Sri Lanka Institute of Information Technology

ISO/IEC 27001:2022 Implementation Simulation – Information Security Consulting Team Project

Gap Analysis Report – Group 060

Group ID - 060	
Name	**IT Number**
S.M.F. Hana	IT23255142
J. Aazaf Ritha	IT23151710
M.F.M. Farhan	IT23422070
H.M.S.H Wijerathna	IT23306936
R.M.T.P. Rasnayake	IT23246546

Module: IE 3102

Enterprise Standards for Information Security

Year 3, Semester 1

B.Sc. (Hons) in Information Technology Specialized in Cyber Security

Contents

1. Executive Summary

This report presents the results of a gap analysis conducted for ARRO (Pvt) Ltd, a leading Sri Lankan e-commerce and logistics technology company, as part of the simulation of implementing an Information Security Management System (ISMS) in alignment with ISO/IEC 27001:2022. The primary objective of this exercise was to evaluate ARRO's current information security posture, identify areas of non-conformance with ISO 27001 requirements, and propose recommendations for improvement.

ARRO manages sensitive customers, vendor, payment, logistics, and employee data through its AWS-hosted marketplace, payment systems, and logistics platform. While the organization demonstrates notable strengths such as AWS redundancy, multi-factor authentication for administrators, and basic fraud detection systems, the analysis identified significant gaps. These include the absence of a formal Information Security Policy, lack of a structured risk management process, no documented Incident Response or Business Continuity Plans, weak vendor onboarding controls, and limited employee awareness and training on information security practices.

A clause-by-clause assessment against ISO/IEC 27001:2022 revealed that ARRO is non-conformant in several critical areas, particularly in governance (Clause 5 – Leadership), planning (Clause 6 – Planning), operational controls (Clause 8 – Operation), and performance evaluation (Clause 9 – Performance Evaluation). In addition, a review of Annex A controls highlighted gaps in access control, supplier security, incident management, and business continuity planning.

The risk assessment identified six major risks with high business impact:

- Customer database breaches due to weak access control
- Fraudulent payment transactions
- Fake vendor accounts undermining trust
- Ransomware attacks disrupting logistics operations
- Insider misuse of employee data
- Denial-of-service attacks on cloud infrastructure

If unaddressed, these risks could result in financial losses, regulatory penalties under the Sri Lankan PDPA and PCI DSS, service downtime, and severe reputational damage.

To mitigate these risks, the report recommends establishing a top management approved Information Security Policy, implementing a risk management methodology and register, strengthening access governance, formalizing incident response and business continuity processes, enhancing supplier onboarding and monitoring, and rolling out a comprehensive training and awareness program.

By addressing these gaps through a phased roadmap, ARRO will significantly improve its information security maturity, achieve compliance with regulatory requirements, and build the resilience and trust needed to maintain its competitive advantage in Sri Lanka's growing digital marketplace.

2. Introduction

Information security has become a critical factor for modern organizations that depend on digital technologies, online platforms, and cloud infrastructures. In today's environment of increasing cyber threats, protecting sensitive information is not only a technical challenge but also a governance and compliance requirement.

ISO/IEC 27001:2022 is the international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System **(ISMS)**. It follows the Plan–Do–Check–Act (PDCA) **cycle**, ensuring a structured lifecycle for managing risks, improving resilience, and achieving continual improvement.

This report presents a gap analysis for ARRO (Pvt) Ltd, a leading e-commerce and logistics technology company in Sri Lanka. The analysis compares ARRO's current security practices against ISO/IEC 27001:2022 Clauses 4–10 (Context, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement) and relevant Annex A controls. The findings highlight areas where ARRO is conformant, partially conformant, or non-conformant, providing a baseline for ISMS implementation.

The results of the Gap Analysis will:

- Identify ARRO's strengths and weaknesses in information security.
- Map out non-conformities against ISO requirements.
- Establish an initial risk register based on asset–threat–vulnerability mapping.
- Recommend risk treatment measures aligned with ISO Annex A controls.
- Provide the foundation for ARRO's ISMS documentation pack (Scope Statement, Information Security Policy, SoA, and Risk Treatment Plan).

By conducting this gap analysis, ARRO will be better positioned to strengthen its security posture, comply with legal and regulatory requirements such as the Sri Lankan Personal Data Protection Act (PDPA) and PCI DSS, and build stronger trust among its 1.2 million active customers and 15,000 registered vendors.

