Sri Lanka Institute of Information Technology

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

ISMS Core Documentation Pack - 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. Introduction

The purpose of this Information Security Management System (ISMS) Core Documentation Pack is to define the policies, scope, roles, and control framework that enable ARRO (Pvt) Ltd to protect its critical information assets. The pack serves as the foundation for implementing and maintaining an ISMS aligned with ISO/IEC 27001:2022, covering organizational, people, physical, and technological controls.

ARRO operates in the e-commerce, logistics, and payment services sectors, relying heavily on digital platforms and cloud infrastructure (AWS). Given the sensitive nature of its customer, vendor, and employee data, ARRO is exposed to multiple risks, including data breaches, payment fraud, ransomware, insider misuse, and service disruptions. This documentation provides a structured response to these risks by embedding security policies, risk management processes, and governance responsibilities within the organization.

The ISMS Core Documentation Pack is organized into the following major components:

- Scope Statement – Defines the boundaries, in-scope business processes, and risk acceptance criteria.
- Information Security Policy – Declares ARRO’s commitment to confidentiality, integrity, availability, and compliance obligations.
- Statement of Applicability (SoA) – Maps Annex A controls, with justification for inclusion/exclusion and implementation status.
- Risk Management Framework – Outlines risk assessment methodology, register, and treatment approach.
- Roles & Responsibilities – Assigns accountability for ISMS governance, control ownership, and compliance.
- Control Categories (Annex A) – Structured into Organizational (A.5), People (A.6), Physical (A.7), and Technological (A.8) controls.
- Monitoring, Evaluation & Continual Improvement – Defines KPIs, audits, management reviews, and corrective actions.

This document is mandatory for all employees, contractors, and relevant third parties who interact with ARRO’s information assets. It is also the primary reference point for internal audits, external certification, and regulatory inspections. By adopting this framework, ARRO strengthens its security posture, ensures compliance with Sri Lanka PDPA, PCI DSS, and fosters trust with customers, vendors, and stakeholders.

2. ISMS Scope Statement

2.1. Purpose of ISMS

The purpose of this scope statement is to define the boundaries and applicability of the Information Security Management System (ISMS) at ARRO (Pvt) Ltd, ensuring a structured approach to managing information security risks in line with ISO/IEC 27001:2022 requirements.

2.2. Boundaries (in-scope processes, systems, locations)

The ISMS applies to all business functions and processes that handle information critical to ARRO's operations, including:

- **E-commerce platforms** – ARRO Mall and ARRO Live (customer ordering, product management, vendor interactions)
- **Payment systems** – online payments, mobile wallets, card transactions, bank transfers, and cash-on-delivery settlements
- **Logistics operations** – ARRO Express (warehousing, distribution hubs, last-mile delivery)
- **Corporate operations** – HR, payroll, employee data, legal, compliance, and finance functions
- **Cloud infrastructure** – AWS-hosted services, databases, applications, backups, and networking components

2.3. Physical Scope

The ISMS covers the following locations:

- Headquarters (Colombo) – corporate and administrative operations
- Regional distribution hubs and logistics centers
- Cloud environments hosted on AWS, irrespective of physical server location

2.4. Information Assets in Scope

- Customer data (personal and financial information)
- Vendor/supplier records and contracts
- Employee HR records and payroll information
- Financial transaction records and audit logs
- Application source code, system configurations, and cloud assets

2.5. Out-of-scope areas

The ISMS does not cover:

- **Third-party systems and infrastructure** not managed or controlled by ARRO (e.g., third-party logistics providers or independent vendor IT systems), except where such systems integrate with ARRO's platforms under formal contracts.
- **Personal devices** (BYOD) unless enrolled in ARRO's mobile device management (MDM) program.

2.6. Risk acceptance criteria

Risks rated as Low after assessment may be accepted by management, provided they are documented and reviewed periodically.

Medium and High risks require treatment via technical, organizational, or procedural controls as defined in the Risk Treatment Plan.

Residual risks are reviewed during management reviews and subject to continual improvement under the PDCA cycle.

2.7. Applicability to Standards and Regulations

This ISMS scope aligns with:

- ISO/IEC 27001:2022 (Clauses 4–10 and Annex A)
- ISO/IEC 27002:2022 implementation guidance
- Sri Lanka Personal Data Protection Act (PDPA)
- PCI DSS v4.0 for payment systems

2.8. Approval

This scope statement is formally approved by ARRO's **Top Management** and will be reviewed annually, or upon significant organizational or environmental changes.

3. Information Security Policy

Commitment from Top Management

The top management of ARRO (Pvt) Ltd is totally dedicated to creating, putting into practice, maintaining, and continuously enhancing the Information Security Management System (ISMS) in compliance with ISO/IEC 27001:2022. Leadership understands that maintaining customer trust, maintaining regulatory compliance, and guaranteeing company continuity all depend on preserving information assets. Consequently, management commits to:

- Support and authorize this information security policy.
- Allocating sufficient financial, human, and technological resources to ISMS projects.
- Information security goals should be incorporated into organizational strategy and decision-making.
- Exhibiting leadership by taking part in audits, improvement initiatives, and ISMS reviews.

