



Proposing an Information Security Framework for Small Scale BPO Sector which Provides Call Center Solution for Telecommunication Sector in Sri Lanka

C J Kalubowilage
(Reg. No.: MS22905840)

Supervisor : Mr. Amila Nuwan

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
(CYBER SECURITY)

December 2024

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

.....

Mr. Amila Nuwan (Supervisor)

Approved for MSc. Research Project:

MSc. Programme Co-ordinator, SLIIT

Approved for MSc:

Head of Graduate Studies, FoC, SLIIT

DECLARATION

This is to certify that the work is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources). The work has not previously been submitted in any form to the Sri Lanka Institute of Information Technology or to any other institution for assessment for any other purpose.

Sign: 

Jaliya Kalubowilage

Date: 28th January 2025

ABSTRACT

Jaliya Kalubowilage

MSc. in Information Technology

Supervisor: Mr. Amila Nuwan

December 2024

This study proposes an information security framework tailored for small-scale Business Process Outsourcing (BPO) companies in Sri Lanka, focusing on those offering call center solutions to the telecommunication sector. The research addresses the critical need for data protection due to the sensitive nature of client information and the increasing risks of cyber threats. A qualitative approach, incorporating literature reviews, case studies, and expert consultations, was adopted to identify existing challenges, including resource constraints, compliance issues, and insider threats. The proposed framework integrates elements from ISO 27001 and NIST Cybersecurity Frameworks, emphasizing data classification, access control, employee training, and incident response. Evaluation of the framework demonstrates its effectiveness in enhancing data security, regulatory compliance, and operational resilience for the BPO sector.

ACKNOWLEDGEMENT

First and foremost, I express my heartfelt gratitude to my supervisor, Mr. Amila Nuwan, for his invaluable guidance, encouragement, and constructive feedback throughout this research. His expertise and unwavering support were instrumental in shaping the direction and completion of this thesis.

I extend my sincere thanks to the faculty and staff of [Your Institution Name] for providing the necessary resources and a conducive environment for academic research. Special thanks to the experts and professionals in the BPO and telecommunication sectors who generously shared their insights, which significantly enriched this study.

Also, I express my heartfelt gratitude to Mr. Manoj Jayakumar senior Manager platforms and security of Ikman.lk, for his invaluable guidance, encouragement throughout this research.

To my family and friends, thank you for your unwavering support, patience, and understanding during this challenging journey. Your encouragement has been my greatest source of strength.

Finally, I am deeply grateful to all those who contributed, directly or indirectly, to the successful completion of this research. Your support and encouragement have been invaluable to me, and I will always cherish your contributions.

TABLE OF CONTENTS

DECLARATION	iii
ABSTRACT	iv
ACKNOWLEDGEMENT	v
TABLE OF CONTENTS	vi
List of Figures.....	xiii
List of Tables.....	xiv
Chapter 1 Introduction	16
1.1 Background	16
1.1.1 Background and Importance of BPO Industry in Sri Lanka.....	16
1.1.2 On the Significance of Information Security in the BPO Industry	16
1.2 Objectives of the Research and Scope of the Study	20
Chapter 2 Literature Review.....	21
2.1 Introduction to Information Security in BPO Sector	21
2.2 Existing Information Security Frameworks	22
2.2.1 ISO 27001 Standard	22
2.2.2 NIST Cybersecurity Framework.....	24
2.3 Challenges in Implementing Information Security in SMEs	25
2.3.1 Resource Constraints	26
2.3.2 Scalability Issues	27
2.4 Data Loss Prevention (DLP) in BPO Sector	29

2.4.1 DLP Mechanisms	30
2.4.2 Case Studies and Applications	31
2.5 Email Security and Quarantine Mechanisms	33
2.5.1 Email Threat Landscape	33
2.5.2 Quarantine and Filtering.....	34
2.5.3 Effectiveness of Quarantine.....	35
2.6 Regulatory and Compliance Considerations	36
2.6.1 Data Protection Regulations	36
2.6.2 Compliance Challenges	37
2.7 Emerging Trends and Future Directions	38
2.7.1 Emerging Security Technologies	38
2.7.2 Future Challenges and Opportunities	40
Chapter 3 Methodology.....	42
3.1 Research Design and Approach.....	42
3.1.1 Literature Review.....	42
3.1.2 Case Study Analysis:.....	43
3.1.3 Expert Consultations:	43
3.2 Data Collection and Analysis Methods.....	43
3.2.1 Data Collection	43
3.3 Data Analysis	44
3.4 Framework Development Process	47

3.4.1 Data Classification	47
3.4.2 Policy Definition	47
Chapter 4 Findings and Discussion.....	49
4.1 Analysis of Information Security Risks and Current Practices in Small BPO Businesses..	49
4.1.1 Information Security Risks in Small and Medium BPO Businesses	49
4.1.2 Current Practices in Information Security	51
4.2 Evaluation of the Proposed Information Security Framework.....	53
4.3 Effectiveness of the Framework.....	55
4.4 Discussion of the Framework’s Effectiveness	56
4.4.1 Addressing Identified Risks.....	57
4.4.2 Improving Data Protection.....	57
4.4.3 Enhancing Compliance.....	57
Chapter 5 Conclusion and Recommendations.....	59
5.1 Summary of Key Findings	59
5.1.1 Contemporary Activities in Information Protection.....	60
5.1.2 Assessment on the provided Information Security framework.....	60
5.2 Implications for the BPO Sector and Recommendations for Implementing the Proposed Framework	61
5.3 Suggestions for Future Research and Improvements	62
5.3.1 Exploring Emerging Threats and Technologies.....	62
5.3.2 Investigating Industry-Specific Challenges	62

