AcmeTech Solutions Pvt. Ltd.

PROJECT

HELIOS

ISO/IEC 27001: 2022

Information Security Management System — GRC Implementation

Scope: Annex A Controls Audit | Gap Analysis | Risk Register | Remediation Roadmap

Document Details

REPORT TITLE	Project Helios — ISO/IEC 27001:2022 GRC Implementation Report
ORGANISATION	AcmeTech Solutions Pvt. Ltd., Lucknow, India
STANDARD	ISO/IEC 27001:2022 (Third Edition)
AUDIT SCOPE	ISMS — SaaS Platform, IT Assets & Support Services
ANALYSIS DATE	01 February 2026
DOCUMENT VERSION	v1.0 — Initial Release
CLASSIFICATION	Academic Use Only — Simulated Data

Project Participants

Kedar Pavaskar
Compliance Analyst & Documentation Lead

Vinay Kumar
Audit Coordinator & Scrum Master

EXECUTIVE SUMMARY

PROJECT HELIOS – ISO/IEC 27001:2022 GRC Implementation

Acme Tech Solutions Pvt Ltd | Simulated Audit | February 2026

Project Helios is a simulated Governance, Risk, and Compliance (GRC) implementation for a mid-sized technology firm. The objective was to audit the organization against **ISO/IEC 27001:2022 Annex A controls**, with Gap Analysis, Risk Register, and design a remediation roadmap.

1. Scope & Organizational Context

The audit covered Acme Tech Solutions Pvt Ltd, a 55-person IT/SaaS firm headquartered in Lucknow, India, operating a hybrid work model on AWS (Mumbai region) as its core cloud infrastructure. The ISMS scope encompassed all information assets supporting SaaS product delivery and client support services, including a customer database, source code repository, endpoint fleet, and third-party SaaS platforms.

2. Key Audit Findings at a Glance

10 Total Assets Inventoried	**8** Risks Identified	**3** High / Critical Risks	**15** ISO Clauses Assessed
0 Clauses Fully Implemented	**12** Clauses Partially Implemented	**3** Clauses Not Implemented	**54.5%** Security Training Coverage

3. Gap Analysis Summary

Of the 15 ISO/IEC 27001:2022 clauses (Clauses 4–10) assessed, none were found to be fully implemented. Twelve are partially implemented and three — Statement of Applicability (6.1.3), Security Awareness Programme (7.3), and Internal Audit (9.2) — remain entirely absent. Critical gaps across Annex A controls include unreviewed privileged account sharing (A.8.9), absence of formal access reviews (A.8.4), and no structured incident response procedure (A.8.35).

4. Remediation Roadmap Highlights

The remediation roadmap is phased across three horizons. Immediate actions (0–30 days) include enforcing MFA on all privileged accounts, deploying EDR across the full endpoint fleet, and appointing an ISMS Manager with documented responsibilities. Short-term actions (30–90 days) cover authoring a Statement of Applicability, launching an all-staff security awareness programme, and establishing a formal access review cycle. Medium-term work (90–180 days) involves implementing a SIEM, formalising the incident response procedure with defined severity levels, and completing an ISO 27001 internal audit. Full certification readiness is projected at 12–18 months with sustained effort.

6. Conclusion

AcmeTech Solutions Pvt Ltd demonstrates a foundational security posture with several technical controls already active. However, the absence of a formal ISMS — evidenced by **zero fully implemented clauses** and three high/critical open risks — represents a material compliance and operational gap. Executing the phased remediation roadmap will significantly reduce risk exposure and position the organization for ISO/IEC 27001:2022 certification.

2. ISO 27001 Overview

2.1 Definition and History

What is ISO 27001?

ISO/IEC 27001 is an internationally recognized standard for Information Security Management Systems (ISMS), developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides a systematic, risk-based approach to managing sensitive information, ensuring its confidentiality, integrity, and availability. Unlike prescriptive controls, ISO 27001 allows organizations to tailor security measures based on their specific risk profile and business context.