- Encouraging all workers and contractors to adopt an information security-aware and accountable culture.

CIA (Confidentiality, Integrity, Availability) Objectives

The CIA triad serves as an essential component of ARRO's information security strategy, and the ISMS is made to support it:

1. **Confidentiality:** Preventing unauthorized access, disclosure, or misuse of private client, vendor, and employee information.
2. **Integrity:** Making certain that information, systems, and procedures continue to be correct, dependable, and shielded from illegal alteration or corruption.
3. **Availability:** Reducing downtime and interruptions by ensuring that vital company systems, e-commerce platforms, payment gateways, and logistics services are always available and operational when needed.

And the specific objectives are:

- Putting strong encryption and access controls in place to safeguard privacy is important.
- Maintaining integrity through validation checks, monitoring systems, and audit trails.
- Implementing catastrophe recovery and business continuity strategies to keep vital operations available.

Compliance with PDPA, PCI DSS, ISO/IEC 27001:2022

ARRO commits to abide by all relevant legal, regulatory, and contractual requirements, such as,

- Sri Lanka Personal Data Protection Act (PDPA), which protects gathered, processed, and stored personal data by guaranteeing lawful processing, user permission, and data subjects' rights.
- PCI DSS v4.0: Protecting payment card information using industry-standard security measures like encryption, robust authentication, and ongoing monitoring.
- The establishment and upkeep of risk-based ISMS in accordance with Annex A controls to fulfill organizational, human, physical, and technology security needs is outlined in ISO/IEC 27001:2022.

External evaluations, internal audits, and ongoing control effectiveness monitoring will all be used to keep an eye on compliance.

Review & Communication

This information security policy will be:

- Reviewed at least annually or whenever there are notable advancements in technology, business, or regulations.
- Interacted with all workers, subcontractors, suppliers, and other parties that handle ARRO's data assets.

- Provided upon request to stakeholders and consumers to show ARRO's dedication to information security.
- Incorporated into awareness-raising training initiatives to guarantee that employees are aware of their roles in safeguarding information assets.

The policy will continue to be a dynamic document that changes in response to new risks, organizational expansion, and legislative modifications.

4. Statement of Applicability (SoA)

The Statement of Applicability (SoA) for ISO/IEC 27001:2022 was prepared to document the applicability and implementation status of controls within ARRO's information security management system. This SoA identifies which controls are conformant (C), partially conformant (PC), non-conformant (NC), or not applicable based on the organization's current operational environment, including the use of external applications, on-site staff, and cloud services. By the end of the third month of the implementation period, all relevant assessments, classifications, and control evaluations were completed, and the SoA was finalized to reflect the current status of policies, procedures, and technical safeguards across organizational, people, physical, and technological domains.

Table 4-1 - Statement of Applicability (SoA) – ISO/IEC 27001:2013 Annex A Controls, Applicability, Implementation Status, Ownership, and Justification

ISO/IEC 27001:2022 SoA		**Applicable (Y/N)**	**Status**	**Owner**	**Implementation Plan / Notes**	**Justification for Non-Applicability**
Area Requirement						
A.5 – Organizational controls						
A.5.1	Policies for information security	Yes	PC	CEO/ Director	Finalize policy, get management approval, publish, communicate to staff, collect acknowledgments	
A.5.2	Information security roles and responsibilities	Yes	PC	IT Manager	Document all roles and responsibilities, assign ownership, communicate to relevant personnel	
A.5.3	Segregation of duties	Yes	NC	Operations Manager	Conflicting duties analysis ongoing; formal segregation procedures not yet applied.	
A.5.4	Management Responsibilities	Yes	PC	CEO/ Director	Continue reinforcing enforcement via quarterly management review meetings,	

					periodic audits, and formal acknowledgment by all department heads	
A.5 .5	Contact with authorities	Yes	PC	IT Manager	Develop formal contact list, assign responsible personnel, establish regular reporting and communication procedures	
A.5 .6	Contact with special interest groups	Yes	NC	IT Manager	Memberships and engagement plan under review.	
A.5 .7	Threat intelligence	Yes	PC	IT Manager	Threat data collection initiated from internal logs and SIEM alerts; plan to integrate external threat feeds and automate analysis by next phase	
A.5 .8	Information security in project management	Yes	C	Operations Manager	Security requirements embedded in project lifecycle templates; all ongoing projects reviewed for compliance	
A.5 .9	Inventory of information and other associated assets	Yes	PC	IT Manager	Initial inventory completed for critical systems and data; full asset registers to be updated and reviewed quarterly	
A.5 .10	Acceptable use of information and other associated assets	Yes	C	IT Manager	Acceptable Use Policy published, communicated, and acknowledged by all personnel	
A.5 .11	Return of assets	Yes	NC	HR Manager	Policy exists but enforcement and tracking asset returns not yet implemented	
A.5 .12	Classification of information	Yes	PC	IT Manager	Initial classification scheme exists; full staff adoption pending.	
A.5 .13	Labelling of information	Yes	PC	IT Manager	Labelling guidelines drafted; implementation ongoing.	
A.5 .14	Information transfer	Yes	PC	IT Manager	Basic secure email/ FTP in place; formal	