5.3.3 Evaluating Framework Effectiveness in Diverse Contexts	62
5.3.4 Enhancing Framework Adaptability	62
5.3.5 Investigating the Impact of Training Programs	63
5.3.6 Addressing Resource Constraints	63
5.3.7 Examining Regulatory Compliance	63
Chapter 6 Implemented New Framework	64
6.1 Detailed Description of the New Information Security Framework	64
6.1.1 Introduction.....	64
6.2 Framework Overview	64
6.3 Data Classification and Protection.....	64
6.3.1 Overview.....	64
6.3.2 Data Classification System	65
6.3.3 Implementation of Protection Measures.....	65
6.3.4 Impact and Effectiveness	65
6.4 Access Control and Authentication	66
6.4.1 Overview.....	66
6.4.2 Multi-Factor Authentication (MFA)	66
6.4.3 Role-Based Access Control (RBAC)	66
6.4.4 Regular Access Reviews.....	66
6.4.5 Impact and Effectiveness	67
6.5 Incident Response and Recovery.....	67

6.5.1 Overview.....	67
6.5.2 Incident Response Process.....	67
6.5.3 Incident Response Plan.....	68
6.5.4 Incident Recovery	68
6.5.5 Impact and Effectiveness	68
6.6 Employee Training and Awareness	68
6.6.1 Overview.....	68
6.6.2 Training Programs.....	69
6.6.3 Impact and Effectiveness	70
6.7 Email Security and Quarantine.....	70
6.7.1 Overview.....	70
6.7.2 Email Filtering	70
6.7.3 Quarantine Strategies.....	70
6.7.4 Manual Review	71
6.7.5 Monitoring and Reporting	71
6.7.6 Impact and Effectiveness	71
6.8 Compliance and Regulatory Requirements.....	71
6.8.1 Overview.....	72
6.8.2 Regulatory Compliance	72
6.8.3 Impact and Effectiveness	73
6.9 Emerging Security Technologies.....	73

6.9.1 Overview.....	73
6.9.2 Artificial Intelligence (AI) and Machine Learning (ML)	73
6.9.3 Blockchain Solutions.....	74
6.9.4 Impact and Effectiveness	74
6.10 Framework Components and Structure.....	74
6.10.1 Data Classification and Protection	74
6.10.2 Access Control and Authentication	75
6.10.3 Incident Response and Recovery	75
6.10.4 Employee Training and Awareness.....	76
6.10.5 Email Security and Quarantine	76
6.10.6 Compliance and Regulatory Requirements	77
6.10.7 Emerging Security Technologies	77
6.11 Implementation Steps and Processes	78
6.11.1 Data Classification and Protection	78
6.11.2 Access Control and Authentication.....	78
6.11.3. Incident Response and Recovery	78
6.11.4. Employee Training and Awareness.....	79
6.11.5 Email Security and Quarantine	79
6.11.6 Compliance and Regulatory Requirements	80
6.11.7 Emerging Security Technologies	80
6.12 Evaluation of the Framework's Impact and Effectiveness	80

6.12.1 Data Protection Improvement	80
6.12.2 Incident Response Effectiveness.....	81
6.12.3 Email Security and Quarantine Effectiveness.....	82
6.12.4 Compliance and Regulatory Adherence	82
Chapter 7 Conclusion.....	83
Bibliography	84
Appendix	93

List of Figures

Figure 3.1 Pillars which masseurs the effectiveness of implementing Security Frame work	45
Figure 3.2 Awareness vs Effectiveness of implementing Security framework	45
Figure 3.3 Framework evaluation vs effectiveness of implementing security framework..	46

List of Tables

Table 6.1 Data Classification Levels	74
Table 6.2 Data Protection Measures	75
Table 6.3 Access Control Mechanisms	75
Table 6.5 Training Programs.....	76
Table 6.6 Email Threat Landscape	76
Table 6.7 Email Security and Quarantine Mechanisms	77
Table 6.8 Compliance Guidelines.....	77
Table 6.9 Emerging Security Technologies	77
Table 6.10 Data Classification Implementation	78
Table 6.11 Access Control Implementation	78
Table 6.12 Incident Response Implementation	79
Table 6.13 Training Implementation	79
Table 6.14 Email Security Implementation.....	79
Table 6.15 Compliance Implementation.....	80
Table 6.16 Emerging Technologies Integration	80
Table 6.17 Data Protection Metrics	81
Table 6.18 Incident Response Metrics.....	81

Table 6.19 Email Security Metrics 82

Table 6.20 Compliance Metrics..... 82