3. Scope and Objectives

4.1. Scope of the Gap Analysis

The scope of this gap analysis covers the information assets, processes, and technologies that support ARRO's core business operations, in alignment with Clause 4 (Context of the Organization) of ISO/IEC 27001:2022. This includes:

- E-commerce Marketplace – ARRO's web and mobile platforms, including ARRO Mall and ARRO Live.
- Logistics & Delivery (ARRO Express) – Nationwide distribution with regional hubs and 50+ delivery centers.
- Payment Systems – Card, wallet, bank transfer, and cash-on-delivery transactions (20,000 daily).

- Cloud Infrastructure – Services hosted on Amazon Web Services (AWS), including applications, databases, and storage.
- Corporate Operations – HR, payroll, employee records, and administrative processes at headquarters and regional hubs

Exclusions:

Third-party systems outside ARRO's direct control are excluded, except where they integrate with in-scope processes (e.g., vendor platforms or payment gateways). Supplier and vendor risks are managed through onboarding checks, contractual clauses, and monitoring.

4.2. Objectives of the Gap Analysis

1. Assess ARRO's current information security posture against ISO/IEC 27001:2022 requirements, including Clauses 4–10 and Annex A controls.
2. Identify gaps, non-conformities, and weaknesses, classifying them as Conformant (C), Partially Conformant (PC), or Non-Conformant (NC).
3. Develop an initial risk register by mapping assets, threats, and vulnerabilities, then assess each risk based on its likelihood and impact.
4. Recommend risk treatment measures aligned with ISO/IEC 27002:2022 implementation guidance and Annex A controls.
5. Support regulatory compliance, including Sri Lanka's Personal Data Protection Act (PDPA) and PCI DSS for payment card data.
6. Provide a foundation for ISMS documentation, including the Scope Statement, Information Security Policy, Statement of Applicability (SoA), and Risk Treatment Plan.
7. Enable continual improvement, ensuring ARRO can adopt the Plan–Do–Check–Act (PDCA) cycle for sustainable ISMS implementation.

4. Gap Analysis Process

4.1. Gap Analysis Procedures

The Gap Analysis was carried out by comparing ARRO's existing information security practices against the requirements of ISO/IEC 27001:2022. The process followed a structured methodology based on the PDCA cycle, ensuring continual improvement and alignment with the standard:

- **Plan** – Identify ARRO's stakeholders, information assets, and compliance requirements (PDPA, PCI DSS). Define the scope, criteria, and methods for the analysis.
- **Do** – Collect and review evidence of current practices, including ARRO's company profile, security posture, and technical safeguards.
- **Check** – Assess current practices against Clauses and the Annex A controls, guided by ISO/IEC 27002:2022.
- **Act** – Classify each requirement as Conformant (C), Partially Conformant (PC), or Non-Conformant (NC), and recommend corrective actions and risk treatments.

Supporting Activities:

- Document Review – Examining ARRO's company profile, current controls, and compliance drivers.
- ISO 27001 Clause Mapping – Evaluating conformance with Clauses 4–10 (Context, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement).
- Annex A Control Review – Identifying the presence or absence of applicable controls such as access management, supplier security, incident response, and business continuity.
- Risk Identification – Using asset–threat–vulnerability mapping to create an initial risk register.
- Evaluation – Classifying each requirement as Conformant (C), Partially Conformant (PC), or Non-Conformant (NC).
- Recommendations – Proposing risk treatments and improvements to close the identified gaps.

This PDCA-driven approach ensures that the findings are not only aligned with ISO/IEC 27001:2022 certification requirements but also provides a continuous improvement path. The results serve as the foundation for developing ARRO's ISMS documentation pack.

4.2. Project Team

The Gap Analysis was conducted by a consulting team with defined responsibilities reflecting information security consulting roles:

1. **Lead Consultant / Project Coordinator - IT23422070 – M.F.M. Farhan**

Established project goals and deliverables, coordinated tasks, monitored progress, and ensured integration of the final report. Facilitated internal communication and led the consultancy approach.

2. **Risk & Controls Analyst - IT23151710 – J. Aazaf Ritha**

Conducted the clause-based gap analysis using ISO/IEC 27001:2022, mapped Annex A controls, developed the risk register, and prepared the risk treatment plan.

3. **ISMS Documentation Specialist - IT23255142 – S.M.F. Hana**

Drafted and formatted the ISMS core documentation, including the Scope Statement, Information Security Policy, Statement of Applicability (SoA), and Risk Treatment Plan. Ensured alignment with ISO/IEC 27001 clauses.