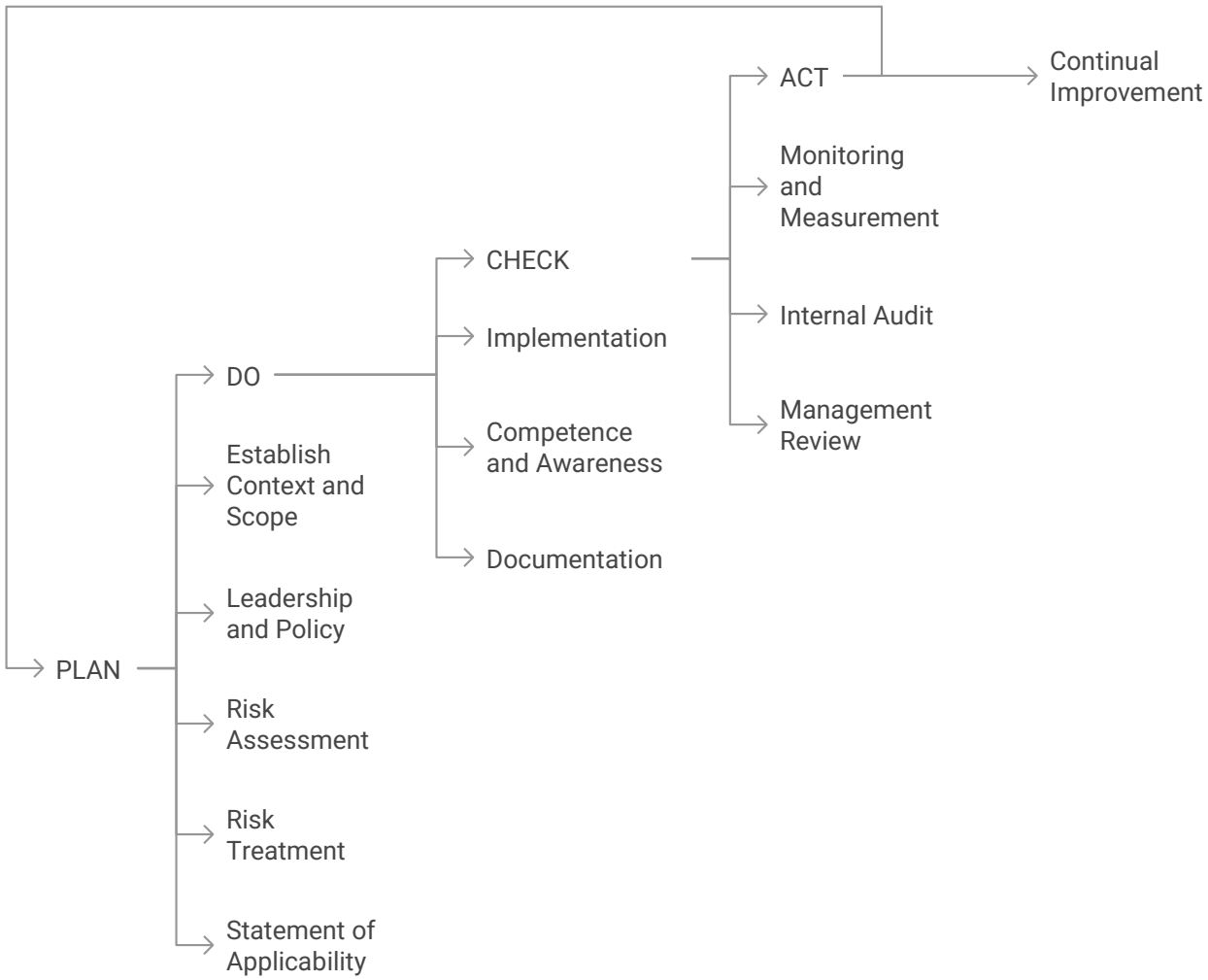
Historical Evolution

Year	Milestone	Significance
1989-1995	UK Department of Trade and Industry develops code of practice; evolves into BS 7799	Foundation of information security management guidelines
1998	BS 7799-2:1998 published	First certifiable standard for information security management
2000	ISO/IEC 17799:2000 adopted	International recognition begins
2005	ISO/IEC 27001:2005 published	First truly international certifiable ISMS standard, replacing BS 7799-2
2013	ISO/IEC 27001:2013 released	Major revision with High-Level Structure alignment; 114 controls across 14 domains
2022	ISO/IEC 27001:2022 current version	Modernized control set with 93 controls across 4 themes (Organizational, People, Physical, Technological); addresses cloud, remote work, supply chain security

The evolution mirrors changing information security landscapes—from physical document protection in the 1990s to today's complex digital ecosystems involving cloud services, AI, and global supply chains.

2.2 How ISO 27001 Works Technically

ISO 27001 operates through the **Plan-Do-Check-Act (PDCA)** cycle, ensuring continuous improvement:



PLAN Phase

Step 1: Establish Context and Scope (Clause 4) – Identify stakeholders, analyze business objectives and regulatory obligations, and define ISMS boundaries (locations, systems, processes, assets).

Step 2: Leadership and Policy (Clause 5) – Top management establishes information security policy aligned with strategic direction and assigns clear roles and responsibilities.

Step 3: Risk Assessment (Clause 6.1.2) – Systematically identify information assets, analyze threats and vulnerabilities, evaluate impact and likelihood, and calculate risk levels using defined criteria.

Step 4: Risk Treatment (Clause 6.1.3) – Select treatment options (modify, retain, avoid, share) and create a Risk Treatment Plan documenting controls, timelines, and responsibilities.

Step 5: Statement of Applicability (SoA) – Document all Annex A controls with applicability status, justification, and implementation references.

DO Phase

Step 6: Implementation (Clause 8) – Deploy selected controls through policies, procedures, technical measures (firewalls, encryption, access controls), and operational processes.

Step 7: Competence and Awareness (Clauses 7.2-7.3) – Ensure personnel competence through training and conduct awareness programs on security responsibilities.

Step 8: Documentation (Clause 7.5) – Create and maintain controlled documentation including scope, policies, risk assessments, SoA, procedures, and records.

CHECK Phase

Step 9: Monitoring and Measurement (Clause 9.1) – Establish processes to monitor security metrics, control effectiveness, and incident trends; analyze results for improvement opportunities.

Step 10: Internal Audit (Clause 9.2) – Conduct periodic audits by competent, objective auditors to verify ISMS conformity and effectiveness; document findings and trigger corrective actions.

Step 11: Management Review (Clause 9.3) – Top management reviews ISMS performance, considering previous actions, external/internal changes, audit results, and improvement opportunities.

ACT Phase

Step 12: Continual Improvement (Clause 10) – Address nonconformities through corrective action, eliminate root causes, and adapt the ISMS to new threats and business changes.

This cyclical process creates a living system that continuously evolves to address the organization's changing risk landscape.

2.3 Target Sectors and Beneficiaries

ISO 27001 is sector-agnostic but particularly critical for certain industries:

Sector	Why ISO 27001 is Critical	Key Drivers
Financial Services	Handle sensitive financial data; frequent cyberattack targets; strict regulatory oversight	Regulatory compliance (PCI DSS, GDPR), customer trust, fraud protection
Healthcare	Manage patient health records; face strict privacy regulations; increasing digitization	HIPAA/GDPR compliance, patient privacy, service continuity, medical IoT security
Technology/SaaS	Store client data; provide critical infrastructure; face constant threats	Customer vendor assurance requirements, competitive differentiation, IP protection
Government/Public Sector	Handle citizen data and critical infrastructure; nation-state attack targets	National security, citizen data protection, public service digitization
Telecommunications	Provide critical communication infrastructure; handle vast customer data	Infrastructure protection, sector regulations, business continuity

Sector	Why ISO 27001 is Critical	Key Drivers
Education	Store student records and research data; increasing cyber threats	Student data protection, research IP safeguarding, reputation management
E-commerce/Retail	Process payments; store customer data; high-volume transaction targets	PCI DSS compliance, customer trust, breach prevention, GDPR compliance
Manufacturing/Critical Infrastructure	Operate critical infrastructure; cyber-physical risks; severe public impact	OT protection, critical infrastructure regulations, supply chain security
Legal/Professional Services	Handle highly confidential client information; professional privilege obligations	Client confidentiality, competitive advantage, professional liability management
Supply Chain/Logistics	Coordinate complex information flows; integrate with multiple parties	Third-party risk management, business partner requirements, competitive positioning

