors emphasise the importance of advanced security measures like multi-factor authentication and DNS authentication to address these risks. However, they note the lack of unified frameworks, as CSPs are more in competition than collaboration, to assess the overall impact of these security issues on organisational resilience, suggesting a gap in current research.

Building on this, Singhal et al. (2013) explores the implications of increased attack surfaces in multi-cloud environments, highlighting the complexities of managing security across multiple providers. Their study introduces a proxy-based multi-cloud computing framework designed to facilitate dynamic, on-the-fly collaborations without predefined agreements. They make a strong case for the adoption of the services cloud service brokers (CSBs) to ease the complexities of leveraging multi-cloud architectures. This framework primarily addresses trust, policy heterogeneity, data privacy issues and enabling seamless collaboration while maintaining security [4]. However, the focus is on improving collaborative efforts rather than directly assessing the resilience of organisations employing multi-cloud models, indicating another gap that the research question - “How do multi-cloud strategies impact organisational resilience” - aims to address.

Muralidhar and Aruna (2014) propose another proxy-based framework that emphasises dynamic resource sharing and enhanced security in multi-cloud environments. Their framework suggests that dynamic management and utilisation of multiple cloud services can enhance resilience by ensuring continuous operations across various platforms [5]. However, they acknowledge persistent security challenges, such as identity management and data protection, which could negatively impact organisational resilience. While they offer solutions for these issues, their study does not thoroughly investigate the overall impact on resilience.

The current literature on multi-cloud environments highlights its dual-edged impact on organisational resilience. Reece et al. (2023) indicate that multi-cloud adoption is instrumental in enhancing reliability and availability, resulting in increased resilience against downtime and failures by leveraging the strengths of various cloud providers [6]. This strategy provides advantages such as the avoidance of vendor lock-in, optimization of service selection, and workload distribution across diverse providers [6]. On the contrary, the fragmented security capabilities across different cloud platforms lead to increased complexities in integration and management [6]. This fragmentation can introduce susceptibility to breaking points, new attack vectors and vulnerabilities, substantially undermining security and resilience. Additionally, the utilisation of multiple providers necessitates comprehensive security measures and complex risk management frameworks as reviewed by Torkura et al., (2021). The literature explains that a holistic vulnerability assessment and mitigation strategy, incorporating risk frameworks like DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) is essential for effectively addressing these security challenges and ensuring sustained resilience in multi-cloud deployments [6] [7] . Overall, while multi-cloud environments offer substantial benefits in terms of organisational resilience, managing the inherent risks across multiple CSPs can be daunting.

In the aim to close the fragmentation gap amongst CSPs, Shukla and Patil (2023) review frameworks aimed at achieving interoperability in multi-cloud environments. They advocate for a cloud-agnostic API layer for application portability, a Federated Identity and Access Management system to streamline identity management and enhance security across multiple clouds [8]. This framework facilitates efficient resource utilisation and better security management, which are essential for maintaining operational continuity and resilience. In addition, they propose a cloud-ontology-driven semantic engine as a key component of the Multi-Cloud Interoperability Framework (MCIF) to facilitate collaboration across platforms. They argue that a standard cloud-ontology remains a prerequisite to achieving interoperability in the cloud. However, further research is needed to quantify the resilience benefits of these interoperability measures.

Adding a current perspective, “The Flexera 2024 State of the Cloud Report” indicates that managing security concerns and optimising costs are top priorities for organisations utilising multi-cloud environments [9]. The report also suggests that handling growing cloud expenditure has become a more pressing challenge than security, highlighting the importance of robust multi-cloud strategies to increase resilience and minimise downtime. In other words, the report makes a strong case for resilience - the ability of cloud infrastructures to remain operational in the face of security challenges. However, there is limited empirical research directly linking these practices to enhanced organisational resilience.

2.1. Implications for Organisational Resilience

Addressing the research question - “How do multi-cloud environments impact organisational resilience?” - requires a comprehensive understanding of the variables that enterprises consider when designing their production environment. These variables affect an organisation’s ability to recover from disruptions by introducing various vulnerabilities, such as compromised credentials, API breaches, and data loss. However, implementing robust measures and using advanced frameworks can significantly enhance resilience by ensuring that services remain available and data stays secure even during attacks or failures.

2.2. Research Gaps Identified:

While the reviewed papers generally provide foundational solutions into strategies to enhance the agility of multi-cloud architectures, a deeper analysis on the impact of multi-cloud on organisational resilience presents itself. Below are the notable research gaps identified:

Empirical data insight: The need for a data-driven approach towards making informed decisions on the optimum number of CPSs to leverage, and therefore, enhance enterprise resilience is vital. Organisations can draw insight from such an approach to optimise their workloads, reduce cost and improve the resilience of their multi-cloud infrastructure.

Comprehensive Risk Management Strategies: Organisational resilience requires a comprehensive risk management approach. This strategy should be informed and guided by quantifiable data.

Interoperability and Governance: Managing security policies, access controls, and compliance across different cloud service providers is a significant challenge. Implementing a cross-platform security governance among multiple clouds demands solutions that extend beyond fragmented approaches and requires unified governance.

2.3 How the Research Question Aims to Address These Gaps:

The research question, "How do multi-cloud environments impact organisational resilience” seeks to build on previous works done by the reviewed papers to achieve the following results:

Data-driven approach to enhancing resilience: The research aims at providing quantifiable metrics to aid organisations in making their decision on embracing multi-cloud or otherwise for the workloads.

Risk Assessment and Management: Aid the risk assessment team by reducing the amount of guesswork. In other words, use insights from the analysis to create risk mitigation strategies.

Governance and Compliance Across Clouds: Results from the linear regression analysis can provide valuable insights into the key factors significantly influencing enterprise resilience. Organisations can prioritise their investments to align with key predictors that enhance resilience. These findings can inform the development of a governance and compliance framework by setting benchmarks for acceptable metrics.

In summary, this investigation aims to address the challenges identified in the existing literature and pave the way for a future where multi-cloud environments become integral to enhancing organisational resilience. By leveraging measured and quantifiable metrics, the research seeks to provide a framework for improving resilience in a calculated approach. This includes establishing benchmarks for critical factors, promoting best practices for risk management, and ensuring that organisations can effectively adapt to evolving threats.

3.0 Methodologies and Specification

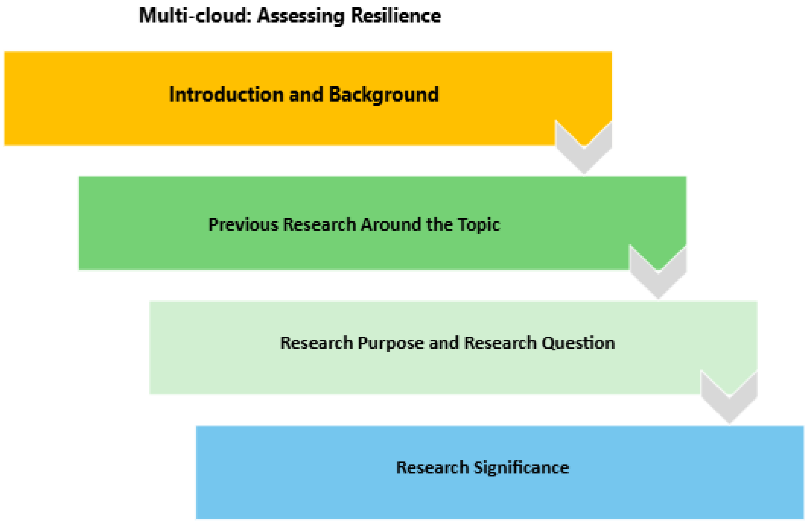

Multi-cloud: Assessing Resilience
Introduction and Background
Previous Research Around the Topic
Research Purpose and Research Question
Research Significance

Figure 3.0 - Thesis Approach

The research methodology consists of comparative analysis, data collection, data transformation, data modelling, result analysis and proposals.