4. **Compliance Advisor - IT23246546 – R.M.T.P. Rasnayake**

Reviewed legal, regulatory, and contractual obligations (e.g., PDPA, PCI DSS, Consumer Protection). Ensured ISMS content addressed compliance requirements and highlighted non-conformities.

5. **Presentation & Stakeholder Engagement Lead - IT23306936 – H.M.S.H Wijerathna**

Designed and delivered the board-level presentation. Prepared executive summaries, visual roadmaps, and facilitated boardroom stakeholder engagement and Q&A.

While each member had a defined role, all contributed across activities to ensure the consultancy pack was cohesive, accurate, and complete.

5. Summary of Findings

The Gap Analysis assessed ARRO's information security practices against ISO/IEC 27001:2022 Clauses 4–10 and selected Annex A controls, with implementation guidance from ISO/IEC 27002:2022. Each gap has also been linked to the PDCA cycle, which underpins ISO 27001's continual improvement model.

5.1. Gap Analysis Reporting

ARRO has established some strong technical foundations, such as AWS redundancy, administrator MFA, and basic fraud detection. However, the analysis reveals major governance and operational weaknesses, including the absence of an Information Security Policy, a structured risk management methodology, supplier security checks, and formal incident response and business continuity planning.

5.2. ISO 27001 Clause Gap Analysis

Table 5-1 - Clause-by-Clause Gap Analysis

Clause	Requirement	Current Status at ARRO	Assessment	PDCA Stage
4 Context of the Organization	Define ISMS scope, stakeholders, and risk criteria	Stakeholders identified, but no documented ISMS scope or risk methodology	PC (Partially Conformant)	Plan
5 Leadership	Approve and communicate an Information Security Policy; assign roles	No formal IS Policy; roles and responsibilities undefined	NC (Non-Conformant)	Plan
6 Planning	Establish risk assessment methodology, treatment plan, and measurable objectives	Risks informally known, but no structured risk register or objectives	NC	Plan

7 Support	Ensure competence, awareness, communication, and controlled documentation	Limited training, no awareness program, no document control	NC	Do
8 Operation	Implement risk treatment, supplier controls, change management, incident processes	No Incident Response Plan; weak supplier verification; access reviews not performed	NC	Do
9 **Performance Evaluation**	Conduct monitoring, internal audits, and management reviews	No audits or management review framework	NC	Check
10 **Improvement**	Establish corrective actions and continual improvement mechanisms	No corrective action or continual improvement process	NC	Act

6.3. Annex A Control Gap Analysis

Table 5-2 – Annex A Control Gap Analysis (Key Controls)

Control Category	Example Areas	Current Status	Gap Identified	Conformance (C/PC/NC)	Treatment Recommendation	PDCA Stage
Organizational Controls (A.5)	IS Policy, Supplier Security, SLAs, Compliance	Draft IS Policy not yet approved; supplier contracts exist but lack SLAs	No formal IS Policy; no supplier SLAs for patching, incident reporting, uptime	NC	Approve and publish IS Policy; update contracts with SLAs (patching ≤14 days, incident ≤24h, uptime 99.9%)	Plan / Do

People Controls (A.6)	Screening, Awareness, Roles, Termination	Awareness sessions informal; no structured program; JML process incomplete	No formal awareness training program; weak joiner–mover–leaver controls	NC	Launch training and phishing simulations via LMS; formalize JML process with quarterly access reviews	Do
Physical Controls (A.7)	Entry Controls, Environmental Safety, Asset Disposal	HQ has guards and logs; hubs less controlled; no secure disposal process	Inconsistent physical access across sites; no documented disposal procedure	PC	Standardize entry controls (badges, CCTV, visitor logs); implement secure disposal (shredding, media wiping)	Do
Technological Controls (A.8)	Access Control (RBAC/MFA), Cryptography, VLANs, Logging, DR	- MFA only for admins; no RBAC model	No cryptography encryption for site	NC		DO

6.4. Strengths

Despite the identified gaps, ARRO (Pvt) Ltd demonstrates several existing strengths that provide a solid foundation for building an ISO/IEC 27001:2022–compliant ISMS:

1. Cloud Infrastructure (AWS)
    - Core platforms (e-commerce, payments, logistics) are hosted on AWS Cloud, benefiting from built-in resilience, data center security, and scalable resources.
    - AWS-native security services (basic encryption, IAM, automated backups) are already in use.
2. Multi-Factor Authentication (MFA) for Administrators

- MFA is enabled for administrator accounts on critical systems, reducing the risk of unauthorized privileged access.