Organization Size Applicability:

- **Small (1-50)**: Streamlined ISMS, cloud services, demonstrates maturity beyond size
- **Medium (51-250)**: Professionalizes security during growth with dedicated resources
- **Large (250+)**: Complex multi-site ISMS coordinating security across business units

Emerging Adoption Areas:

Cryptocurrency/blockchain, AI/machine learning, IoT ecosystems, smart cities

Universal Drivers for ISO 27001:

1. Regulatory compliance and contractual obligations
2. Customer security assurance requirements
3. Systematic risk management
4. Competitive market differentiation
5. Operational efficiency through standardization
6. Business continuity and resilience
7. Third-party assurance for partners/investors
8. Security culture transformation

The standard's risk-based approach makes it scalable and adaptable—organizations implement controls proportionate to their specific risks, regardless of sector, size, or location. This universality, combined with international recognition, makes ISO 27001 the gold standard for information security management worldwide

ISO 27001 Real Case Studies (2023-2024)

Case Study 1: MGM Resorts Ransomware Attack

Field	Details
Organization Name	MGM Resorts International
Date	September 2023
Industry	Hospitality and Gaming
What Happened	MGM Resorts experienced a sophisticated ransomware attack carried out by the ALPHV/BlackCat group. The attackers gained initial access through social engineering techniques, specifically vishing (voice phishing), where they impersonated an employee to the IT help desk. Once inside the network, they deployed ransomware that encrypted critical systems. MGM chose not to pay the ransom and instead took systems offline to contain the breach.
Impact with Numbers	- Estimated financial loss: $110 million - Operations disrupted for approximately 10 days - 150+ properties affected across multiple states - Hotel room key systems, slot machines, ATMs, and reservation systems were non-functional - Customer data potentially compromised (no specific number disclosed) - Stock price dropped 7% in the immediate aftermath
Outcome	MGM refused to pay the ransom and worked with cybersecurity experts and law enforcement to restore systems. The company invested heavily in rebuilding its security infrastructure. The incident highlighted critical gaps in identity management (A.5.16), authentication controls (A.8.5), privileged access management (A.8.2), and incident response capabilities (A.5.24-A.5.27). The attack demonstrated the importance of security awareness training (A.6.3) as the initial breach occurred through social engineering. MGM

	implemented enhanced security protocols and multi-factor authentication across all systems.

Case Study 2: MOVEit Transfer Vulnerability Mass Exploitation

Field	Details
Organization Name	Multiple Organizations (Cl0p ransomware group targeting MOVEit Transfer users - notable victims include Shell, Siemens Energy, Schneider Electric, PwC, EY, BBC, British Airways, and numerous US government agencies)
Date	May-June 2023 (discovery and exploitation)
Industry	Cross-industry (Financial Services, Energy, Professional Services, Government, Aviation, Media)
What Happened	The Cl0p ransomware group discovered and exploited a zero-day SQL injection vulnerability (CVE-2023-34362) in Progress Software's MOVEit Transfer file transfer application. The attackers systematically scanned the internet for vulnerable MOVEit instances and deployed web shells to extract sensitive data before organizations could patch the vulnerability. This was a supply chain attack affecting organizations using the popular file transfer software. The exploitation occurred before the vulnerability was publicly disclosed, giving defenders no warning.
Impact with Numbers	- Over 2,700 organizations affected globally - More than 77 million individuals' personal data compromised - Estimated total cost across all victims: $12+ billion - US federal agencies: 8+ agencies affected - Shell: 80,000+ employees' data exposed - UK government: BBC employees' pension data compromised - Financial services sector particularly impacted with customer financial data at risk
Outcome	Progress Software released emergency patches within days of discovering the vulnerability. However, the damage was extensive as many organizations were already compromised. Affected organizations faced regulatory investigations, particularly under GDPR in Europe and various US state breach notification laws. The incident emphasized critical failures in vulnerability management (A.8.8), supplier security management (A.5.19-A.5.23), technical vulnerability assessment (A.8.8), and secure system architecture (A.8.27). Organizations learned the importance of having robust third-party risk management programs, rapid patch deployment capabilities, and network segmentation (A.8.22) to limit blast radius. Many organizations implemented enhanced monitoring of file transfer systems and moved toward zero-trust architecture principles.