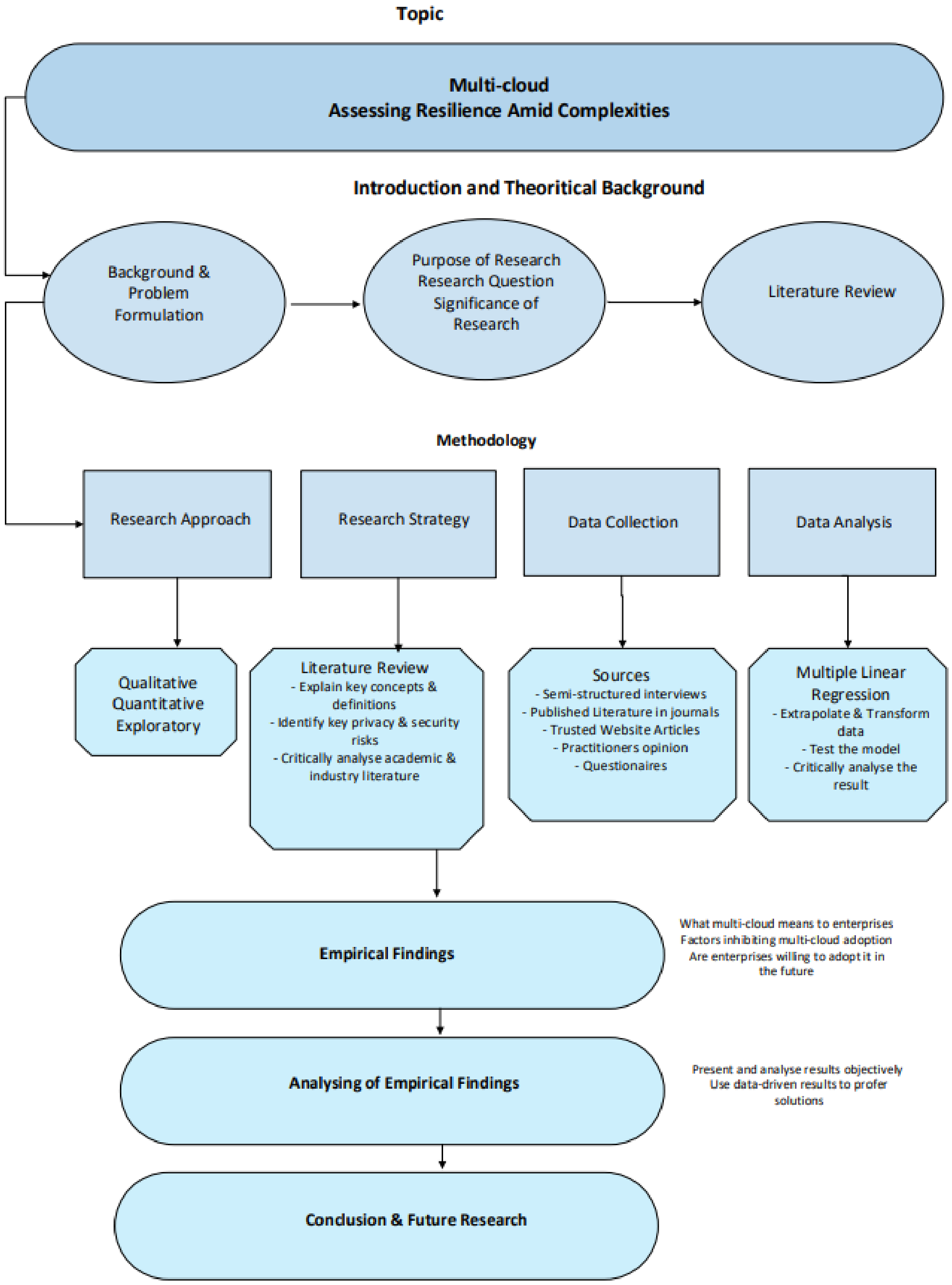

Topic
Multi-cloud
Assessing Resilience Amid Complexities
Introduction and Theoritical Background
Background & Problem Formulation
Purpose of Research
Research Question
Significance of Research
Literature Review
Methodology
Research Approach
Research Strategy
Data Collection
Data Analysis
Qualitative
Quantitative
Exploratory
Literature Review
- Explain key concepts & definitions
- Identify key privacy & security risks
- Critically analyse academic & industry literature
Sources
- Semi-structured interviews
- Published Literature in journals
- Trusted Website Articles
- Practitioners opinion
- Questionaires
Multiple Linear Regression
- Extrapolate & Transform data
- Test the model
- Critically analyse the result
Empirical Findings
What multi-cloud means to enterprises
Factors inhibiting multi-cloud adoption
Are enterprises willing to adopt it in the future
Analysing of Empirical Findings
Present and analyse results objectively
Use data-driven results to profer solutions
Conclusion & Future Research

Figure 3.1 - Research Methodology Steps Diagram

3.1. Comparative Analysis: Examining How Multi-Cloud Strategies Impact Resilience

The choice between single cloud and multi-cloud strategies influences an organisation's infrastructural resilience meaningfully. Infrastructural resilience refers to the ability of an organisation's IT infrastructure to withstand and quickly recover from disruptions, including hardware failures, software issues, and cyber-attacks. Effective resilience strategies ensure minimal downtime and data loss, maintaining business continuity and service reliability. According to Manghui Tu et al. (2013), resilience is a critical aspect of modern IT strategies, especially as cyber threats and operational disruptions become sophisticated and rampant [10]. Single cloud strategies rely on a single cloud service provider (CSP), while multi-cloud strategies distribute services across multiple CSPs. This comparative analysis investigates how multi-cloud environments impact organisational resilience, drawing on insights from academic literature to highlight the benefits and challenges associated with each approach.

3.1.1. Single Cloud Strategies - Advantages

Organisations adopting single cloud strategies often benefit from streamlined operations and centralised management. By consolidating services with a single CSP, these organisations can achieve deep integration and optimization, leading to potentially better performance and more favourable service level agreements (SLAs). The homogeneity of the environment simplifies infrastructure management, monitoring, and compliance, as there is a unique set of processes and tools to oversee [11].

Disadvantages

Single cloud strategies have significant drawbacks in terms of resilience. A primary concern is the risk of vendor lock-in, where dependency on one provider can limit flexibility and adaptability over time [12]. From a resilience perspective, a single point of failure is a critical risk; if the CSP experiences an outage or security breach, the entire organisational infrastructure can be compromised. Additionally, relying on a single provider may restrict access to diverse and innovative services that other CSPs might offer, potentially limiting the robustness and responsiveness of the infrastructure.

3.1.2. Multi-Cloud Strategies - Advantages

Multi-cloud strategies offer enhanced resilience by distributing services across multiple CSPs. This approach mitigates the risk of vendor lock-in and provides a safeguard against service outages, as the failure of one provider can be offset by another [13]. By leveraging the unique strengths of different CSPs, organisations can optimise their infrastructure for performance, cost, and security. This diversification allows for more comprehensive risk management and the ability to implement best-of-breed solutions tailored to specific needs [14].

Disadvantages

Despite these advantages, multi-cloud strategies introduce complexity in management and coordination. Ensuring interoperability and consistent governance across different cloud platforms can be challenging and resource-intensive [15] [16]. The increased complexity heightens the risk of misconfigurations and gaps in security or performance monitoring. Furthermore, orchestrating disaster recovery and incident response across multiple CSPs requires sophisticated tools and elaborate processes to ensure timely and effective mitigation of issues.

3.2. Comparative Analysis - Response to Hardware Failures

In single cloud environments, hardware failures can be swiftly addressed within the unified infrastructure of the CSP, often with rapid failover mechanisms and dedicated support. However, the impact can be widespread if the failure is within a critical part of the CSP's infrastructure [17]. In contrast, multi-cloud environments benefit from redundancy across different providers. If one provider experiences hardware failures, other CSPs can continue to operate, thereby minimising disruption. This redundancy enhances overall resilience but demands effective synchronisation and data consistency strategies [18].

3.3. Response to Software Issues

Single cloud strategies benefit from streamlined software management and uniformity, which can simplify updates, patches, and troubleshooting. However, software issues can propagate quickly through a homogenous environment, potentially leading to significant disruptions. Multi-cloud strategies, on the other hand, compartmentalise software environments, reducing the likelihood that an issue in one CSP's software stack will affect the entire infrastructure [19]. This compartmentalization, however, requires rigorous management to maintain compatibility and coherence across different software ecosystems.