3. Basic Encryption in Place
    - Databases and storage buckets on AWS have baseline encryption enabled, providing an initial layer of protection for sensitive information.
4. Vendor & Supplier Governance (Partially Established)
    - Contracts exist with key suppliers and vendors, covering basic service delivery terms, which can be expanded into formal security clauses and SLAs.
5. Operational Awareness
    - Management acknowledges security risks (fraud, ransomware, insider threats) and has initiated a gap analysis exercise, showing top-level buy-in for an ISMS.
6. Backup & Redundancy
    - Automated backups for customer and transaction data exist within AWS services, forming a foundation for a future Business Continuity/DR strategy.
7. Dedicated ISMS Project Team
    - A cross-functional project team (documentation specialist, lead consultant, analyst, stakeholders) has been established, ensuring shared responsibility for ISMS implementation.

6.5. Weaknesses

The Gap Analysis revealed several weaknesses and non-conformities in ARRO's current information security posture. These represent priority areas that must be addressed to align with ISO/IEC 27001:2022:

1. Information Security Policy and Governance
    - No formally approved or communicated Information Security Policy.
    - Absence of an ISMS Steering Committee or defined roles and responsibilities for security.
2. Risk Management Deficiencies
    - No structured risk assessment methodology or risk register in place.
    - Lack of risk treatment objectives and measurable ISMS performance indicators.
3. Access Control Weaknesses
    - No RBAC (Role-Based Access Control) framework; excessive privileges granted.
    - MFA coverage limited only to administrators; not extended to all employees or customers.

4. Cryptography and Data Protection
    - No formal Cryptography Policy or documented key management process.
    - Existing AWS encryption not monitored or centrally controlled.
5. Supplier and Third-Party Security
    - Supplier contracts lack security clauses and SLAs for patching, incident reporting, and uptime.
    - No formal supplier re-validation or third-party due diligence.
6. Physical Security Gaps
    - Security controls (guards, logs, CCTV) exist only at headquarters.
    - Distribution hubs and logistics centers lack consistent physical access management.
7. Monitoring and Incident Response
    - No centralized logging or SIEM solution.
    - Absence of a formal Incident Response Plan (IRP) or defined reporting/escalation procedures.
8. Business Continuity & Disaster Recovery (BCP/DR)
    - Backups exist but no documented RTO/RPO objectives or tested DR plans.
    - No regular continuity exercises (e.g., failover or tabletop drills).
9. People & Awareness
    - No structured training and awareness program.
    - Weak Joiner-Mover-Leaver (JML) process for revoking access after termination.

6.6. Current Security Posture

ARRO's security posture can be described as technically strong but managerially weak. While reliance on AWS cloud infrastructure and MFA provides resilience at a technical level, the absence of formal ISMS governance, risk management, and business continuity planning leaves ARRO highly exposed to threats such as ransomware, and data breaches.

The PDCA mapping shows that:

- Planning gaps exist in governance, leadership, and risk management.
- Do gaps exist in operational controls, supplier management, access control, and incident response.
- Check gaps exist in performance monitoring and internal audits.
- Act gaps exist in business continuity and continual improvement.

This demonstrates that ARRO's ISMS maturity is low, and improvements are needed across all stages of PDCA to reach ISO/IEC 27001:2022 compliance.

6. Risk Assessment

6.1. Methodology

The risk assessment was conducted using an asset–threat–vulnerability mapping approach, aligned with ISO/IEC 27001:2022 Clause 6 (Planning) and supported by ISO/IEC 27002:2022 guidance. Risks were assessed based on:

- Asset – Valuable information or system (e.g., customer database, payment system).
- Threat – Potential cause of an unwanted incident (e.g., ransomware, fraud, insider misuse).
- Vulnerability – Weakness that could be exploited (e.g., lack of access reviews, no incident response plan).
- Impact – Consequences to confidentiality, integrity, or availability (rated Low, Medium, High, Very High).
- Likelihood – Probability of occurrence (Low, Medium, High).
- Risk Level – Combined severity from impact and likelihood.
- Treatment Recommendation – Proposed mitigation measures mapped to ISO/IEC 27001 Annex A controls.
- PDCA Stage – Where the risk treatment action belongs in the ISMS lifecycle.