Case Study 3: Capita Data Breach

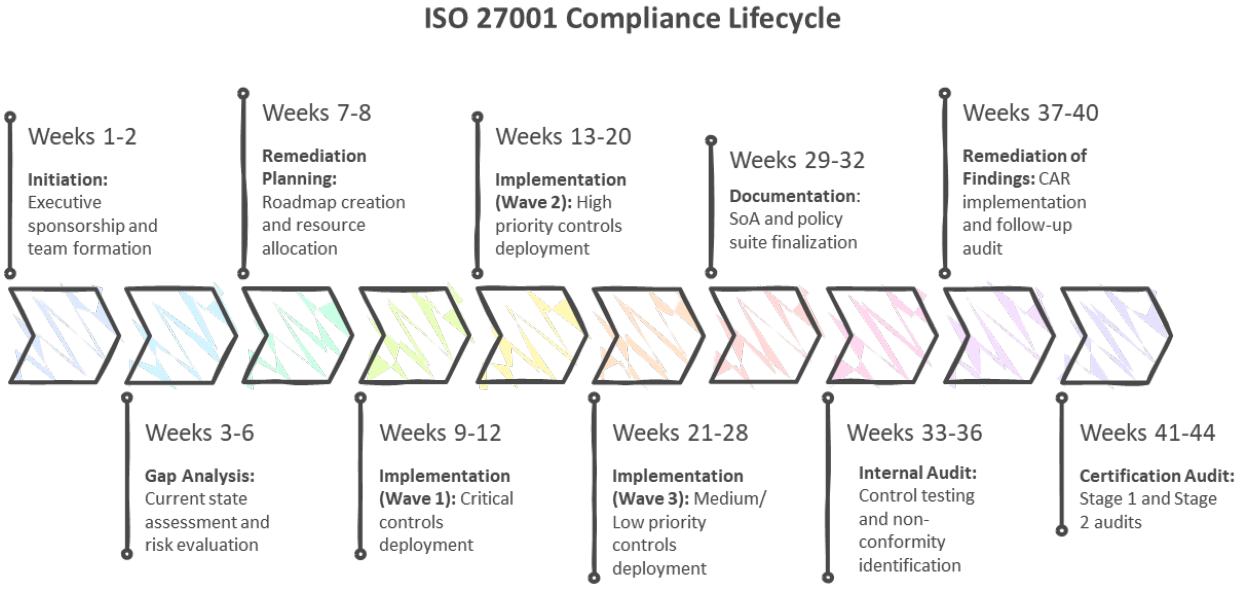
Field	Details

Organization Name	Capita plc
Date	March-April 2023
Industry	Business Process Outsourcing and Professional Services
What Happened	Capita, a major UK outsourcing company providing services to government departments, the NHS, and private sector clients, suffered a significant cyberattack. Attackers gained access to Capita's internal systems and exfiltrated sensitive data belonging to both the company and its clients. The attack was attributed to the Black Basta ransomware group. Capita's Microsoft 365 environment was compromised, affecting email systems and SharePoint repositories. The company took several days to detect the full scope of the breach, and the incident response involved taking multiple systems offline while conducting forensic investigation.
Impact with Numbers	- Direct costs of remediation: £25 million ($31 million) - Total financial impact including lost business: £50+ million ($62+ million) - 90+ client organizations affected - Personal data of potentially millions of individuals compromised (exact number undisclosed) - 4% drop in share price immediately following disclosure - Operations disrupted for approximately 2 weeks - NHS pension services for 1.5+ million members affected - Several UK government department services impacted
Outcome	Capita launched a comprehensive investigation with external cybersecurity experts and notified affected clients and regulatory authorities including the UK Information Commissioner's Office (ICO). The company faced intense scrutiny over its security practices given its role as a trusted service provider to critical infrastructure and government entities. The breach exposed significant deficiencies in network security (A.8.20-A.8.22), access controls (A.5.15-A.5.18), monitoring capabilities (A.8.16), backup systems (A.8.13), and incident detection/response (A.5.24-A.5.26). Capita subsequently invested in a major security transformation program, implementing enhanced encryption, improved access controls, 24/7 security operations center capabilities, and more rigorous third-party security assessments. The incident resulted in contract reviews with several major clients and highlighted the cascading risk when managed service providers are compromised.

3. ISO 27001 compliance Lifecycle Overview

The ISO 27001 compliance lifecycle represents a structured, risk-based approach to establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). This lifecycle follows the Plan-Do-Check-Act (PDCA) methodology, beginning with gap assessment and risk identification, progressing through prioritized remediation phases, and culminating in third-party certification audit. The 11-phase framework spans approximately 44 weeks, organized into three implementation waves that address critical, high-priority, and medium/low-priority controls sequentially.

This phased approach ensures rapid risk mitigation (MFA and EDR deployment within 9 weeks) while maintaining operational continuity and resource efficiency. Post-certification, the lifecycle transitions to continuous improvement mode with regular internal audits, management reviews, and surveillance audits to maintain certification validity over the 3-year certification cycle.



3.1 Stage-by-Stage Breakdown

Phase 1: Initiation (Weeks 1-2)

Objectives: Secure executive buy-in, define ISMS scope, establish project governance

Key Activities:

- Executive presentation and budget approval (~$70,000 Year 1)
- Scope definition: 55 employees, HQ office, AWS infrastructure, customer database, 55 laptops/mobiles
- Project team formation (CTO sponsor, ISMS PM, Technical Lead, Compliance Coordinator)
- Deliverable: Project charter, RACI matrix, communication plan

Techniques: Cost-benefit analysis, facilitated scope workshop, stakeholder alignment meeting

Phase 2: Gap Analysis (Weeks 3-6) - COMPLETED

Objectives: Assess current security posture, identify gaps, complete risk assessment

Key Activities:

- Control maturity assessment using 4-level scale (0-3)
- Risk assessment using NIST 800-30 methodology (Risk Score = Likelihood × Impact)
- Asset inventory validation (current: 10 assets documented, target: all 55 laptops tracked)
- Deliverable: Gap analysis report and risk register

Current State Summary:

- **Critical Gaps:** A.5.1 (Policies), A.6.1 (Background checks), A.6.3 (Training - 54.5% coverage), A.7.4 (CCTV), A.8.5 (No MFA)
- **High Risks:** R-01 (Weak credentials - Risk Score 15), R-02 (Malware - Risk Score 16), R-04 (Single-region backup - Risk Score 10)

Techniques: Document review, interviews, technical testing, risk workshops, evidence sampling

Phase 3: Remediation Planning (Weeks 7-8)

Objectives: Develop prioritized roadmap, allocate resources, identify quick wins

Key Activities:

- Risk-based prioritization into 3 implementation waves
- Tool selection: EDR (Microsoft Defender), SIEM (Microsoft Sentinel), MFA (Entra ID), Asset Management (Snipe-IT), Training (KnowBe4)
- Resource allocation: ISMS PM (100%), IT Security Lead (80%), external consultant (3 days/week)
- Quick wins: Enable MFA (1 week), Deploy EDR (1 week), Enforce screen lock policy

Budget Breakdown:

- Tool licensing: ~$20,000/year
- Consulting & certification: ~$42,000
- Infrastructure (CCTV, access control): ~$7,000
- **Total: ~$70,000 Year 1**

Techniques: Prioritization matrix, vendor PoC testing, resource capacity planning

Phase 4: Implementation Wave 1 - Critical Controls (Weeks 9-12)

Objectives: Address critical risks (R-01, R-02) and foundational security controls

Key Activities:

- **Week 9:** MFA implementation via Entra ID Conditional Access (A.8.5, R-01) - 100% user enrollment
- **Week 9:** EDR deployment to all 55 endpoints (A.8.7, R-02)
- **Week 10-11:** Policy framework update - 10 core policies (A.5.1, A.5.10, A.5.15, A.6.7, A.5.23)
- **Week 11:** Background verification process with 3rd party vendor (A.6.1)
- **Week 12:** CCTV installation - 4 cameras with 30-day retention (A.7.4)