					agreements to be established.	
A.5 .15	Access control	Yes	C	IT Manager	RBAC and MFA fully applied; periodic review ongoing.	
A.5 .16	Identity management	Yes	PC	IT Manager	Account creation/deletion process drafted; full audit needed.	
A.5 .17	Authentication information	Yes	C	IT Manager	Password policy in place; multi-factor authentication implemented for all users.	
A.5 .18	Access rights	Yes	PC	IT Manager	Periodic reviews started; full automation pending.	
A.5 .19	Information security in supplier relationships	Yes	PC	Operations Manager	Some suppliers assessed; full supplier base pending.	
A.5 .20	Addressing information security within supplier agreements	Yes	PC	Operations Manager	Standard clauses drafted, rollout to contracts in progress.	
A.5 .21	Managing information security in the information and communication technology (ICT) supply chain	No	-			Organization does not currently have ICT suppliers
A.5 .22	Monitoring, review and change management of supplier services	Yes	PC	Operations Manager	Process drafted; review schedules being set.	
A.5 .23	Information security for use of cloud services	Yes	PC	IT Manager	AWS infrastructure redundancy and basic protections are in place (firewalls, antivirus, backups). Full governance, monitoring, and contractual/cloud security policies are to be rolled out.	

A.5.24	Information security incident management planning and preparation	Yes	PC	IT Manager	Incident Response Plan drafted in; tabletop drill completed. Further role-specific procedures and communication plans being finalized.	
A.5.25	Assessment and decision on information security events	Yes	PC	IT Manager	Basic event logging and monitoring exist; formal categorization and escalation procedures are being implemented.	
A.5.26	Response to information security incidents	Yes	PC	IT Manager	IR procedures documented; active incident response exercises ongoing to ensure readiness	
A.5.27	Learning from information security incidents	Yes	PC	IT Manager	Post-incident review process defined but not consistently applied. Integration into internal audit and training cycles planned.	
A.5.28	Collection of evidence	Yes	PC	IT Manager	Draft chain-of-custody process exists. Staff training and formal adoption scheduled during security training rollout.	
A.5.29	Information security during disruption	Yes	PC	IT Manager	AWS redundancy provides baseline resilience. Formal integration with BCP/DR testing will define security expectations during outages.	
A.5.30	ICT readiness for business continuity	Yes	PC	IT Manager	Draft BCP/DR plan exists. Business Impact Analysis (BIA) and recovery objectives to be completed and tested in upcoming phase.	
A.5.31	Legal, statutory, regulatory and contractual requirements	Yes	PC	Operations Manager	Regulatory requirements identified. Continuous monitoring and contractual compliance clauses to be verified during	

					vendor and audit programs.	
A.5.32	Intellectual property rights	Yes	PC	Operations Manager	Policies drafted. Awareness training to be delivered, with enforcement mechanisms through internal audits.	
A.5.33	Protection of records	Yes	PC	IT Manager	Backups and access controls applied. Record retention and destruction procedures to be tested and audited.	
A.5.34	Privacy and protection of personal identifiable information (PII)	Yes	PC	IT Manager	Encryption and MFA exist. Formal privacy policy and staff training to be rolled out alongside awareness program.	
A.5.35	Independent review of information security	Yes	NC	IT Manager	Audit framework drafted. First internal audit scheduled in the upcoming cycle.	
A.5.36	Compliance with policies, rules and standards for information security	Yes	C	CEO / Director	Information Security Policy and topic-specific policies have been approved and communicated. Compliance reviews will be integrated into the internal audit program to ensure continual enforcement.	
A.5.37	Documented operating procedures	Yes	PC	IT Manager	Core operating procedures exist informally. Formal documentation and distribution to staff will be done during the secure operations rollout.	
A.6 - People Controls						
A.6.1	Screening	Yes	PC	HR Manager	Basic checks before hiring are done, but process is not fully documented. A formal screening policy will be enforced.	

A.6.2	Terms and conditions of employment	Yes	C	HR Manager	Contracts include confidentiality and security responsibilities. Future updates will ensure alignment with ISMS.	
A.6.3	Information security awareness, education and training	Yes	PC	HR Manager / IT Manager	Staff get basic induction. A full training program with phishing simulations will be launched.	
A.6.4	Disciplinary process	Yes	PC	HR Manager	HR process exists but not IS-specific. A formal disciplinary policy for IS violations will be created and shared	
A.6.5	Responsibilities after termination or change of employment	Yes	C	HR Manager / IT Manager	Offboarding already ensures account deactivation and confidentiality duties continue after employment ends.	
A.6.6	Confidentiality or non-disclosure agreements	Yes	C	HR Manager	NDAs are already signed by all staff. A review cycle will be added.	
A.6.7	Remote working	No	-			ARRO staff work only on-site with company-managed systems. Remote working is not permitted under current business operations.
A.6.8	Information security event reporting	Yes	PC	HR Manager	IT support handles reports informally. A clear reporting channel and guidance for staff will be set up.	
A.7 Physical controls						
A.7.1	Physical security perimeters	Yes	C	Facilities Manager / IT Manager	Access perimeters fully established with signage and controls.	