6.2. Initial Risk Register

Table 6-1 – Initial Risk Register for ARRO (Pvt) Ltd

Risk ID	Asset	Threat / Vulnerability	Impact	Likelihood	Risk Level	Treatment Recommendation	Relevant Annex A Controls	PDCA Stage
R1	Customer Database	Unauthorized access due to weak access governance	Very High	Medium	High	Enforce RBAC, MFA for all privileged accounts, encrypt data at rest/in transit, quarterly access reviews	A.5, A.8, A.12	Plan / Do

R2	Payment Systems	Fraudulent transactions from insufficient monitoring	High	Medium	High	PCI DSS alignment, anomaly detection, segregation of duties (SoD), daily reconciliation	A.8, A.12, A.13	Do
R3	Vendor Portal	Fake seller onboarding (weak verification)	High	Medium	High	KYC/AML-style verification, contractual security clauses, periodic re-validation	A.5, A.15	Plan / Do
R4	Logistics Platform	Ransomware attack on unpatched systems	High	Medium	High	Patch SLAs, EDR, network segmentation, immutable backups, IR drills	A.12, A.16, A.17	Do / Act
R5	Employee Data	Insider misuse due to excessive privileges	Medium – High	Low–Medium	Medium – High	Implement Joiner-Mover-Leaver (JML) process, DLP, quarterly access recertifications	A.5, A.8	Do
R6	Cloud Infrastructure (AWS)	DoS attacks or misconfigurations causing downtime	High	Medium	High	AWS Shield, Auto Scaling, multi-region redundancy, IaC guardrails, DR testing	A.12, A.17	Act

6.3. Risk Assessment Summary

The assessment shows that ARRO faces multiple high-level risks, especially related to data breaches, fraudulent transactions, fake vendors, ransomware, and cloud downtime. These risks threaten:

- Financial stability (fraud losses, recovery costs).
- Regulatory compliance (violations of PDPA and PCI DSS).
- Operational continuity (logistics and e-commerce service disruptions).
- Reputation (loss of customer/vendor trust).

By mapping treatments to the PDCA cycle, ARRO can ensure a structured path to risk reduction:

- Plan – Establish policies, governance, risk methodology (R1, R3).
- Do – Implement technical and operational controls (R2, R4, R5).

- Check – Regularly monitor controls through audits and reviews.
- Act – Improve resilience through BCP, DR testing, and continual improvement (R4, R6).

7. Risk Treatment Recommendations

The risk assessment (Section 7) identified multiple high-priority risks to ARRO's information assets, processes, and infrastructure. This section outlines the treatment recommendations for each risk, aligned with Annex A controls of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 implementation guidance. Recommendations are also mapped to the PDCA cycle to support continual improvement.

8.1. Employee Security Policies

- Acceptable Use Policy (AUP): Employees must follow secure practices when using ARRO systems.
- Multi-Factor Authentication (MFA): Mandatory for administrators and all staff with privileged access.
- Joiner–Mover–Leaver (JML) Policy: Ensure access rights are granted, updated, or revoked promptly.
- Confidentiality Agreement: All employees must sign NDAs and comply with PDPA obligations.
- Security Awareness Policy: Induction + quarterly refresher training, including phishing simulations.

8.2. Vendor/Supplier Security Policies

- Vendor Onboarding Policy: All vendors must undergo identity verification (KYC/AML-style checks).
- Supplier Security Agreement: Contracts must include security clauses (data protection, breach notification, compliance).
- Vendor Access Control Policy: Limit and monitor vendor access to ARRO systems.
- Re-Verification Policy: Periodic vendor re-validation to prevent fake seller accounts.

8.3. Customer Security Measures

- Introduce Optional MFA: Enable MFA for customer accounts to reduce account takeover risks.
- Password Security: Enforce strong passwords and provide reset reminders.
- Transaction Verification: Apply OTPs for high-value or unusual transactions.
- Fraud Analytics: Monitor for suspicious activities in real-time.