Deliverables: MFA enrollment report, EDR coverage report, policy suite with employee acknowledgment, CCTV system operational

Techniques: Phased MFA rollout, Group Policy push for EDR, DocuSign for policy acknowledgment

Phase 5: Implementation Wave 2 - High Priority (Weeks 13-20)

Objectives: Address high-risk items and implement detection/monitoring capabilities

Key Activities:

- **Week 13-14:** Cross-region backup replication AWS Mumbai → Singapore (A.8.12, R-04)
- **Week 14-15:** 802.1X network access control with guest VLAN segregation (A.8.20, R-05)
- **Week 15-16:** Automated offboarding workflow -
- **Week 16-17:** Asset management tool (Snipe-IT) deployment with physical asset tagging (A.5.9)
- **Week 17-18:** Security awareness training platform - 5 modules + phishing simulation (A.6.3, R-07)
- **Week 18-20:** SIEM implementation (Microsoft Sentinel) with 6 data sources (A.8.16)

Success Metrics: 100% backup redundancy, phishing click rate

Techniques: S3 Cross-Region Replication, RADIUS/NPS deployment, Jira Service Desk automation, KnowBe4 training modules

Phase 6: Implementation Wave 3 - Medium/Low Priority (Weeks 21-28)

Objectives: Complete remaining controls, establish operational maturity

Key Activities:

- **Week 21:** Threat intelligence subscriptions - CERT-In, CISA, SANS ISC (A.5.7)
- **Week 21-22:** Cloud governance policy with CASB deployment (A.5.23)
- **Week 22-24:** Infrastructure-as-Code (Terraform) with CIS Benchmark baseline (A.8.9)
- **Week 24-25:** Data retention policy aligned with DPDP Act 2023 (A.8.10)
- **Week 25-26:** Secure coding guidelines (OWASP Top 10) with SAST tool (A.8.28)
- **Week 26-28:** Business Continuity Plan with annual tabletop exercise (A.8.36)

Deliverables: Threat log process, approved cloud services list, Terraform repository, retention schedule, secure coding checklist, BCP document

Techniques: Threat intelligence aggregation, Microsoft Defender for Cloud Apps CASB, Checkov compliance scanning, Business Impact Analysis

Phase 7: Documentation (Weeks 29-32)

Objectives: Compile ISMS documentation, prepare evidence repository

Key Activities:

- **Week 29-30:** Statement of Applicability (SoA) - all 93 Annex A controls
- **Week 30:** Risk Treatment Plan finalization with residual risk calculations
- **Week 30-31:** Complete policy suite (10 policies) with management approval
- **Week 31-32:** Procedures, work instructions, and templates library
- **Week 32:** Evidence repository organization in SharePoint

Deliverables: SoA document, Risk Treatment Plan, 10 approved policies, 20+ procedures, evidence folder structure

Techniques: Control-by-control SoA assessment, residual risk calculation (post-mitigation), policy template standardization

Phase 8: Internal Audit (Weeks 33-36)

Objectives: Independent verification of control effectiveness

Key Activities:

- **Week 33:** Internal audit planning - scope, sampling strategy, interview schedule
- **Week 34-35:** Control testing - 100% critical controls, 50% others
- **Week 35:** Non-conformity identification and Corrective Action Requests (CARs)
- **Week 36:** Management review meeting - audit findings, corrective actions, ISMS performance

Sampling Strategy:

- Critical controls (A.8.5, A.8.7, A.5.1): 100% testing
- High-priority controls: 70% sampling
- Medium/low priority: 40% sampling

Expected Findings: 5-10 minor non-conformities, 0-2 major non-conformities (target)

Techniques: ISO 19011 audit methodology, interview-based verification, evidence sampling, technical testing

Phase 9: Remediation of Findings (Weeks 37-40)

Objectives: Close all audit non-conformities

Key Activities:

- **Week 37-38:** CAR implementation - root cause analysis and corrective actions
- **Week 39:** Evidence re-collection and documentation updates
- **Week 40:** Follow-up audit - verification of CAR closure

Success Criteria: 100% CAR closure, zero open major non-conformities before Stage 1 audit

Techniques: 5 Whys root cause analysis, PDCA cycle, evidence re-audit

Phase 10: Certification Audit (Weeks 41-44)

Objectives: Achieve ISO 27001:2022 certification

Stage 1 Audit (Week 41-42) - Documentation Review:

- ISMS scope verification
- SoA and Risk Treatment Plan review
- Policy and procedure adequacy assessment
- Readiness assessment for Stage 2

Stage 2 Audit (Week 43-44) - Implementation Verification:

- On-site/remote audit (3 days)
- Control testing and employee interviews
- Evidence sampling and technical verification
- Audit report and certificate issuance (if no major non-conformities)

Certification Body Requirements: UKAS/ANAB accredited (e.g., BSI, DNV, SGS, Bureau Veritas)

Techniques: Document review, control walkthroughs, employee interviews, technical spot checks

Phase 11: Continuous Improvement (Ongoing)

Objectives: Maintain and improve ISMS effectiveness

Ongoing Activities:

- **Quarterly:** Risk reviews, access reviews, threat intelligence analysis
- **Semi-Annual:** Management reviews, backup restore testing
- **Annual:** Internal audits, BCP tabletop exercises, policy reviews, security awareness training
- **Year 2 & 3:** Surveillance audits (1-day each year)
- **Year 3:** Recertification audit (Stage 1 + Stage 2)

Key Performance Indicators (KPIs):

- Incident response time:
- Phishing simulation click rate: <5%
- Patch compliance: >95% within 30 days
- Training completion: 100% annually
- Audit non-conformities:

Techniques: PDCA (Plan-Do-Check-Act) cycle, KPI dashboards, continuous monitoring

3.2 CIA Triad Impact Analysis

Based on AcmeTech's gap analysis and risk register, the following table analyzes the impact on Confidentiality, Integrity, and Availability:

CIA Component	Impact Level	Explanation
Confidentiality	**High**	**Critical Gaps:** No MFA on M365 accounts (A.8.5, R-01) exposes customer database (A-01) and source code repository (A-02) to unauthorized access. Weak password hygiene increases credential compromise risk. Employee PII in HRMS (A-04) accessible to excessive users (R-03). No DLP on endpoints (R-06) allows data exfiltration by disgruntled employees. **Risks:** Customer data breach, intellectual property theft, GDPR/DPDP Act violations with potential fines up to ₹250 crore. **Remediation:** MFA implementation (Week 9), access control tightening (Week 15-16), DLP deployment reduce confidentiality risk from High to Low.