A.7.2	Physical entry	Yes	C	Facilities Manager	Access cards and entry logs fully operational; reviewed regularly.	
A.7.3	Securing offices, rooms and facilities	Yes	C	Facilities Manager	Access controls, key management, and entry logging are fully implemented	
A.7.4	Physical security monitoring	Yes	C	Facilities Manager / IT Manager	CCTV monitoring and retention procedures fully operational and reviewed periodically	
A.7.5	Protecting against physical and environmental threats	Yes	PC	Facilities Manager	Fire suppression and UPS systems in place; risk assessment and testing schedule to be formalized	
A.7.6	Working in secure areas	Yes	PC	HR Manager / IT Manager	Staff assigned access to secure areas. Awareness training and access reviews planned.	
A.7.7	Clear desk and clear screen	Yes	PC	HR Manager / IT Manager	Policy drafted; staff awareness sessions required for full compliance.	
A7.8	Equipment siting and protection	Yes	C	Facilities Manager / IT Manager	IT and office equipment are properly sited, secured, and protected against environmental and unauthorized access risks.	
A7.9	Security of assets off-premises	No	-			Organization does not allow off-premises processing or storage of information.
A7.10	Storage media	Yes	PC	IT Manager	Media labeling and storage procedures exist; destruction and tracking procedures to be finalized.	
A7.11	Supporting utilities	Yes	C	Facilities Manager	Utilities supporting information processing facilities (power, HVAC, water) are in place, monitored, and maintained to ensure continuous operation.	

A7.12	Cabling security	Yes	PC	IT Manager	Critical cabling routed securely; documentation and periodic review planned.	
A7.13	Equipment maintenance	Yes	C	Facilities Manager / IT Manager	Maintenance procedures for all critical equipment are documented and regularly followed, ensuring operational reliability and security.	
A7.14	Secure disposal or re-use of equipment	Yes	NC	Facilities Manager / IT Manager	Development of formal processes for data wiping, equipment decommissioning, and staff training on secure disposal are under planning.	
A.8 Technological controls						
A.8.1	User end point devices	Yes	NC	IT Manager	Endpoint security measures are insufficient or inconsistently applied; full inventory, patching, and monitoring plan required.	
A.8.2	Privileged access rights	Yes	C	IT Manager / SysAdmin	Privileged access is restricted through enforced RBAC and regular reviews of admin accounts.	
A.8.3	Information access restriction	Yes	PC	IT Manager	Access rights are granted based on least privilege and business need, with documented approval processes.	
A.8.4	Access to source code	No	-			Organization does not develop software in-house; no access to source code occurs.
A.8.5	Secure authentication	Yes	C	IT Manager	MFA is enforced for all critical systems and has been expanded to all user accounts as planned,	

A.8 .6	Capacity management	Yes	NC	IT Manager	Formal capacity planning and monitoring process in place; need to implement resource utilization tracking, thresholds, and reporting to prevent performance or availability issues.	
A.8 .7	Protection against malware	Yes	PC	IT Manager	Antivirus deployed; automated threat detection improvements planned.	
A.8 .8	Management of technical vulnerabilities	Yes	NC	IT Manager	Formal vulnerability management program in place; need to establish regular scanning, patch prioritization, and remediation tracking.	
A.8 .9	Configuration management	Yes	PC	IT Manager	Baseline configurations exist; version control and change management processes being formalized.	
A.8 .10	Information deletion	Yes	NC	IT Manager	No standardized process for secure deletion of sensitive data; formal policies, secure wipe tools, and verification procedures required.	
A.8 .11	Data masking	No	-			No sensitive production data is exposed to third party environments .
A.8 .12	Data leakage prevention	Yes	NC	IT Manager / Security Officer	No formal DLP solution or training in place; need to deploy DLP tools, define policies, and conduct employee awareness training.	
A.8 .13	Information backup	Yes	C	IT Manager	Backup procedures are established, tested periodically, and meet	

					business continuity requirements.	
A.8 .14	Redundancy of information processing facilities	Yes	C	IT Manager	Redundancy mechanisms are implemented and are regularly tested to ensure availability during disruptions.	
A.8 .15	Logging	Yes	NC	IT Manager	Logging exists but is incomplete; gaps in retention, coverage, and regular review. Next steps: Implementing centralized log management, define retention policy, and establish periodic log review process in progress	
A.8 .16	Monitoring activities	Yes	PC	IT Manager / Security Officer	SIEM monitoring in place; KPIs and automated alerts being added.	
A.8 .17	Clock synchronization	Yes	C	IT Manager	NTP services configured for all critical systems; synchronization verified.	
A.8 .18	Use of privileged utility programs	Yes	C	IT Manager / SysAdmin	Access to privileged utilities is restricted and monitored; controls applied to all relevant systems.	
A.8 .19	Installation of software on operational systems	Yes	PC	IT Manager / SysAdmin	Procedures exist but enforcement across all systems is ongoing and formalizing approval workflow and audit installations in process	
A.8 .20	Networks security	Yes	C	IT Manager / Network Admin	Firewalls, segmentation, and monitoring in place; continuous improvement through patching and configuration management.	