8.4. Risk Treatment Plan

Table 7-1 – Risk Treatment Plan for ARRO (Pvt) Ltd

Risk ID	Key Issue	Treatment Recommendation	Annex A Controls	PDCA Stage	Responsible Owner	Residual Risk
R1	Customer DB breach (weak access control)	Enforce RBAC, MFA for privileged accounts, encryption, quarterly access reviews	A.5, A.8, A.12	Plan / Do	Head of Engineering	Medium
R2	Payment fraud	PCI DSS compliance, anomaly detection, SoD, daily reconciliation	A.8, A.12, A.13	Do	CFO + Payments Lead	Medium
R3	Fake vendor accounts	KYC verification, contractual clauses, re-verification	A.5, A.15	Plan / Do	Vendor Operations Manager	Low
R4	Ransomware (logistics downtime)	Patch SLAs, EDR, network segmentation, immutable backups, IR drills	A.12, A.16, A.17	Do / Act	IT Operations Lead / IT Manager	Low
R5	Insider misuse (employee data)	JML process, DLP solutions, quarterly recertifications	A.5, A.8	Do	HR + IT Security	Low
R6	DoS attacks (cloud infra)	AWS Shield, Auto Scaling, multi-region redundancy, DR tests	A.12, A.17	Act	Cloud Platform Lead	Low

8.5. Treatment Summary

The proposed treatments address ARRO's most critical risks by:

- Establishing governance (policies, responsibilities, supplier agreements).
- Enforcing technical safeguards (MFA, encryption, monitoring, fraud analytics, AWS resilience).
- Implementing operational measures (patch management, backups, incident response).
- Building a culture of awareness and accountability among employees, vendors, and customers.

By implementing these measures within the PDCA framework, ARRO will move toward compliance with ISO/IEC 27001:2022, strengthen regulatory alignment with PDPA and PCI DSS, and enhance resilience against cyber threats.

8. Step-by-step Plan to Address Gaps

9.1. Purpose and Prioritization

This roadmap translates the gap analysis into a sequenced, actionable plan for ARRO (Pvt) Ltd. It is aligned with ISO/IEC 27001:2022 Clauses 4–10 and Annex A controls, and informed by ARRO's business scope (e-commerce, payments, logistics on AWS, corporate operations). Steps are prioritized based on business impact and feasibility:

- P1 (0–3 months): Establish governance and close urgent gaps
- P2 (3–6 months): Roll out controls, training, continuity testing
- P3 (6–12 months): Audit, management review, certification readiness

9.2 Key Gaps to Close

No Information Security Policy or defined ISMS roles (Clause 5, Annex A.5–A.6)

No risk methodology, risk register, or measurable objectives (Clause 6)

No Incident Response or Business Continuity Plans (Annex A.16, A.17)

Weak supplier onboarding and contractual security (Annex A.15)

Limited employee training and awareness (Clause 7)

Missing internal audit and management review (Clauses 9–10)

Weak access governance, patch management, monitoring, and secure development (Annex A.8, A.12, A.14)

9.3. Roadmap Table

Table 8-1 – Gap Closure Roadmap for ARRO (Pvt) Ltd

Step	Action	ISO Ref	PDCA	Priority	Deliverables	Challenges & Mitigation	Success Indicators
1	From ISMS Steering Committee & assign roles	Cl.5, A.6	Plan	P1	ISMS Charter, RACI	Stakeholder delays → short weekly stand-ups	Roles assigned; RACI approved
2	Approve & publish Information	Cl.5, A.5	Plan	P1	IS Policy, policy register	Low adoption → exec memo	≥95% staff attestations

	Security Policy + supporting policies					& LMS onboarding	
3	Define ISMS Scope & Risk Methodology	Cl.4, Cl.6	Plan	P1	Scope Statement, risk criteria	Scope creep → clear in/out of scope list	Scope approved; risk criteria defined
4	Build Asset Register & Risk Register	Cl.6	Plan	P1	Asset Register, Risk Register v1, RTP	Asset owners' time → workshops	100% risk-assessed
5	Close high-risk technical gaps: MFA, RBAC, patch mgmt, SIEM, IR Plan	A.8, A.12, A.16	Do	P1	Access Control Policy, SIEM dashboards, IR Plan	Tooling complexity → start with payments, DB	MFA >90%; SIEM live; IR drill done
6	Strengthening Supplier Onboarding & Contracts	A.15	Do	P1	Supplier Security Standard, updated contracts	Contract updates slow → addenda at renewal	100% new contracts secure; 80% critical vendors re-verified
7	Produce Statement of Applicability (SoA)	Cl.6, Annex A	Plan/ Do	P1	SoA v1.0	Over/under selection → peer review	SoA approved; controls have owners
8	Develop Business Continuity & DR Plan; run test	A.17	Act	P1–P2	BIA, BCP/DR Plan, DR test report	Test downtime → partial pilots	Critical apps meet RTO/RPO
9	Establish Document	Cl.7	Do	P2	Doc Mgmt Procedure,	Doc sprawl → one repository	100% ISMS docs