3.4. Cyber-Attacks and Security Breaches

Single cloud organisations can implement robust security measures within a consolidated environment, enabling comprehensive monitoring and rapid response. Nevertheless, the centralised nature makes them more vulnerable to targeted attacks that exploit the single point of failure [12]. Multi-cloud strategies diversify security postures across multiple CSPs, reducing the risk of a complete infrastructure compromise. The varied security implementations can complicate management but also provide a layered defence, making it more difficult for attackers to exploit vulnerabilities across all platforms simultaneously [15].

While single cloud environments offer simplicity, centralised control, and potentially faster responses to certain issues, they are more vulnerable to single points of failure. Multi-cloud environments appear to provide greater redundancy and flexibility, enhancing resilience through diversification but requiring more complex management and coordination efforts. Organisations must evaluate their specific needs, risk profiles, and resource capabilities when deciding between single cloud and multi-cloud strategies. By understanding the distinct advantages and challenges of each approach, organisations can better prepare their IT infrastructures to withstand and recover from disruptions, thus, enhancing the resilience of their operations in our ever-evolving digital world.

3.5. Data Collection

Questionnaire (see appendix) was the primary medium of collecting data for this research from sampled organisations. Data was also collected from interviews where possible. Given the limited time and resources, we were able to get 76 samples after dropping some data with missing fields.

3.6. Ethical Issues

Data Privacy: To stay within the confines of the law, we ensured that all data collected complies with privacy laws such as GDPR and organisational confidentiality agreements.

Bias in Data Collection: To limit bias we ensured the inclusion of a diverse range of companies across verticals using a mix of different cloud architectures in the study.

Impact on Participants: Care was made in considering the probable adverse impact on organisations participating in the study, especially in the process of carrying out the research. To conform with data laws like GDPR, we limited our request to the data needed for the research.

Consent and Anonymity: Beyond obtaining informed consent for using their data in the study, efforts were made in protecting the anonymity of participating organisations.

3.7. Tools and Test Data

Statistical Analysis Software: R, Python, IBM SPSS

Data Collection Technique: Questionnaires and Interviews

4.0 Empirical Analysis - Derivation of the Resilience Score Formula

To develop a comprehensive resilience score, we integrated theoretical insights and empirical data into our work. Hereafter, we outline the derivation process, including the theoretical foundation, empirical analysis, and assumptions made.

Theoretical Foundation:

Our approach builds on the work of Luz (2024), which discusses the importance of multi-cloud strategies in enhancing system resilience in the banking sector. This study emphasises that distributing workloads across multiple cloud providers ensures high availability and resilience in a way that optimises operational efficiency and maintains compliance with regulators [20]. Additionally, in their book - “Multi-Cloud Strategy for Cloud Architects” - Jeroen Mulder et al (2023) explores the architectural models of multi-cloud native applications and the challenges; providing a comprehensive overview of the benefits and complexities involved in multi-cloud adoption [21].

4.1. Empirical Observations:

We analysed data from enterprises, focusing on key predictors of resilience. The dataset included variables such as the number of cloud providers, percentage of services distributed, annual IT budget, downtime, incident response time, and redundancy measures.

4.1.1. Statistical Methods:

Using multiple linear regression, we quantified the contribution of each variable to the overall resilience score. The regression coefficients were as follows:

- Number of Cloud Providers (N_p): 10
- Percentage of Services Distributed (S_d): 0.2
- Annual IT Budget (B): 1/100000
- Downtime (hours/year) (D_t): -0.5
- Incident Response Time (hours) (R_t): -2
- Redundancy Measures (R_m): 20
- ϵ: Random noise (normal distribution with mean 0 and standard deviation 5)

4.1.2. Assumptions and Simplifications:

Null Hypothesis(H_0): There is no relationship between the variables and resilience score

Alternative Hypothesis(H_1): There is a statistically significant relation between the variables and resilience score.

We assumed linear relationships between the predictors and resilience score. We also assumed equal weightage of the variables to calculate the initial Resilience Score as shown below:

$$R_{initial} = 0.2N_p + 0.2S_d + 0.2B + 0.2D_t + 0.2R_m$$

We used the values to run a regression test and refined the model given the coefficients returned which indicated the variables had different weights of influence on the resilience score. The final formula is stated in section 4.1.3 below and is validated by the subsequent regression results. The IT budget was scaled to simplify its contribution.

Data augmentation was also done to generate additional data points based on the collected dataset from 76 valid questionnaires returned. Data augmentation is often used in data analysis to expand the dataset to make it normally distributed and suitable for a thorough statistical analysis [22] [23].

4.1.3. Derivation Process:

1. We Identified key variables from literature and expert interviews.
2. Collected and analysed data from enterprises (To achieve spread, original dataset was augmented using python) see appendix.
3. Performed multiple linear regression to determine the impact of each variable.
4. Combined these impacts into the final formula, incorporating random noise to reflect real-world variability.

The resulting formula is:

$$R = \left(N_p \times 10\right) + (S_d \times 0.2) + \left(\frac{B}{100000}\right) + (R_m \times 20) - (D_t \times 0.5) - (R_t \times 2) + \epsilon$$

This formula provides a quantifiable measure of enterprise resilience, integrating both cost and operational metrics. The significance of using multiple cloud providers and redundancy measures is supported by Luz (2024) and the Journal of Cloud Computing (2020) [24] respectively, highlighting their role in understanding resilience by distributing risks across multiple vendors and optimising resources. Additionally, the inclusion of random noise (ϵ) aligns with the Linear Regression methodologies outlined by Guo et al. (2023) to account for variability in regression models [25].

Variable	Description
N_p	Number of Cloud Providers
S_d	Percentage of Services Distributed
B	Annual IT Budget (in dollars)
D_t	Downtime (hours/year)
R_t	Incident Response Time (hours)
R_m	Redundancy Measures (0 for no, 1 for yes)
ϵ	Random Noise, where $\epsilon \sim N$ (0,5).

Table 1.0 - Variables and Descriptions

5.0. Testing the model:

Exploratory Data & Statistics

First few rows of the dataset:

```
   Number of Cloud Providers Percentage of Services Distributed  ...  Redundancy Measures
Enterprise Resilience Score

0                    3                    75.852937  ...              0                -3.507575

1                    4                    62.887709  ...              1                -6.417368

2                    1                    44.762209  ...              0               -58.170854

3                    3                    85.103602  ...              1                27.888244

4                    3                    74.778494  ...              0                 2.565009

[5 rows x 7 columns]
```

Summary statistics:

```
       Number of Cloud Providers  Percentage of Services Distributed  ...  Redundancy Measures
Enterprise Resilience Score

count              1000.000000                      1000.000000  ...          1000.000000
1000.000000
```

```
mean            2.534000                59.980381  ...          0.505000
8.255721

std            1.151595                23.344016  ...          0.500225
26.094302

min             1.000000                20.370562  ...          0.000000              -
77.097474

25%             1.000000                38.954617  ...          0.000000              -
9.935517

50%             3.000000                60.043327  ...          1.000000
8.610564

75%             4.000000                79.978319  ...          1.000000
26.570082

max             4.000000                99.977414  ...          1.000000
89.809811

[8 rows x 7 columns]
```

Missing values in each column:

```
Number of Cloud Providers            0

Percentage of Services Distributed    0

Annual IT Budget                     0

Downtime (hours/year)                0

Incident Response Time (hours)        0

Redundancy Measures                  0

Enterprise Resilience Score          0

dtype: int64
```