A.8 .21	Security of network services	Yes	PC	IT Manager / Network Admin	Security mechanisms defined and implemented; SLA agreements for service levels are in progress.	
A.8 .22	User end point devices	Yes	C	Network Admin	VLANs and access controls implemented for segregating user groups and services.	
A.8 .23	Web filtering	Yes	C	IT Manager	Web filtering policies and controls deployed; ongoing review and tuning	
A.8 .24	Use of cryptography	Yes	PC	IT Manager / Security Officer	Cryptographic rules defined; key management procedures are being rolled out and staff trained.	
A.8 .25	Secure development life cycle	No				No in-house software development; only third-party applications used.
A.8 .26	Application security requirements	Yes	PC	IT Manager	Security requirements for externally developed applications have been defined and agreed with the development team; full coverage across all deployed systems planned during rollout.	
A.8 .27	Secure system architecture and engineering principles	Yes	PC	IT Manager / Security Officer	Basic secure architecture guidelines exist; full implementation planned.	
A.8 .28	Secure coding	No	-			Organization uses third-party software only; no internal coding occurs.

A.8.29	Security testing in development and acceptance	Yes	NC	IT Manager / Security Officer	Security testing not yet integrated into all development and acceptance processes; plans include automated and manual testing adoption.	
A.8.30	Outsourced development	Yes	PC	IT Manager	Outsourced development agreements exist; security requirements to be strengthened and enforced.	
A.8.31	Separation of development, test and production environments	Yes	PC	IT Manager	Environments are logically separated; formal policies and monitoring to be implemented.	
A.8.32	Change management	Yes	PC	IT Manager / SysAdmin	Basic change management process exists; full workflow, approval, and logging to be formalized.	
A.8.33	Test information	No	-			IT Manager Test data handling procedures are not applicable as no sensitive or production data is used in testing environments
A.8.34	Protection of information systems during audit testing	Yes	PC	IT Manager / Security Officer	Audit access protocols exist; additional monitoring and formal agreements with auditors to be implemented.	

Table 4-2 Statement of applicability summary

Area	Number of ISO/IEC 27001 Controls	Number of Applicable Controls	% Controls Applicable	Number of Applicable Controls Implemented	% Applicable Controls Implemented
A.5 Information security policies	37	36	97.3%	5	13.9%
A.6 Organization of information security	8	7	87.5%	3	42.9%
A.7 Physical controls	14	13	92.8%	7	53.9%
A.8 Technological controls	34	29	85.3%	9	31%

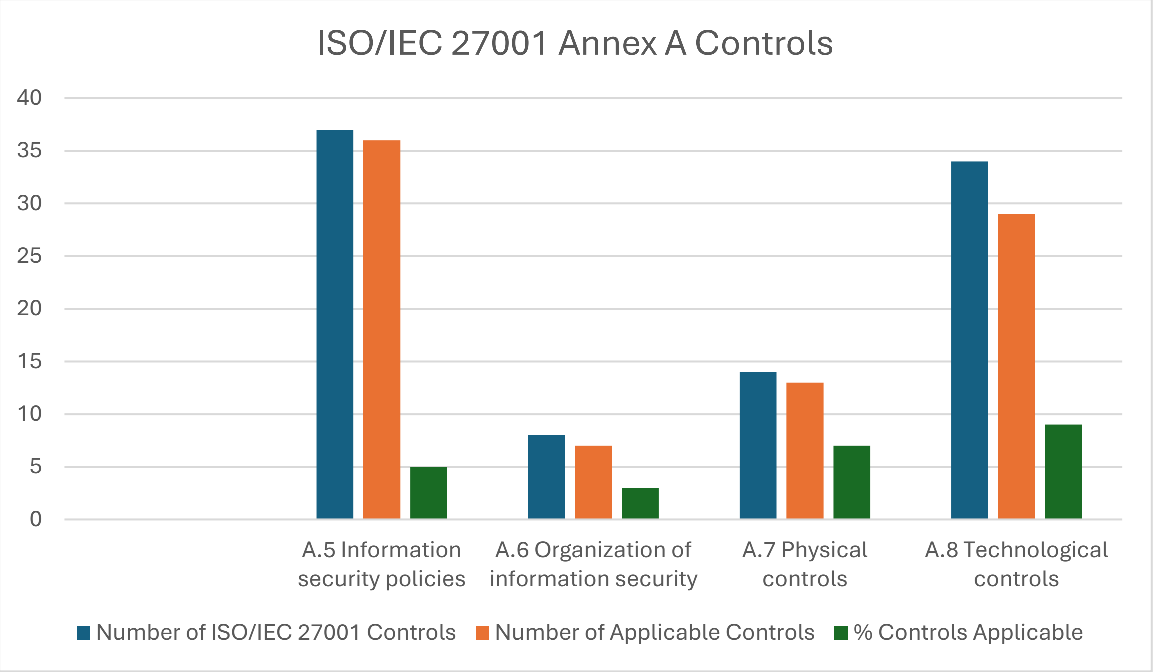

Figure 4-1- ISO/IEC 27001 Annex A Controls – Comparison of Total Controls, Applicable Controls, and Percentage Applied across Organizational, People, Physical, and Technological categories.