	Control for ISMS				templates, repo		version-controlled
10	Training & Awareness Program	Cl.7	Do	P2	Training plan, modules, phishing sims	Low engagement → micro-learning	≥95% completion ; phishing fails trending down
11	Performance Evaluation: KPIs, Internal Audit, Management Review	Cl.9–10	Chec k/Act	P2–P3	KPI dashboard, audit reports, review minutes	Auditor independence → cross-functional audits	100% audits complete; ≥90% CAPAs closed
12	Certification Readiness	—	Act	P3	Readiness report, mock audit results	Last-mile gaps → pre-audit sprint	Mock NCs closed; readiness checklist green

9.4. Success Indicators (KPIs - Key Performance Indicator)

To ensure that ARRO's ISMS implementation is effective, a set of Key Performance Indicators (KPIs) will be used. These indicators provide measurable evidence of progress and align with ISO/IEC 27001's PDCA cycle.

Table 8-2 – Success Indicators (KPIs)

Domain	**KPI (Indicator)**	**Target**	**ISO/IEC Ref**
Governance & Policy	% of ISMS roles formally assigned and acknowledged	100%	Clause 5, A.6
	% of staff who signed/acknowledged IS Policy	≥95%	Clause 5, A.5
Risk Management	% of in-scope assets risk-assessed	100%	Clause 6
	% of high-risk items with active Risk Treatment Plans	100%	Clause 6

Access Control (RBAC, MFA)	MFA coverage for all privileged accounts	≥95%	A.8
	% of accounts under Role-Based Access Control (RBAC)	≥90%	A.8
	% of quarterly access reviews completed on time	100%	A.8
Operations Security	% of systems patched within SLA (e.g., 14 days for critical)	≥95%	A.12
	% of systems logging into SIEM	≥90%	A.12
Incident Management	Mean Time to Detect (MTTD)	≤24h	A.16
	Mean Time to Respond (MTTR)	≤48h	A.16
	% of incidents with post-incident review completed	≥90%	A.16
Supplier Security	% of new contracts with security clauses	100%	A.15
	% of critical suppliers re-verified annually	≥80%	A.15
Business Continuity	% of critical services tested against RTO/RPO	100%	A.17
	Annual BCP/DR test completion	1 per year	A.17
Training & Awareness	Employee training completion rate	≥95%	Clause 7
	Phishing simulation failure rate	<10% (decreasing trend)	Clause 7
Audit & Review	% of planned internal audits executed	100%	Clause 9
	Corrective Action closure rate	≥90%	Clause 10
	Annual Management Review completed	Yes/No	Clause 9

9.5. Timeline

The remediation roadmap has been sequenced into three phases over a 6–12-month horizon to balance urgency with feasibility. Activities are aligned with ISO/IEC 27001:2022 requirements and follow the PDCA cycle.

- **P1** (0–3 months) – Establish ISMS foundations and close critical gaps
    - Governance: Form ISMS Steering Committee, assign roles and responsibilities
    - IS Policy: Draft, approve, and communicate the Information Security Policy

- Scope & Risk Register: Define ISMS scope, methodology, and build initial Risk Register
- Statement of Applicability (SoA): Document applicable Annex A controls
- Technical Controls: Enforce MFA, RBAC, patching, and SIEM monitoring
- Incident Response: Publish Incident Response Plan and conduct a tabletop drill
- Supplier Security: Introduce vendor onboarding checks and contractual clauses

- **P2** (3–6 months) – Roll out operational controls and strengthen resilience
  - Training & Awareness: Launch induction and quarterly security training, phishing simulations
  - Business Continuity & DR: Conduct BIA, define RTO/RPO, prepare and test BCP/DR plan
  - Secure Operations: Implement monitoring KPIs, log management, and patch compliance tracking
  - Internal Audit: Establish audit program, execute first round of internal audits
- **P3** (6 months and beyond) – Institutionalize continuous improvement and readiness
  - Management Review: Conduct annual management review covering risks, KPIs, and audit results
  - Corrective Actions: Close identified non-conformities and update SoA/Risk Register
  - Certification Readiness: Run mock audit, prepare evidence packs, finalize readiness checklist