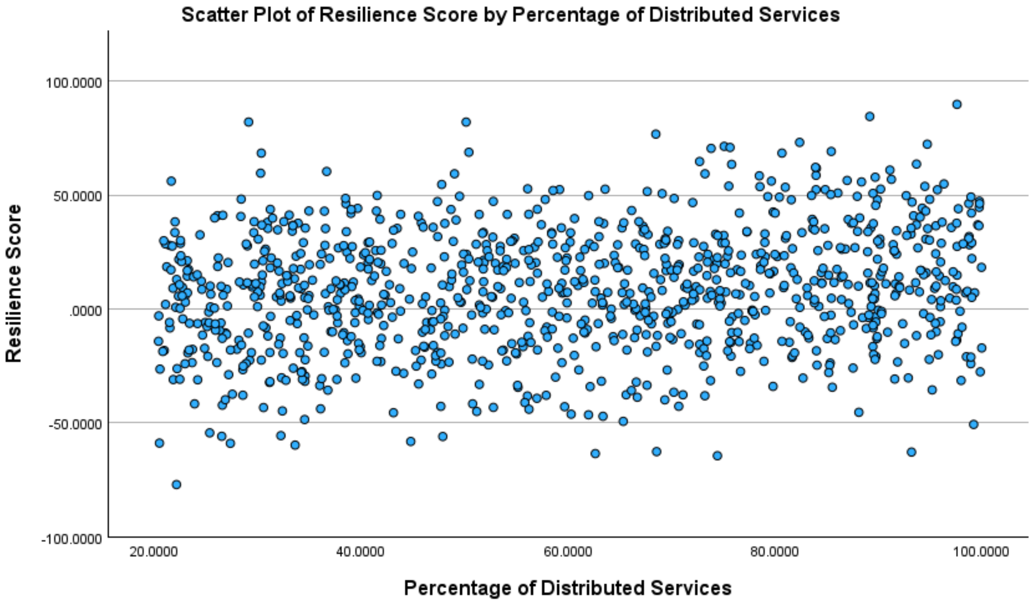


Figure 4.1 - Scatter Plot of % of Distributed Services vs. Enterprise Resilience Score

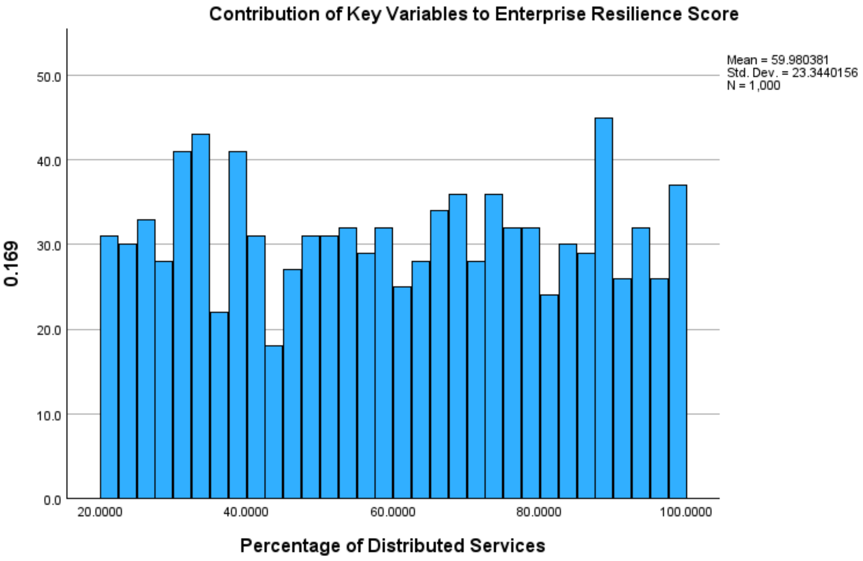


Figure 4.2 - % of Distributed Services Beta Coefficients

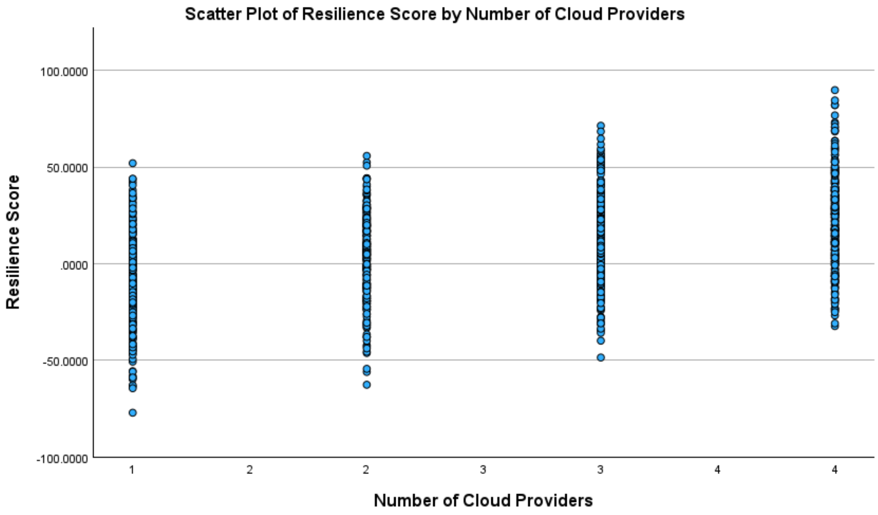


Figure 4.3 - Scatter Plot of Number of Cloud providers vs. Enterprise Resilience Score

5.1 Results Overview

The linear regression analysis was conducted to evaluate the impact of multiple factors on enterprise resilience. The independent variables included:

- Number of Cloud Providers
- Percentage of Distributed Services
- Annual IT Budget
- Downtime (hours/year)
- Incident Response Time (hours)
- Redundancy Measures

The dependent variable was the Enterprise Resilience Score.

The following table summarises the key results from the linear regression analysis we carried out, including the unstandardized coefficients (B), standard errors, Standardized Coefficients (Beta), t-values, and significance levels (p-values).

Variable	**Unstandardized Coefficients (B)**	**Std. Error**	**Standardized Coefficients (Beta)**	**t-value**	**Sig. (p-value)**
Constant	0.369	0.754	-	0.489	0.625
Number of Cloud Providers	9.891	0.137	0.437	71.976	<0.001

Percentage of Distributed Services	0.189	0.007	0.169	27.891	<0.001
Annual IT Budget	0.00001	0.000	0.207	34.133	<0.001
Downtime (hours/year)	-0.496	0.005	-0.550	-90.716	<0.001
Incident Response Time (hours)	-2.006	0.024	-0.506	-83.394	<0.001
Redundancy Measures	20.427	0.317	0.392	64.536	<0.001

Table 2.0 - Summary of Regression Coefficients

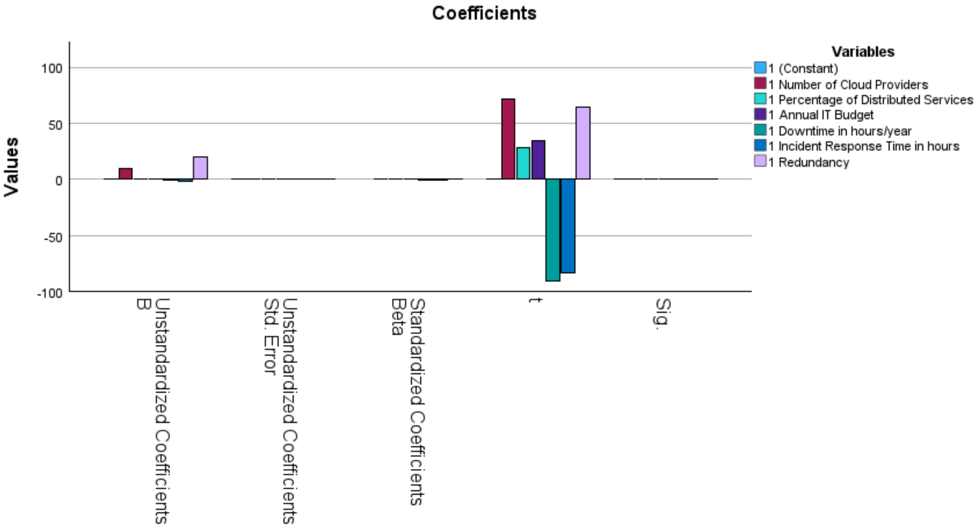


Figure 4.4 - “Standardized” coefficients (Beta values) of Variables

5.2. Interpretation of Results

1. Constant:

The constant term (intercept) is 0.369, with a standard error of 0.754. This value is not statistically significant (p = 0.625), indicating that the constant term does not significantly contribute to the model. A p-value greater than 0.05 suggests that the constant does not have a meaningful impact on the resilience score [26].

2. Number of Cloud Providers:

At (p < 0.001), this variable is highly significant and indicates a strong positive impact on the Enterprise Resilience Score. For every additional cloud provider, the resilience score increases by approximately 9.891 units. This finding is consistent with previous research showing that a p-value less than 0.001 points to very strong evidence against the null hypothesis, suggesting the variable is a crucial predictor [27].