CIA Component	Impact Level	Explanation
Integrity	**Medium**	**Moderate Gaps:** No configuration management (A.8.9) leads to undocumented AWS infrastructure changes, increasing risk of misconfigurations. Lack of secure coding guidelines (A.8.28) exposes applications to injection attacks. Incomplete incident records (R-08) hinder forensic analysis and root cause determination. **Risks:** Data corruption through unauthorized changes, application vulnerabilities leading to data manipulation, inability to detect integrity violations due to insufficient logging. **Remediation:** Infrastructure-as-Code (Week 22-24), secure coding standards (Week 25-26), enhanced logging/SIEM (Week 18-20) reduce integrity risk from Medium to Low.
Availability	**High**	**Critical Gaps:** Single-region backup architecture (R-04) creates single point of failure - if AWS ap-south-1 (Mumbai) region fails, RPO could exceed 24 hours. No EDR on 30% of laptops (R-02) increases ransomware risk (MGM Resorts suffered $110M loss from similar attack). No business continuity plan (A.8.36) means undefined recovery procedures. Incomplete asset inventory (A.5.9) hampers disaster recovery. **Risks:** Ransomware encryption of production systems, prolonged outage from regional AWS failure, customer SLA breaches, revenue loss estimated at ₹50 lakh per day of downtime. **Remediation:** Cross-region backups (Week 13-14), EDR deployment (Week 9), BCP development (Week 26-28) reduce availability risk from High to Medium (residual risk remains due to cloud dependency).

CIA Triad Risk Summary:

Pre-Remediation (Current State):

- Confidentiality: High Risk (Score: 15/25) - Immediate action required
- Integrity: Medium Risk (Score: 8/25) - Moderate attention needed
- Availability: High Risk (Score: 16/25) - Immediate action required

Post-Remediation (Target State - Week 44):

- Confidentiality: Low Risk (Score: 4/25) - Acceptable residual risk
- Integrity: Low Risk (Score: 3/25) - Acceptable residual risk
- Availability: Medium Risk (Score: 6/25) - Managed with compensating controls (multi-region architecture)

Key Insight: AcmeTech's highest risks impact Confidentiality and Availability. The prioritized implementation approach (Wave 1 focusing on MFA and EDR) directly addresses these critical CIA triad weaknesses within the first 12 weeks, demonstrating risk-based decision making aligned with ISO 27001 principles.

4. Detection Methods for AcmeTech Solutions

Effective detection is critical for AcmeTech's security posture, particularly given the identified gaps in monitoring (A.8.16) and incident management (A.8.35). This section outlines comprehensive detection methods tailored to AcmeTech's current environment: 55 employees, hybrid work model (40% remote), AWS infrastructure, and identified critical risks including weak authentication (R-01), malware exposure (R-02), and insider threats (R-06).

4.1 Indicators of Compromise (IOCs)

Network-Based IOCs

Authentication Anomalies (Related to R-01: Weak Credentials)

- Multiple failed login attempts from single IP address (>5 failures in 10 minutes)
- Successful login from impossible travel locations (e.g., Mumbai login followed by US login within 2 hours)
- Login attempts outside business hours (10 PM - 6 AM IST) for non-IT staff
- Concurrent sessions from geographically distant locations
- First-time login from new countries/regions without travel request approval
- Use of legacy authentication protocols (POP3, IMAP without modern auth) on M365

Data Exfiltration Indicators (Related to R-06: Source Code Repository Risk)

- Unusual outbound traffic volumes (>500 MB in single session to external IP)
- Connections to file-sharing services (Mega.nz, WeTransfer, unapproved cloud storage)
- Large downloads from source code repository (>100 MB) outside development hours
- ZIP/RAR file creation on endpoints followed by external transfer
- Database queries returning >10,000 records by non-administrative users
- Use of data transfer protocols (FTP, SCP, rsync) to unknown destinations

Malware Communication Patterns (Related to R-02: Ransomware Risk)

- Beacon traffic at regular intervals to external IPs (e.g., every 60 seconds)
- DNS queries to recently registered domains (
- Connections to known Command & Control (C2) server IPs (reference: abuse.ch, AlienVault OTX)
- Outbound traffic on non-standard ports (e.g., HTTP on port 8080, 8888)
- TLS/SSL connections with invalid or self-signed certificates
- Communication with Tor exit nodes or anonymization networks

AWS Cloud Infrastructure IOCs

- Root account usage (should be zero except emergency break-glass scenarios)
- IAM policy changes granting broad permissions (e.g., `*:*` actions)
- Security group modifications opening ports to 0.0.0.0/0 (public internet)
- S3 bucket ACL changes making buckets publicly accessible
- Snapshot or AMI sharing with unknown AWS account IDs
- Unusual EC2 instance launches (regions not typically used, large instance types)

- CloudTrail logging disabled or log deletion attempts

Host-Based IOCs

Endpoint Compromise Indicators

- New scheduled tasks or cron jobs created by non-administrative users
- Modification of Windows Registry `Run` keys for persistence
- Creation of new local administrator accounts
- Unauthorized software installations (particularly remote access tools: TeamViewer, AnyDesk without approval)
- PowerShell execution with encoded commands (`-EncodedCommand` flag)
- Suspicious process parent-child relationships (e.g., `winword.exe` spawning `powershell.exe`)
- File encryption activity (multiple files renamed with extensions like `.locked`, `.encrypted`, `.crypt`)
- Abnormal CPU/memory usage spikes (potential cryptomining malware)

File System Anomalies

- Creation of files in suspicious locations (`C:\Windows\Temp`, `C:\ProgramData` with executable extensions)
- Modification of system files or binaries in `C:\Windows\System32`
- Large-scale file modifications in short timeframe (>1000 files modified in
- Shadow copy deletion (via `vssadmin delete shadows` command)
- Creation of hidden shares (e.g., `C$` modifications, new `$` shares)
- Suspicious file names (double extensions like `invoice.pdf.exe`, random character strings)