5. Risk Management Framework

5.1. Risk Assessment Methodology

ARRO's risk assessment approach follows ISO/IEC 27001:2022 Clause 6 (Planning) and is grounded in an asset–threat–vulnerability mapping model identified during the gap analysis.

Each risk was evaluated in terms of its likelihood and impact on the confidentiality**,** integrity**,** and availability **(**CIA**)** of critical assets such as the customer database, payment systems, vendor portal, logistics platform, cloud infrastructure, and employee records.

The process applied was:

1. Asset Identification – All in-scope assets (customer, vendor, payment, employee, and logistics data hosted on AWS).
2. Threat Mapping – Key threats included ransomware, fraudulent transactions, unauthorized access, fake vendor accounts, and denial-of-service (DoS) attacks.
3. Vulnerability Assessment – Weak access governance, lack of incident response plans, and weak vendor onboarding processes were highlighted.
4. Risk Evaluation – Risks rated using a Likelihood × Impact matrix (Low–High scale).
5. Risk Level Derivation – Overall severity categorized into High, Medium–High, or Medium.
6. Treatment Mapping – Controls aligned with Annex A were proposed (e.g., MFA, RBAC, DLP, patch management, vendor KYC, AWS Shield).
7. Integration with PDCA – Risks were linked to the Plan**,** Do**,** Check**,** Act stages to ensure continual monitoring and improvement.

This structured methodology ensures that ARRO's high-impact risks—such as customer database breaches, payment fraud, fake vendor onboarding, ransomware in logistics, insider misuse, and DoS attacks—are consistently identified, prioritized, and treated.

5.2. Risk Register (ARRO v1)

ID	Asset	Threat / Vulnerability	Likelihood	Impact	Risk Level	Treatment Summary
R1	Customer Database	Unauthorized access from weak access governance	Medium	Very High	High	Enforce RBAC, MFA (privileged), encrypt at rest/in-transit, quarterly access reviews (A.5, A.8, A.12)
R2	Payment Systems	Fraud from insufficient monitoring / SoD gaps	Medium	High	High	PCI alignment, anomaly detection, segregation of duties, daily reconciliation (A.8, A.12, A.13)

R3	Vendor Portal	Fake seller onboarding due to weak verification	Medium	High	High	KYC/AML-style checks, security clauses, periodic re-verification (A.5, A.15)
R4	Logistics Platform	Ransomware via unpatched systems	Medium	High	High	Patch SLAs, EDR, segmentation , immutable backups, IR drills (A.12, A.16, A.17)
R5	Employee Data	Insider misuse from excessive privileges	Low–Medium	Medium–High	Medium–High	JML process, DLP, quarterly access recertifications (A.5, A.8)
R6	AWS Cloud	DoS/misconfig causing downtime	Medium	High	High	AWS Shield, Auto Scaling, multi-region DR testing (A.12, A.17)

5.3. Risk Treatment Plan

Reduce each priority risk to an acceptable residual level by implementing targeted governance, technical, and operational controls mapped to Annex A and placed on the PDCA track for verification

Risk ID	Key Issue	Treatment Actions (mapped to Annex A)	PDCA	Owner	Target Residual
R1	Customer DB breach (weak access control)	RBAC with least-privilege; MFA for admins; DB encryption; quarterly access reviews (A.5, A.8, A.12)	Plan/Do	Head of Engineering	Medium
R2	Payment fraud	PCI DSS alignment; anomaly detection; SoD; daily reconciliation (A.8, A.12, A.13)	Do	CFO + Payments Lead	Medium
R3	Fake vendor accounts	KYC verification; security clauses in contracts; periodic re-verification (A.5, A.15)	Plan/Do	Vendor Ops Manager	Low
R4	Ransomware downtime	Patch SLAs; EDR; network segmentation; immutable backups;	Do/Act	IT Ops Lead	Low

		IR drills (A.12, A.16, A.17)			
R5	Insider misuse (employee data)	JML process; DLP; quarterly access recertifications (A.5, A.8)	Do	HR + IT Security	Low
R6	DoS on cloud infra	AWS Shield; Auto Scaling; multi-region redundancy; DR tests (A.12, A.17)	Act	Cloud Platform Lead	Low

The gap analysis produced a risk treatment plan directly mapped to Annex A controls and ARRO's operational context. Treatments focus on governance, technical safeguards, and awareness:

- Customer Database (R1) – Enforce Role-Based Access Control (RBAC), extend MFA to all privileged accounts, apply data encryption, and mandate quarterly access reviews.
- Payment Systems (R2) – Implement fraud detection analytics, segregation of duties, and daily reconciliation aligned with PCI DSS.
- Vendor Portal (R3) – Introduce KYC/AML-style onboarding, security clauses in contracts, and annual vendor re-verification.
- Logistics Platform (R4) – Enforce patch SLAs, EDR solutions, and immutable backups, with routine incident response (IR) drills for ransomware preparedness.
- Employee Data (R5) – Apply a Joiner-Mover-Leaver (JML) process, deploy DLP solutions, and enforce quarterly access recertification.
- AWS Cloud Infrastructure (R6) – Adopt AWS Shield, auto-scaling, and multi-region redundancy, supported by annual disaster recovery (DR) testing.