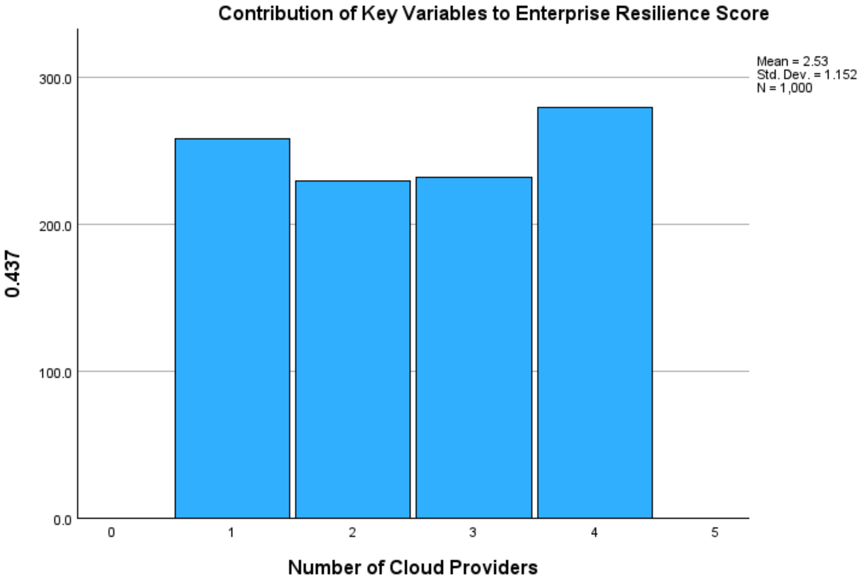


Figure 4.5 – Coefficient(B) contribution of Number of Providers

3. Percentage of Distributed Services:

The significant value (p < 0.001) shows that the variable is statistically significant, suggesting that an increase in the percentage of distributed services positively affects the resilience score. Specifically, for each percentage point increase in distributed services, the resilience score increases by 0.189 units. Once again, we reject the null hypothesis and accept the alternative.

4. Annual IT Budget:

This variable is significant (p < 0.001), indicating that higher IT budgets contribute positively to the resilience score. For every unit increase in the IT budget, the resilience score increases by 0.00001 units.

5. Downtime (hours/year):

This variable is highly significant (p < 0.001), indicating a strong negative impact on the resilience score. For each additional hour of downtime, the resilience score decreases by 0.496 units.

6. Incident Response Time (hours):

This variable is statistically significant (p < 0.001), demonstrating that longer incident response times negatively affect the resilience score. For each additional hour of response time, the resilience score decreases by 2.006 units.

7. Redundancy Measures:

This variable is significant (p < 0.001), showing that implementing redundancy measures has a strong positive impact on the resilience score. Having redundancy measures increases the resilience score by 20.427 units.

5.3. Framework Proposal:

These findings can be utilised to develop strategic initiatives aimed at improving resilience. As empirically demonstrated through the regression model, concrete strategies can be baked into regulatory standards to benchmark the requirements for enterprise deployment. Thus, guided by respective impacts of the variables, resources can be properly allocated to reflect their significant impact on the resilience of systems.

Risk assessment can also be aided by the regression result as potential outliers are removed, and decisions made from a quantifiable perspective. The regression model indicates that increased spending is not an outlier and has a direct correlation on the ability of enterprises to increase their footprint in multi-cloud adoption and hence, increase their organisation’s IT infrastructural resilience. Also, a case can be made for the distribution of services (SaaS, PaaS, IaaS, IaC) based on quantifiable metrics towards their impact on resilience.

6.0. Conclusion and Future Work

The regression analysis reveals several key factors that significantly contribute to enhancing enterprise resilience. It can be proven that predictors like increasing the number of cloud providers and redundancy measures impact the resilience of systems in a positive way. By leveraging these findings, a structured approach guided by empirical evidence to systematically enhance enterprise resilience can be achieved. Implementing these evidence-based strategies will go a long way in helping organisations to better withstand and recover from service disruptions thereby enhancing their workload resilience.

Future research should focus on further exploring the interactions between these variables and examining additional factors like APIs, serverless computing and unified security measures that may influence enterprise resilience. As the digital landscape evolves, exploring a time series forecast/analysis approach by collecting data over multiple time points to analyse trends and changes will further reveal ways to enhance resilience within multi-cloud strategies. The insights from such analysis will deepen the research, and hence, open the possibilities of creating viable solutions.

References

[1] C. Custer, ‘The State of Multi-Cloud 2024 - Strategies and Adoption Patterns’, Cockroach Labs, Inc, Industry Report, 2024.

[2] Grand View Research, ‘Multi-Cloud Management Market Size, Share & Trends Analysis Report By Deployment (Public, Private, Hybrid), By Service (Operations Management, Security & Compliance Management), By Region, And Segment Forecasts, 2023 - 2030’. Accessed: Apr. 14, 2024. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/multi-cloud-management-market-report

[3] B. C T and S. Mohan Kumar, ‘A Review on Security issues in Multi Cloud Computing and prevention by security measures’, *IJSRP*, vol. 13, no. 6, pp. 248–254, Jun. 2023, doi: 10.29322/IJSRP.13.06.2023.p13835.

[4] M. Singhal *et al.*, ‘Collaboration in multicloud computing environments: Framework and security issues’, *Computer*, vol. 46, no. 2, pp. 76–84, Feb. 2013, doi: 10.1109/MC.2013.46.

[5] P. Muralidhar and E. R. Aruna, ‘A Framework of Collaboration in Multicloud Computing Environments for Security Problems. Vol. 5, Issue 3.’, *International Journal of Computer Science and Technology,* vol. 5, no. 3, 2014.

[6] M. Reece *et al.*, ‘Systemic Risk and Vulnerability Analysis of Multi-cloud Environments’, Jul. 07, 2023, *arXiv*: arXiv:2306.01862. Accessed: Apr. 14, 2024. [Online]. Available: http://arxiv.org/abs/2306.01862

[7] K. A. Torkura, M. I. H. Sukmana, F. Cheng, and C. Meinel, ‘SlingShot - Automated Threat Detection and Incident Response in Multi Cloud Storage Systems’, in *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA: IEEE, Sep. 2019, pp. 1–5. doi: 10.1109/NCA.2019.8935040.

[8] P. R. Shukla and V. M. Patil, ‘A Comprehensive Review of Frameworks for Achieving Interoperability in Multi-Cloud Environments’, in *2023 Second International Conference on Informatics (ICI)*, Noida, India: IEEE, Nov. 2023, pp. 1–6. doi: 10.1109/ICI60088.2023.10421703.

[9] T. Luxner, ‘Cloud computing trends: Flexera 2024 State of the Cloud Report’, Flexera Blog. Accessed: Aug. 10, 2024. [Online]. Available: https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/

[10] Manghui Tu and Dianxiang Xu, ‘System resilience modeling and enhancement for the cloud’, in *2013 International Conference on Computing, Networking and Communications (ICNC)*, San Diego, CA: IEEE, Jan. 2013, pp. 1021–1025. doi: 10.1109/ICCNC.2013.6504231.

[11] D. Cowen, K. A. Johnston, and K. Vuke, ‘How cloud computing influences business strategy within South African enterprises’, in *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, Mauritius: IEEE, Aug. 2016, pp. 272–278. doi: 10.1109/EmergiTech.2016.7737351.

[12] B. Varghese and R. Buyya, ‘Next generation cloud computing: New trends and research directions’, *Future Generation Computer Systems*, vol. 79, pp. 849–861, Feb. 2018, doi: 10.1016/j.future.2017.09.020.

[13] M. Al-Roomi, S. Al-Ebrahim, S. Buqrais, and I. Ahmad, ‘Cloud Computing Pricing Models: A Survey’, *IJGDC*, vol. 6, no. 5, pp. 93–106, Oct. 2013, doi: 10.14257/ijgdc.2013.6.5.09.

[14] M. Sajid and Z. Raza, ‘Cloud Computing: Issues & Challenges’, International Journal of Computer Networks and Communications Security, Dec. 2013, pp. 41–53.