Credential Access Indicators

- Attempts to access Windows credential stores (`C:\Windows\System32\config\SAM`)
- LSASS memory dumping (using tools like ProcDump, Mimikatz)
- Kerberos ticket-granting ticket (TGT) requests without corresponding service ticket requests
- NTLM authentication attempts to internal systems from workstations (potential lateral movement)
- Clipboard monitoring activity (keylogging/credential harvesting)

4.2 Behavioral Indicators (Suspicious Activities)

User Behavior Anomalies

Insider Threat Patterns (Related to R-06)

- Employee accessing files/systems outside their job function (HR accessing source code repository, developer accessing HRMS)
- Mass file downloads from SharePoint/file servers (>100 files in single session)
- Copying data to personal USB drives (if not blocked)
- Accessing customer database (A-01) during resignation notice period
- Emailing documents to personal email addresses (Gmail, Yahoo)

- Working unusual hours without justification (late-night access after performance review meeting)
- Disabling antivirus or security tools on assigned laptop

Account Compromise Indicators

- Sudden change in email behavior (mass forwarding rules created, unusual recipients)
- Unexpected VPN connections from user's account while they're on vacation/sick leave
- Access to systems user doesn't normally use (e.g., marketing user accessing AWS console)
- Password change followed immediately by suspicious activity
- Multiple devices logged in simultaneously for single-device users
- Divergence from established access patterns (always accesses CRM from office, suddenly from home at 3 AM)

Privilege Escalation Attempts

- Repeated attempts to access restricted folders/systems
- Requests for elevated privileges without business justification
- Use of administrative tools by standard users (e.g., `net user`, `dsquery` commands)
- Attempts to modify security policies or configurations
- Accessing confidential documents not related to current project assignments

Application and System Behavior

Web Application Anomalies

- SQL injection attempts in application logs (single quotes, `UNION`, `SELECT` keywords in form inputs)
- Excessive 404 errors from single IP (reconnaissance/directory brute-forcing)
- POST requests with abnormally large payloads (>10 MB)
- High-frequency API calls exceeding rate limits (>1000 requests/minute)
- User-Agent strings indicating automated tools (e.g., `sqlmap`, `Nikto`, `Nessus`)
- Geographic anomalies (application access from countries where AcmeTech has no customers)

Database Behavior

- Queries running longer than historical baselines (>5 minutes for typically
- Full table scans on production databases during business hours
- `DROP`, `TRUNCATE`, or `ALTER` statements from application service accounts (should only be schema changes during maintenance windows)
- Export operations to CSV/Excel for large datasets (>10,000 rows) without BI tool involvement
- Privilege escalation queries (`GRANT ALL`, `CREATE USER` from non-DBA accounts)

AWS Resource Behavior

- Cryptocurrency mining indicators: Sudden spike in EC2 compute usage, GPU instance launches, connections to mining pools

- Data staging: Large S3 PUT operations followed by public sharing or cross-region transfers
- Resource hijacking: Lambda functions created in unused regions, unexpected CloudFormation stack deployments
- Cost anomalies: 300% increase in AWS monthly spend without corresponding business growth

4.3 Detection Tools

Enterprise-Grade Solutions (Recommended for AcmeTech)

1. **Microsoft Sentinel (SIEM) - $15,000/year**
    - **Coverage:** Centralized log aggregation from AWS CloudWatch, M365 audit logs, Azure AD, Windows endpoints, network firewalls
    - **Capabilities:**
        - Pre-built detection rules for 200+ threat scenarios
        - User and Entity Behavior Analytics (UEBA) for insider threat detection
        - Automated incident response playbooks (e.g., disable compromised user, isolate endpoint)
        - Integration with Microsoft 365 Defender for unified XDR
    - **AcmeTech Use Cases:**
        - Detect R-01 (multiple failed logins triggering MFA bypass attempts)
        - Alert on R-04 (backup deletion attempts in AWS)
        - Correlate R-07 (phishing email click + credential entry on suspicious site)
    - **Deployment:** Cloud-native SaaS, 2-week implementation timeline
    - **Retention:** 90 days active, 1 year cold storage (S3 Glacier archive)
2. **Microsoft Defender for Endpoint (EDR) - Included in M365 E5 ($57/user/month = $3,135/month for 55 users)**
    - **Coverage:** Real-time threat protection for all 55 Windows laptops
    - **Capabilities:**
        - Behavioral analysis and machine learning-based threat detection
        - Automated investigation and remediation (AIR)
        - Attack surface reduction rules (block Office macros, script execution)
        - Endpoint detection and response with 180-day timeline
        - Integration with threat intelligence feeds (Microsoft Threat Intelligence)
    - **AcmeTech Use Cases:**
        - Block R-02 ransomware via behavioral detection (file encryption patterns)
        - Detect credential dumping attempts (Mimikatz, ProcDump)
        - Alert on suspicious PowerShell usage
    - **Deployment:** Group Policy or Intune deployment, 1-week rollout
3. **AWS GuardDuty - $5-10/month (usage-based pricing)**
    - **Coverage:** Threat detection for AWS infrastructure (VPC Flow Logs, CloudTrail, DNS logs)
    - **Capabilities:**
        - Anomaly detection for AWS account activity
        - Cryptocurrency mining detection
        - Compromised EC2 instance identification

        - Malicious IP reputation checks
        - IAM credential compromise detection
    - **AcmeTech Use Cases:**
        - Detect unauthorized S3 bucket access or public exposure
        - Alert on root account usage
        - Identify EC2 instances communicating with known botnet C2 servers
    - **Deployment:** One-click enablement in AWS Console, immediate threat detection
4. **KnowBe4 Security Awareness Training + Phishing Simulator - $1,375/year ($25/user)**
    - **Coverage:** All 55 employees
    - **Capabilities:**
        - Monthly automated phishing simulations with 1000+ templates
        - Real-time reporting of user click rates and credential entry
        - Remedial training for users who fail simulations
        - Baseline and progress tracking (target:
    - **AcmeTech Use Cases:**
        - Measure susceptibility to R-07 (phishing-based account compromise)
        - Track improvement in security awareness from current 54.5% training coverage to 100%
    - **Deployment:** Cloud-based platform, 1-week configuration

