

Sri Lanka Institute of Information Technology



Gap Analysis Report

Group Number – 59

ESIS Assignment

IE3102 - Enterprise Standards for Information Security

Group Details:

	Student ID	Student Name	Email	Contact Number
1	IT23415140	U.L.K.H. Liyanage	it23415140@my.sliit.lk	0773092825
2	IT23159730	W.H.M.S.R. Bandara	it23159730@my.sliit.lk	0763366659
3	IT23269484	T.H. Ranasinghe	it23269484@my.sliit.lk	0762090122
4	IT23187214	N.K.B.H. Rathnayake	it23187214@my.sliit.lk	0719106526
5	IT23171138	D.P.D.K. Perera	it23171138@my.sliit.lk	0710426973

Contents

1. Introduction.....	4
2. Current Information Security Posture	5
3. Gap Analysis Against ISO/IEC 27001:2022	6
4. Summary of Findings.....	7
5. Initial Risk Register - Dynamic Biz IT Solutions	8
6. Risk Treatment Recommendations	10
7. Conclusion	11

1. Introduction

Dynamic Biz IT Solutions includes around 20 employees in various sectors such as software development, customer service, marketing, design, and accounting. It is classified in the small-sized online IT service industry. The organization IT service provider for the clients whom they handle managing Logical Property as well as highly sensitive data and financial transaction, therefore is exposed to various types of issues such as phishing, ransomware, unauthorized access and misuse, and insider threat.

The Company has implemented in their organization an application for role-specific Security Awareness and Policy Management. This application does role-oriented training and exercises (Quizzes, simulations, games), maintains policy version control, and tracks compliance for different policy documents. A strong initiative to sustain documents has been made, however, there is a gap that ISO/IEC 27001:2022 has, as there is a lack in an all-about Industrial Security Management System that encompasses governance, risk management, continuous improvement, and alignment to regulatory frameworks.

This report aims to find the Gap Analysis of Dynamic Biz's current security posture of the organization is to the requirements of ISO/IEC 27001:2022, map and analyze the risks and recommend appropriate actions to improve the level of maturity in the organization's ISMS.

2. Current Information Security Posture

Dynamic Biz has made progress in strengthening its technical controls and employee awareness. Key practices already implemented include:

- Role-based access control (RBAC) and MFA for user accounts.
- Training modules personalized to roles such as developers, marketers, and accountants.
- Policy management platform with document publishing and compliance tracking.
- Encryption standards (HTTPS, AES-256) and secure password hashing (bcrypt/Argon2).
- Audit logs are reviewed monthly to monitor system activities.

Despite these assets, several **ISO 27001 core elements are missing**:

- No formal ISMS governance framework or scope statement.
- Lack of structured risk assessment and treatment plan.
- Minimal evidence of leadership involvement in approving policies.
- Limited monitoring and evaluation of ISMS performance.

3. Gap Analysis Against ISO/IEC 27001:2022

The following table highlights where the Dynamic Biz needs to align with ISO 27001 and where the gaps exist.

ISO 27001 Clause	Current Status	Gap Identified
Clause 4 - Context of the Organization	Security awareness system exists.	No documented ISMS scope, context analysis, or interested parties list.
Clause 5 - Leadership	Policies exist but no executive endorsement.	No evidence of management-approved Information Security Policy or assigned ISMS roles.
Clause 6 - Planning	Technical measures are deployed.	No structured risk assessment or risk treatment methodology.
Clause 7 - Support	Training delivered via awareness platform.	No competency framework, awareness KPIs, or documented communication strategy.
Clause 8 - Operation	Compliance tracking is automated.	Missing incident response procedures, supplier risk evaluation, and change management.
Clause 9 - Performance Evaluation	Logs reviewed monthly.	No internal audit program, management reviews, or KPI dashboards.
Clause 10 - Improvement	Feedback loops in awareness modules.	No structured non-conformity handling or continual improvement process.

Annex A Gaps:

- A.5.9 - Asset inventory missing.
- A.5.21 - Supplier management not formalized.
- A.5.29 - No Business Continuity Planning (BCP).
- A.8.28 - Secure development lifecycle not fully documented.