[15] C. Ramalingam and P. Mohan, ‘Addressing Semantics Standards for Cloud Portability and Interoperability in Multi Cloud Environment’, *Symmetry*, vol. 13, no. 2, p. 317, Feb. 2021, doi: 10.3390/sym13020317.

[16] Chinazor Prisca Amajuoyi, Luther Kington Nwobodo, and Mayokun Daniel Adegbola, ‘Transforming business scalability and operational flexibility with advanced cloud computing technologies’, *Comput. sci. IT res. j.*, vol. 5, no. 6, pp. 1469–1487, Jun. 2024, doi: 10.51594/csitrj.v5i6.1248.

[17] M. Kavis, *Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS)*. in The Wiley CIO series. Hoboken, New Jersey: Wiley, 2014.

[18] S. M. Almufti and S. R. M. Zeebaree, ‘Leveraging Distributed Systems for Fault-Tolerant Cloud Computing: A Review of Strategies and Frameworks’, *ACAD J NAWROZ UNIV*, vol. 13, no. 2, pp. 9–29, May 2024, doi: 10.25007/ajnu.v13n2a2012.

[19] K. Merseedi and S. Zeebaree, ‘Cloud Architectures for Distributed Multi-Cloud Computing: A Review of Hybrid and Federated Cloud Environment’, *Indonesian Journal of Computer Science*, vol. 13, pp. 1644–1673, Apr. 2024.

[20] A. Luz, ‘Embracing Multi-Cloud Strategies in the Banking Sector Author’, *EasyChair*, no. 13369, May 2024, Accessed: Jun. 08, 2024. [Online]. Available: https://easychair.org/publications/preprint/pfHj

[21] J. Mulder, *Multi-cloud strategy for cloud architects: learn how to adopt and manage public clouds by leveraging baseops, finops, and devsecops*, Second edition. Birmingham: Packt Publishing, 2023.

[22] D. Haba, *DATA AUGMENTATION WITH PYTHON enhance deep learning accuracy with data augmentation methods for image, text, audio, and tabular data*, 1st edition. England: PACKT PUBLISHING LIMITED, 2023.

[23] R. Khare, A. Mahapatra, and Accenture, ‘SURVEY ON COMPREHENSIVE TECHNIQUES OF TEXT DATA AUGMENTATION’, *IJEAST*, vol. 8, no. 2, pp. 47–56, Jun. 2023, doi: 10.33564/IJEAST.2023.v08i02.007.

[24] J. Alonso *et al.*, ‘Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review’, *J Cloud Comp*, vol. 12, no. 1, p. 6, Jan. 2023, doi: 10.1186/s13677-022-00367-6.

[25] Y. Guo, W. Wang, and X. Wang, ‘A Robust Linear Regression Feature Selection Method for Data Sets with Unknown Noise’, *IEEE Trans. Knowl. Data Eng.*, pp. 1–1, 2021, doi: 10.1109/TKDE.2021.3076891.

[26] J. Cohen, *Statistical power analysis for the behavioral sciences*, 2nd ed. Hillsdale, N.J: L. Erlbaum Associates, 1988.

[27] D. S. Moore, W. Notz, and M. A. Fligner, *The basic practice of statistics*, 6th ed., Student ed. New York: W.H. Freeman, 2013.

Appendix

Questionnaire

Thank you for participating in this survey. By providing the information requested in this questionnaire, you agree to allow your data to be used for research purposes. All efforts will be made to keep your responses anonymous and confidential.

Questionnaire for Assessing Factors Influencing Enterprise Resilience

Section A: General Information

1. **Organization Name**: ____
2. **Industry**: ____
3. **Number of Employees**: _____________________________________

Section B: Cloud Infrastructure

1. **Number of Cloud Providers**
   - How many different cloud service providers does your organization use?
     - □ 1
     - □ 2
     - □ 3
     - □ 4
     - □ More than 4 (Please specify): ___________
2. **Percentage of Services Distributed Across Multiple Cloud Providers**
   - What percentage of your organization’s IT services are distributed across multiple cloud providers?
     - □ Less than 20%
     - □ 20% - 39%
     - □ 40% - 59%
     - □ 60% - 79%
     - □ 80% - 100%

Section C: Financial Investment

1. **Annual IT Budget**
   - What is your organization’s annual IT budget?

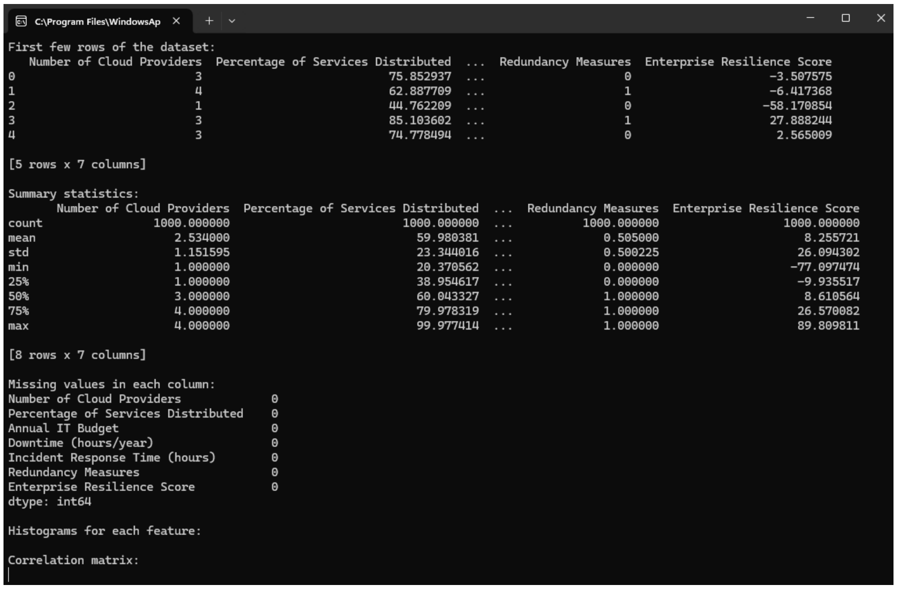
- □ Less than $100,000
- □ $100,000 - $499,999
- □ $500,000 - $999,999
- □ $1,000,000 - $1,999,999
- □ $2,000,000 or more

Section D: Operational Performance

1. **Downtime (hours/year)**
   - What is the total annual downtime for your organization’s IT services (in hours)?
     - □ Less than 10 hours
     - □ 10 - 19 hours
     - □ 20 - 29 hours
     - □ 30 - 39 hours
     - □ 40 hours or more (Please specify): ___________
2. **Incident Response Time (hours)**
   - What is the average time taken to respond to IT incidents (in hours)?
     - □ Less than 1 hour
     - □ 1 - 3 hours
     - □ 4 - 6 hours
     - □ 7 - 9 hours
     - □ 10 hours or more (Please specify): ___________