Each treatment was assigned to a responsible owner (e.g., Head of Engineering, CFO, Vendor Ops Manager, Cloud Lead) with residual risk levels reduced to Medium or Low.

6. Roles & Responsibilities

6.1. Management

Responsibilities:

- Give approval and support for the information security policy and its implementing protocols.
- Ensure alignment with company objectives and demonstrate leadership commitment for the ISMS implementation.
- Provide the financial, technical, and human resources required for information security projects.
- Track ISMS performance using internal audit results, KPIs, and management evaluations.

- Verify that the organization complies with the PDPA, PCI DSS, ISO/IEC 27001:2022, and other relevant laws.

6.2. ISMS Steering Committee

Responsibilities:

- Supervise the application of ISMS in all business divisions and vital operations.
- Maintain RACI matrices and specify roles and responsibilities for information security governance.
- Examine risk assessments, authorize strategies for risk treatment, and track the status of remediation.
- Organize management evaluations, gap closing initiatives, and recurring internal audits.
- Monitor the ISMS roadmap's development and make sure that policies, practices, and controls are always being improved.

6.3. IT Manager

Responsibilities:

- Oversee IT operations and ensure alignment with ISMS policies.
- Implement and maintain technical security controls, including access management and patching.
- Monitor systems and coordinate incident response with the Security Officer.
- Support risk assessments and implement IT-related controls.
- Maintain IT documentation for audits and compliance.
- Collaborate with the Steering Committee and Security Officer to support ISMS initiatives.

6.4. Security Officer

Responsibilities:

- Keep the information security policy and procedures up to date and distribute them.
- Maintain the Risk Register, carry out routine risk assessments, and keep an eye on high- and medium-risk treatments.
- Supervise the use of technical, operational, and physical security controls.
- Document security events, direct incident response, and assist with post-event evaluations.
- Create, organize, and record information security awareness and training initiatives for employees.

6.5. Risk Owners & Control Owners

Responsibilities:

- Determine, evaluate, and record the risks connected to the departments, procedures, or assets they have been given.
- Effectively implement, oversee, and maintain the designated Annex A controls.

- Verify that the Risk Treatment Plan is followed when implementing high- and medium-risk treatment plans.
- Maintain proof of control efficacy for management reviews, audits, and compliance checks.
- Work together with the Steering Committee and ISO to address new risks and encourage ongoing risk reduction.

6.6. Employees & Contractors

Responsibilities:

- Adhere to the standards, protocols, and information security policies.
- Participate in awareness campaigns and finish the required security training.
- Quickly report any suspicious activity, security problems, or policy infractions.
- Prevent unwanted access to or disclosure of private clients, vendors, and business data.
- Adhere to acceptable usage policies (AUP), password management, access control, and other operational security protocols.

7. Document Control & Records Management

The integrity of ARRO's Information Security Management System (ISMS) depends on efficient document control and records management. This framework protects against unauthorized alteration or loss while guaranteeing that policies, procedures, risk registers, and other ISMS artefacts stay up-to-date, correct, and available to authorized stakeholders in compliance with ISO/IEC 27001:2022 Clause 7.5.

Versioning

- A unique document ID, title, author, and version number must be included with every ISMS document.
- Version numbers will be in the Major. Minor format (e.g., 2.1), where major updates reflect significant changes. and minor updates indicate editorial or clarifying modifications
- The type of alteration, the date of the change, and the approver's signature must all be recorded in change logs.

Approval

- The ISMS Steering Committee will peer-review draft materials before they are forwarded to upper management.
- The CEO will formally provide approval, which will be recorded in the approval register.
- Until an ISMS document is properly approved and made available via the Document Control System (DCS), it is not considered valid.

Retention & Archival

- The retention and archival are kept for a minimum of five years, or longer if required by law or contract, ISMS records including audit reports, risk assessments, training logs, and incident reports must also be kept until the specified retention period.
- Versions that have been superseded are stored with the designation as "superseded" and are available for use as a reference in audits and inquiries.
- Archival records must be kept in safe, digital and/or physical repositories that are regulated by access and include integrity protections (e.g., backups and checksums).

Confidentiality & Access Control

- ARRO's information classification scheme (public, internal, confidential, and restricted) will be used to classify documents.
- Using Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC), access permissions are allowed based on need-to-know.
- Sensitive documents (such as incident reports and risk registers) both in transit and at rest will be encrypted.
- Contractors and employees are forbidden to duplicate, reveal, or destroy ISMS records without authorization. Disciplinary actions will be taken for violations.