4. Summary of Findings

Strengths:

- Strong technical foundation: MFA, RBAC, encryption.
- Innovative role-based awareness platform.
- Active compliance monitoring through audit logs.

Weaknesses / non-conformities:

- Missing ISMS governance (scope, roles, leadership involvement).
- Missing documented risk assessment or SoA.
- Weak supplier risk management.
- Missing formal BCP or incident response plan.
- Limited evidence of continual improvement cycle.

Opportunities for Improvement:

- Integrate awareness platform with ISO 27001 governance fundamentals (incident reporting, compliance dashboards).
- Build a formal risk management framework aligned to Annex A.
- Involve leadership in approving and endorsing the Information Security Policy.

5. Initial Risk Register - Dynamic Biz IT Solutions

Asset	Threat	Vulnerability	Impact	Likelihood	Risk Level	Recommended Control (ISO/IEC 27001 Annex A)
Clients' Financial Records	Data breach, unauthorized access	Weak supplier agreements, poor monitoring	High	Medium	High	Supplier due diligence & SLA clauses (A.5.21), access control monitoring (A.5.15).
Source Code Documents	Insider misuse, theft	Lack of segregation of duties, weak logging	High	Medium	High	Secure coding controls (A.8.28), RBAC & monitoring (A.8.30).
Employee's Email Accounts	Phishing/social engineering	Training not consistent	Medium	High	High	Phishing simulations, targeted training (A.6.3, A.6.7).
Policy Documents	Outdated/conflicting policies	No formal review lifecycle	Medium	Medium	Medium	Annual reviews, approval workflows (A.5.9, A.5.20).
Customer Databases	Ransomware, breach	Backups not tested	High	Medium	High	Regular backup testing (A.8.13), enhanced encryption monitoring (A.8.24).
Authentication System	Credential compromise	Partial MFA rollout	High	Medium	High	MFA across all accounts (A.5.17), enforce strong password policies (A.5.18).
IT Services Continuity	Service outage	Missing BCP/DRP	High	Low	Medium	Develop & test BCP/DRP (A.5.29).

Marketing Accounts	Brand damage from takeover	Shared credentials	Medium	Medium	Medium	Unique credentials, MFA for all accounts (A.5.17, A.8.16).
End-User Devices	Malware infection	Weak patching, admin rights too broad	High	Medium	High	Patch management (A.8.23), restrict privileges (A.5.15).
Cloud Services	Third-party breach	Weak supplier SLA	High	Medium	High	SLA-based supplier risk assessment (A.5.21).

6. Risk Treatment Recommendations

1. **Formalize ISMS Governance:** Draft ISMS scope, assign roles (ISMS Manager, Risk Officer), and ensure leadership endorsement.
2. **Implement Risk Management Framework:** Carry out the planned risk evaluation and risk treatment plan in conjunction with Annex A controls.
3. **Enhance Compliance Processes:** Define the scope and structure of internal audits, management reviews, and objectives.
4. **Supplier & Third-Party Management:** Implement due diligence and contract provisions with enhanced confidentiality safeguards.
5. **Business Continuity & Incident Response:** Improve existing Business Continuity Plans and Incident Response Plans through periodic testing and adaptation.
6. **Continuous Awareness & Measurement:** Incorporate awareness KPIs and improvement cycles into the integration of platform modules.

7. Conclusion

Dynamic Biz IT Solutions is building a strong technical capability and awareness foundation through its security awareness programs and MFA and encryption use. However, ISO/IEC 27001:2022 is more than technical measures and requires a complete management system perspective.

The Gap Analysis identifies a strong awareness, and access control skills, and significant shortcomings in governance, risk management, oversight of suppliers, business continuity, and continual improvement. Without formal governance of the ISMS that covers risk treatment and monitoring, security efforts will remain uncoordinated.

These gaps, particularly the lack of sufficient leadership, structured risk evaluation, supplier due diligence, and continuity planning, Dynamic Biz can work towards ISO 27001 readiness. This will bolster resilience, enhance client trust, and provide a valuable competitive advantage in the IT services industry.