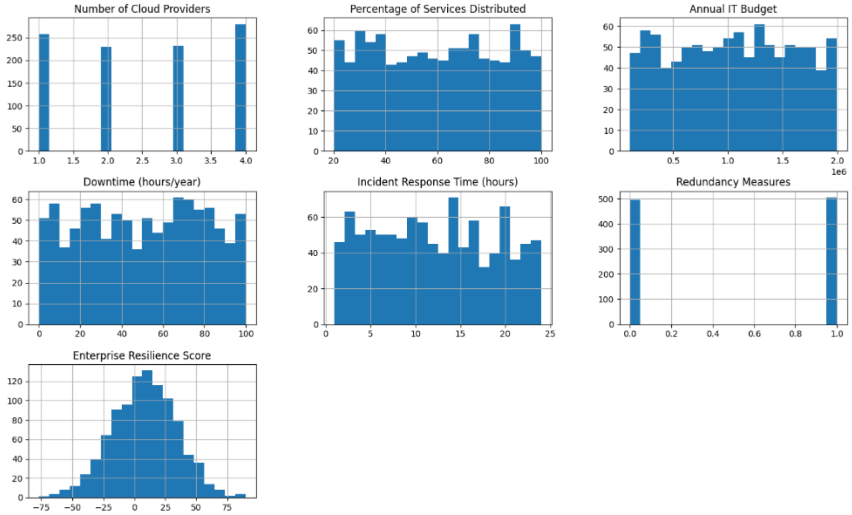
Section E: Redundancy Measures

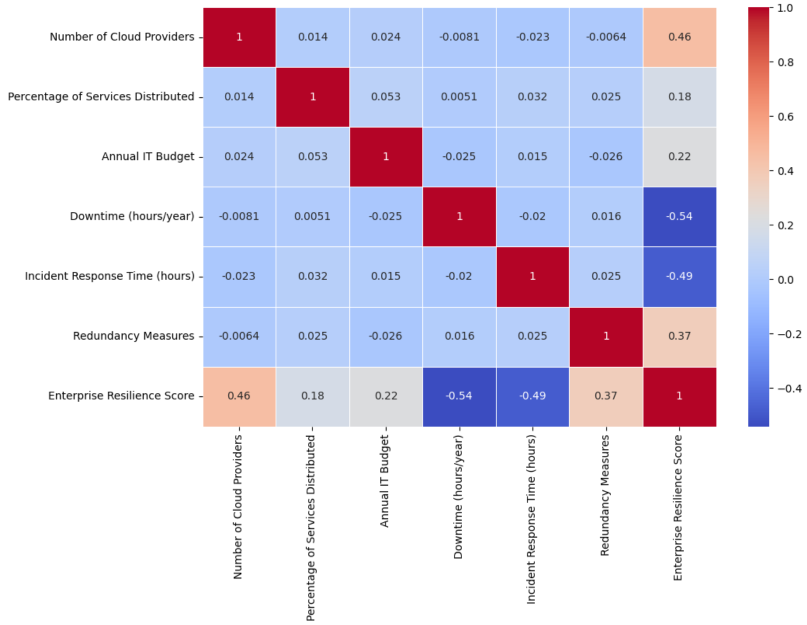
1. **Redundancy Measures**
   - Does your organization have redundancy measures (e.g., backup systems, failover mechanisms) implemented?
     - □ Yes
     - □ No



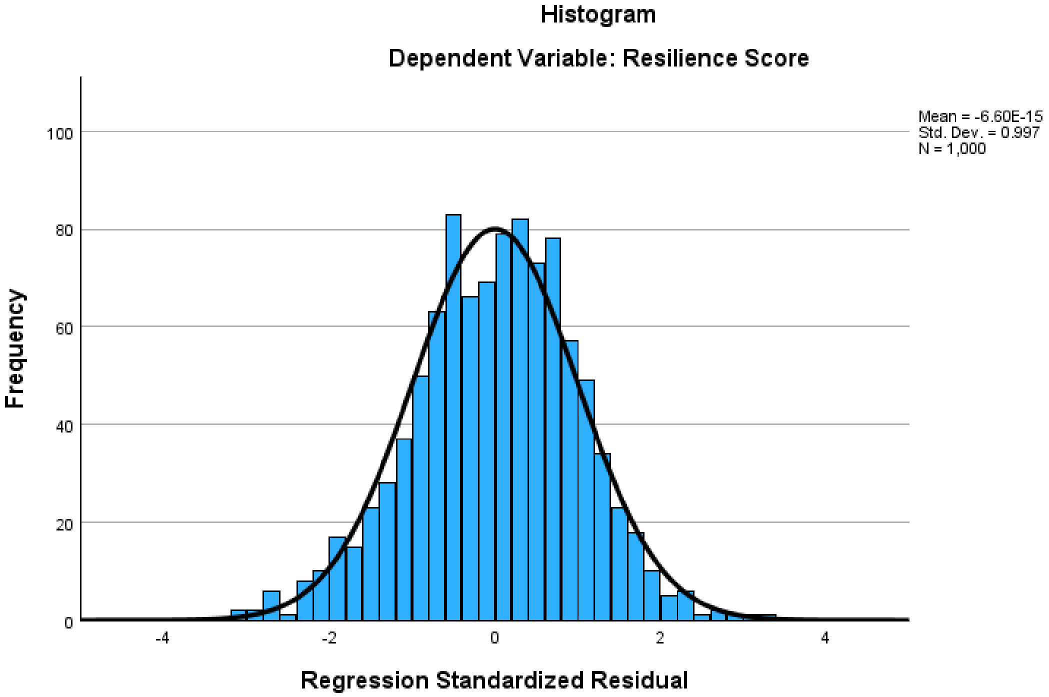
```
First few rows of the dataset:
   Number of Cloud Providers  Percentage of Services Distributed  ...  Redundancy Measures  Enterprise Resilience Score
0                          3                           75.852937  ...                    0                    -3.507575
1                          4                           62.887709  ...                    1                    -6.417368
2                          1                           44.762209  ...                    0                   -58.170854
3                          3                           85.103602  ...                    1                    27.888244
4                          3                           74.778494  ...                    0                     2.565009

[5 rows x 7 columns]

Summary statistics:
       Number of Cloud Providers  Percentage of Services Distributed  ...  Redundancy Measures  Enterprise Resilience Score
count                1000.000000                         1000.000000  ...          1000.000000                  1000.000000
mean                    2.534000                           59.980381  ...             0.505000                     8.255721
std                     1.151595                           23.344016  ...             0.500225                    26.094302
min                     1.000000                           20.370562  ...             0.000000                   -77.097474
25%                     1.000000                           38.954617  ...             0.000000                    -9.935517
50%                     3.000000                           60.043327  ...             1.000000                     8.610564
75%                     4.000000                           79.978319  ...             1.000000                    26.570082
max                     4.000000                           99.977414  ...             1.000000                    89.809811

[8 rows x 7 columns]

Missing values in each column:
Number of Cloud Providers             0
Percentage of Services Distributed    0
Annual IT Budget                      0
Downtime (hours/year)                 0
Incident Response Time (hours)        0
Redundancy Measures                   0
Enterprise Resilience Score           0
dtype: int64

Histograms for each feature:

Correlation matrix:
```

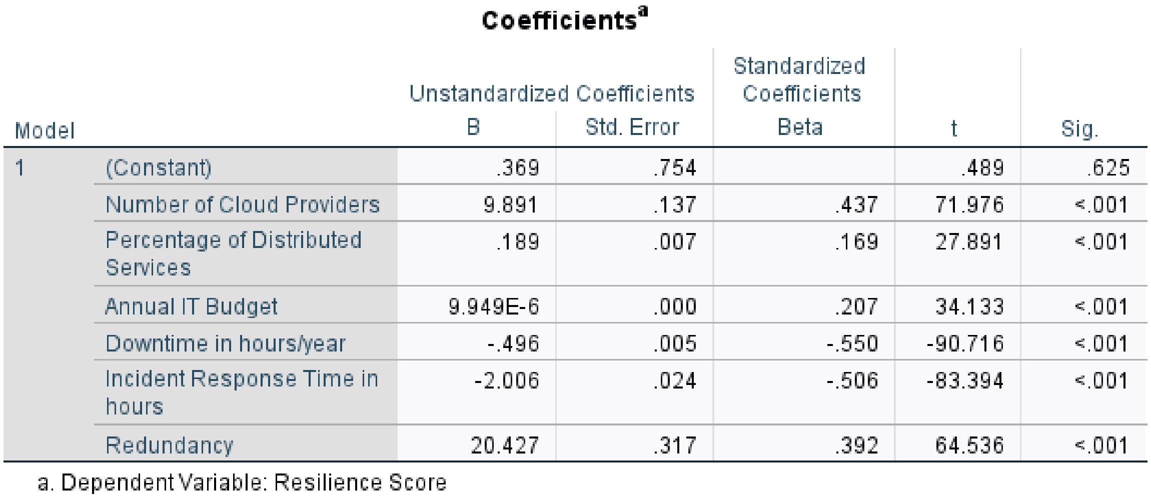
Exploratory and data check





Correlation matrix

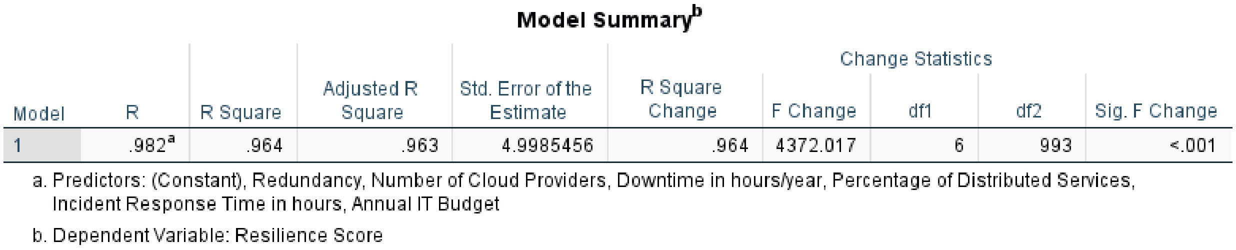




Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.369	.754		.489	.625
	Number of Cloud Providers	9.891	.137	.437	71.976	<.001
	Percentage of Distributed Services	.189	.007	.169	27.891	<.001
	Annual IT Budget	9.949E-6	.000	.207	34.133	<.001
	Downtime in hours/year	-.496	.005	-.550	-90.716	<.001
	Incident Response Time in hours	-2.006	.024	-.506	-83.394	<.001
	Redundancy	20.427	.317	.392	64.536	<.001