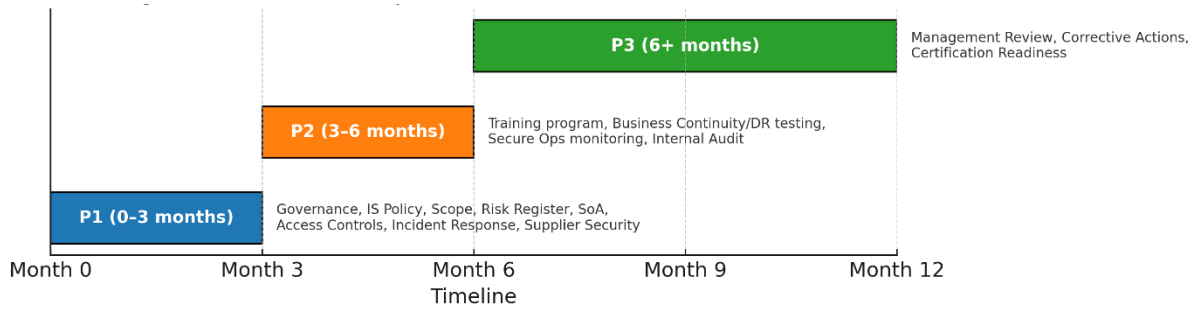

Figure 8-1– ISMS Gap Closure Timeline (At a Glance)

9. Closure

The gap analysis revealed that ARRO (Pvt) Ltd has a strong technical foundation through AWS cloud infrastructure, administrator MFA, and fraud detection mechanisms. However, it also identified significant weaknesses in governance, risk management, incident response, supplier security, and business continuity. These gaps place the organization at risk of data breaches, fraud, operational disruptions, and regulatory penalties under the Sri Lankan PDPA and PCI DSS.

The risk assessment confirmed that the majority of ARRO's risks fall into the high impact and medium likelihood category, requiring urgent treatment. Key risks include unauthorized access to customer data, payment fraud, fake vendor accounts, ransomware, insider misuse, and denial-of-service attacks.

To address these issues, a comprehensive risk treatment plan and a step-by-step roadmap were developed. The plan recommends immediate governance actions (ISMS Steering Committee, Information Security Policy, Scope, and Risk Register), priority technical controls (MFA, RBAC, SIEM, Incident Response, Supplier Security), and medium-term measures (Business Continuity/DR testing, training and awareness, secure development practices). Longer-term actions include internal audits, management reviews, and certification readiness.

By implementing this roadmap within a 90–180 day phased timeline, ARRO will move from non-conformance to certification readiness, aligning with ISO/IEC 27001:2022 requirements. This will not only improve compliance and resilience but also build trust with customers, vendors, and regulators.

In conclusion, closing these gaps will enable ARRO to:

- Strengthen its information security posture,
- Protect sensitive customer and vendor data,
- Ensure business continuity,
- Achieve compliance with PDPA, PCI DSS, and ISO/IEC 27001:2022, and
- Gain competitive advantage in Sri Lanka's growing digital marketplace.

10. List of Acronyms

Acronym	Meaning
ARRO	ARRO (Pvt) Ltd (Company under assessment)
AWS	Amazon Web Services
BCP	Business Continuity Plan
CAPA	Corrective and Preventive Actions

CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, Availability
DB	Database
DLP	Data Loss Prevention
DoS	Denial of Service
DR	Disaster Recovery
IAM	Identity and Access Management
ICT	Information and Communication Technology
IR	Incident Response
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
JML	Joiner–Mover–Leaver (access lifecycle process)
KPI	Key Performance Indicator
KYC	Know Your Customer
LMS	Learning Management System
MFA	Multi-Factor Authentication
MTTD	Mean Time to Detect (average time to identify a threat)
MTTR	Mean Time to Respond (average time to contain/recover from an incident)
NC	Non-Conformant
PC	Partially Conformant
PDCA	Plan–Do–Check–Act (ISO management cycle)
PDPA	Personal Data Protection Act (Sri Lanka)
PCI DSS	Payment Card Industry Data Security Standard
RACI	Responsible, Accountable, Consulted, Informed
RBAC	Role-Based Access Control
RPO	Recovery Point Objective
RTO	Recovery Time Objective

SIEM	Security Information and Event Management
SLA	Service Level Agreement
SoA	Statement of Applicability
SoD	Segregation of Duties
SOP	Standard Operating Procedure
SDLC	Software Development Life Cycle

11. References

ISO/IEC 27001:2022 Standard

Sri Lanka PDPA

PCI DSS