8. Monitoring & Evaluation

Monitoring and evaluation of the ISMS is important to point out its effectiveness, by spotting weaknesses, and promoting further development. In accordance with ISO/IEC 27001:2022 Clauses 9.1–9.3, ARRO implements a multi-layered assurance architecture that incorporates formal management reviews, internal audits, and key performance indicators (KPIs).

Internal Audit Program

- Internal ISMS audits must be carried out at least once a year and more frequently when significant events occur (like the launch of new cloud services or large incidents).
- The scope of the audit will include adherence to Annex A controls and ISO/IEC 27001:2022 Clauses 4–10.
- Independence is preserved by Assigning audit responsibility to individuals who are not directly involved in the audited process.
- Corrective actions are recorded in the CAPA (Corrective and Preventive Actions) register, and findings are classified as either observation, minor non-conformity, major non-conformity, or conformity.
- The continuous improvement cycle (PDCA) is informed by the results, which are entered into the Risk Register.

KPIs & Success Indicators

Performance indicators offer unbiased proof of ISMS efficacy and risk mitigation. The following KPIs will be monitored by ARRO:

- Mean Time to Detect (MTTD): The average amount of time needed to identify security incidents. For high-severity occurrences, the target is less than 24 hours.
- Mean Time to Respond/Recover (MTTR): The average amount of time needed to contain and recover from incidents. Goal: less than 72 hours.
- Patch SLA Compliance: The proportion of serious vulnerabilities that are fixed within the allotted time frame (e.g., 14 days). Goal: ≥95%.
- Training Completion Rate: The proportion of staff members who finished the yearly required security awareness training. Goal: 100%.
- Audit closure rate: The percentage of corrective actions completed by the predetermined deadline. Goal: 90% or more.

The Security Officer will examine KPI dashboards every month, and Top Management will receive quarterly reports.

Management Review

Formal review meetings shall occur at least once annually

The agenda will include:

- Findings from both external and internal audits
- Progress toward ISMS goals and KPIs
- Current state of risk treatment initiatives and unresolved risks
- Trends in incidents, lessons discovered, and corrective actions
- Obligations for compliance (PDPA, PCI DSS, contractual)
- Opportunities for continuous improvement
- Meeting minutes shall be recorded and kept in the Document Control System.
- The PDCA cycle tracks and implements management decisions (such as resource allocation and policy updates).

9. Continuous Improvement

9.1. Corrective & Preventive Actions (CAPA)

To ensure that weaknesses identified in the gap analysis do not recur, ARRO will formalize a CAPA program:

- Corrective Actions – Immediate fixes such as implementing MFA, publishing an Information Security Policy, and formalizing supplier agreements.

- Preventive Actions – Long-term measures including quarterly phishing simulations, periodic access reviews, secure SDLC practices, and continuous vendor monitoring.

- Tracking & Closure – Each CAPA will be logged, assigned, and monitored via ARRO's ISMS dashboard. Success will be measured using KPIs (e.g., MTTR < 48h, >95% staff trained annually).

9.2. Lessons Learned

ARRO lacked structured mechanisms to capture knowledge from past incidents. The ISMS will institutionalize post-incident reviews and "lessons learned" workshops after major security events or audits. These will feed into:

- Updating policies and procedures (e.g., vendor onboarding, access governance).
- Enhancing resilience (e.g., refining disaster recovery after ransomware tests).
- Raising awareness among staff and management.

This ensures that each incident or non-conformance becomes an opportunity to strengthen defenses rather than a repeat exposure.

9.3. How ARRO Applies the PDCA Cycle

The PDCA cycle (Plan–Do–Check–Act) will serve as ARRO's backbone for continual improvement:

- Plan – Define scope, roles, and policies; conduct risk assessments; build the asset/risk registers.
- Do – Implement risk treatments (MFA, fraud analytics, patching, BCP, vendor KYC).
- Check – Monitor through KPIs (MTTD, MTTR, patch SLA compliance), conduct internal audits, and track CAPA closure rates.
- Act – Perform management reviews, update the SoA and Risk Register, and refine processes after incidents or drills.

By embedding PDCA into its ISMS governance, ARRO will not only meet ISO/IEC 27001:2022 requirements but also maintain resilience against emerging cyber threats while ensuring compliance with PDPA and PCI DSS

10. Appendices

Acronyms & Definitions

Acronym	Meaning
ARRO	ARRO (Pvt) Ltd – Organization 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
EDR	Endpoint Detection and Response
HSM	Hardware Security Module (for key management)
ICT	Information and Communication Technology
IR	Incident Response
IRP	Incident Response Plan
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
JML	Joiner–Mover–Leaver (access management process)
KPI	Key Performance Indicator
KYC	Know Your Customer (vendor onboarding process)
LMS	Learning Management System
MFA	Multi-Factor Authentication
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
NC	Non-Conformant
PC	Partially Conformant
PDCA	Plan–Do–Check–Act (management cycle)
PDPA	Personal Data Protection Act (Sri Lanka)
PCI DSS	Payment Card Industry Data Security Standard
RACI	Responsible, Accountable, Consulted, Informed (roles model)
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
SAST/DAST	Static Application Security Testing / Dynamic Application Security Testing
VLAN	Virtual Local Area Network (network segmentation)