a. Dependent Variable: Resilience Score



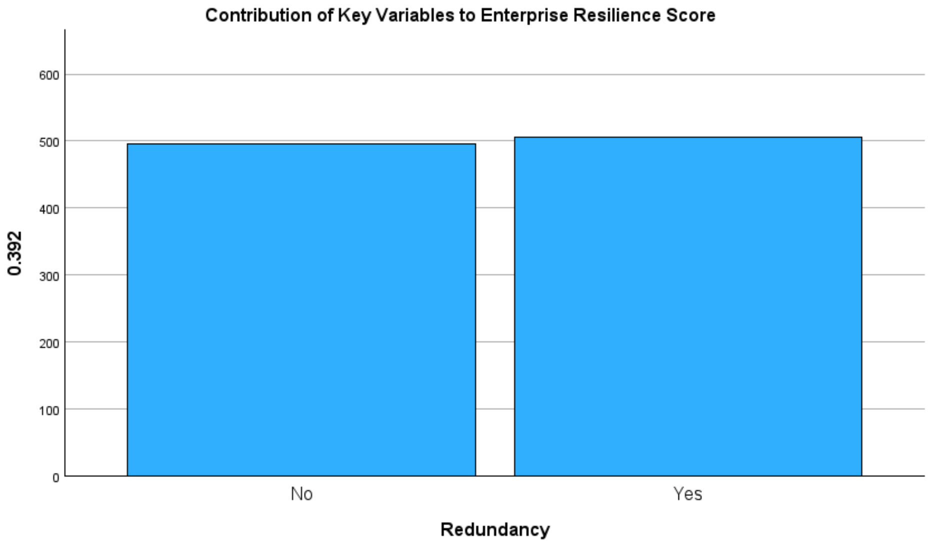
Model Summary[b]

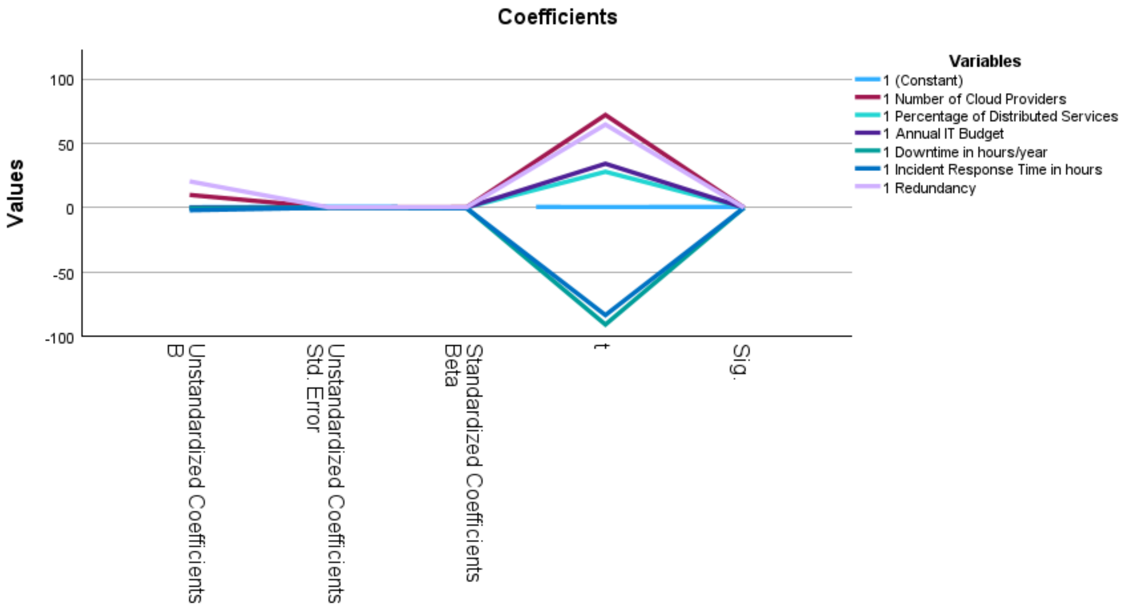
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.982[a]	.964	.963	4.9985456	.964	4372.017	6	993	<.001

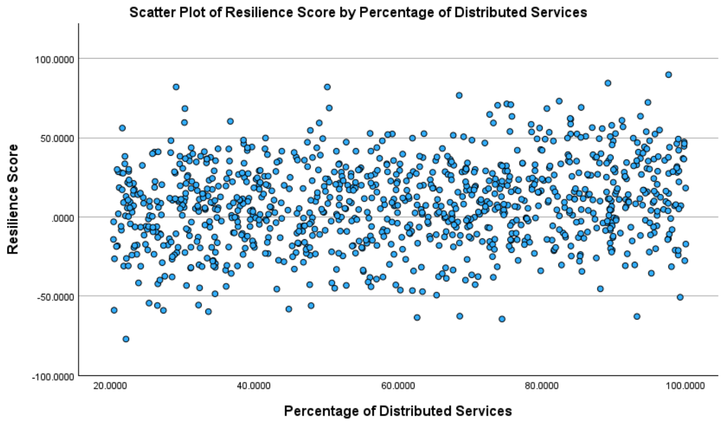
a. Predictors: (Constant), Redundancy, Number of Cloud Providers, Downtime in hours/year, Percentage of Distributed Services, Incident Response Time in hours, Annual IT Budget

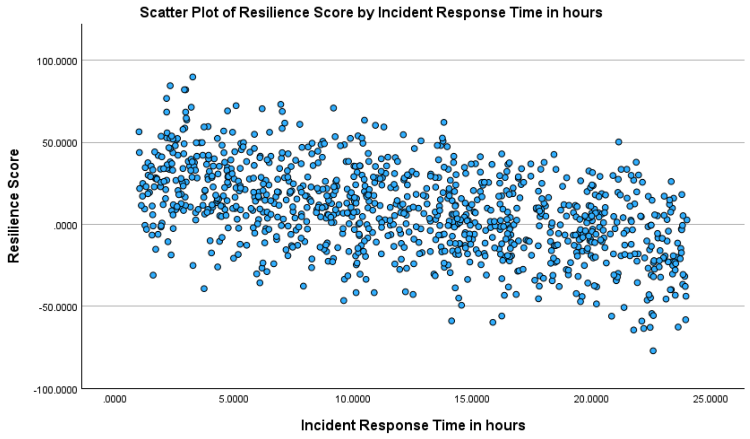
b. Dependent Variable: Resilience Score

Regression Analysis Output/Result




Coefficients
Values
100
50
0
-50
-100
Unstandardized Coefficients B
Unstandardized Coefficients Std. Error
Standardized Coefficients Beta
t
Sig.
Variables
1 (Constant)
1 Number of Cloud Providers
1 Percentage of Distributed Services
1 Annual IT Budget
1 Downtime in hours/year
1 Incident Response Time in hours
1 Redundancy


Scatter Plot of Resilience Score by Percentage of Distributed Services
Resilience Score
100.0000
50.0000
.0000
-50.0000
-100.0000
20.0000
40.0000
60.0000
80.0000
100.0000
Percentage of Distributed Services


Scatter Plot of Resilience Score by Incident Response Time in hours
Resilience Score
100.0000
50.0000
.0000
-50.0000
-100.0000
.0000
5.0000
10.0000
15.0000
20.0000
25.0000
Incident Response Time in hours