Free and Open-Source Detection Tools

1. **Wazuh (Open-Source SIEM/XDR) - Free**
    - **Coverage:** Host-based intrusion detection, file integrity monitoring, log analysis
    - **Capabilities:**
        - Agent-based monitoring for Windows, Linux, macOS
        - Compliance reporting (PCI DSS, GDPR, ISO 27001)
        - Integration with VirusTotal, AlienVault OTX for threat intelligence
        - Rootkit and malware detection
    - **AcmeTech Use Cases:**
        - File integrity monitoring for critical AWS EC2 instances
        - Detect unauthorized changes to `/etc/passwd`, Windows Registry
        - Log aggregation for systems not covered by Sentinel (development/test environments)
    - **Deployment:** Self-hosted on AWS EC2 (t3.medium instance ~$30/month), 2-week setup
    - **Limitations:** Requires dedicated personnel for rule tuning and maintenance
2. **Suricata (Network Intrusion Detection System) - Free**
    - **Coverage:** Network traffic analysis at office HQ and AWS VPC level
    - **Capabilities:**
        - Deep packet inspection (DPI) for protocol anomalies
        - Signature-based detection using Emerging Threats ruleset (free)
        - TLS certificate inspection
        - HTTP/DNS request analysis
    - **AcmeTech Use Cases:**

        - Detect C2 beacon traffic patterns
        - Identify lateral movement via SMB/RDP
        - Alert on DNS tunneling attempts
    - **Deployment:** Deploy on pfSense firewall or dedicated AWS EC2 instance, 1-week configuration
    - **Limitations:** Encrypted traffic (HTTPS) requires SSL/TLS inspection proxy
3. **OSSEC (Host Intrusion Detection) - Free**
    - **Coverage:** Lightweight agent for endpoint monitoring
    - **Capabilities:**
        - Log analysis and correlation
        - File integrity monitoring (FIM)
        - Rootkit detection
        - Active response (automatically block IP after failed login threshold)
    - **AcmeTech Use Cases:**
        - Monitor critical directories on AWS servers (`/var/www`, `/etc`, application config files)
        - Detect brute-force SSH login attempts
        - Alert on unauthorized sudo usage
    - **Deployment:** Agent installation via Ansible/Puppet, 3-day rollout
    - **Limitations:** No central management UI (consider OSSEC-WUI or Wazuh for visualization)
4. **Snort (Network Intrusion Detection) - Free**
    - **Coverage:** Real-time traffic analysis and packet logging
    - **Capabilities:**
        - Protocol analysis and content matching
        - Community-driven ruleset (30,000+ signatures)
        - Integration with pfSense, VyOS routers
    - **AcmeTech Use Cases:**
        - Detect port scanning activities
        - Identify exploit attempts (EternalBlue, Log4Shell)
        - Monitor for data exfiltration over non-standard protocols
    - **Deployment:** Inline deployment on network gateway or mirror port, 2-week tuning period
    - **Limitations:** High false-positive rate requiring expert tuning
5. **ClamAV (Antivirus) - Free**
    - **Coverage:** Server-side malware scanning for Linux systems, email gateway
    - **Capabilities:**
        - On-demand and scheduled scanning
        - Email attachment scanning
        - Daily signature updates
    - **AcmeTech Use Cases:**
        - Scan uploaded files on web applications before storage in S3
        - Scan email attachments at Exchange Online gateway (using third-party integration)
        - Supplement Defender with Linux server protection

- **Deployment:** Package installation on Ubuntu/CentOS servers, 1-day setup
- **Limitations:** Lower detection rate compared to commercial solutions (~70% vs. 95%)

6. **TheHive + Cortex (Incident Response Platform) - Free**
   - **Coverage:** Case management for security incidents
   - **Capabilities:**
     - Incident tracking and workflow automation
     - Integration with MISP for threat intelligence sharing
     - Observable analysis (IOC enrichment via VirusTotal, AbuseIPDB)
     - Collaboration features for incident response team
   - **AcmeTech Use Cases:**
     - Centralized tracking of security incidents (currently tracked ad-hoc in Jira - R-08)
     - Document incident response timeline for compliance audits
     - Correlate IOCs across multiple incidents
   - **Deployment:** Docker containers on AWS, 1-week configuration
   - **Limitations:** Requires manual integration with detection tools (no native SIEM connector)

Detection Tool Comparison Matrix

Tool	Type	Cost/Year	Deployment	AcmeTech Priority	Addresses Risks
Microsoft Sentinel	SIEM	$15,000	2 weeks	**Critical**	R-01, R-04, R-06, R-07
Microsoft Defender for Endpoint	EDR	Included in E5	1 week	**Critical**	R-02, R-06
AWS GuardDuty	Cloud Security	$100-120	1 day	**High**	R-04, R-05
KnowBe4	Awareness Training	$1,375	1 week	**High**	R-07
Wazuh	SIEM/XDR	Free	2 weeks	Medium	R-02, R-06 (backup)
Suricata	NIDS	Free	1 week	Medium	R-05, R-06
OSSEC	HIDS	Free	3 days	Low	Server-side monitoring

Tool	Type	Cost/Year	Deployment	AcmeTech Priority	Addresses Risks
TheHive	Incident Response	Free	1 week	Low	R-08 (incident tracking)

4.4 Early Warning Signs

Pre-Incident Indicators

Environmental Precursors (Increased Risk Conditions)

- **Organizational Changes:** Layoffs announced, poor performance reviews, merger/acquisition rumors (increases insider threat risk R-06)
- **Security Tool Degradation:** Antivirus license expired, EDR agents offline on >10% endpoints, log collection failures
- **Patch Delays:** Critical vulnerabilities (CVSS 9.0+) unpatched for >30 days due to resource constraints
- **Security Awareness Decline:** Phishing simulation click rates increasing (trend from 8% → 15% over 3 months)
- **Audit Findings:** Internal audit identifies major non-conformities in access control or logging
- **Third-Party Compromises:** News of breach at supplier/vendor AcmeTech integrates with (supply chain risk)

Technical Precursors

- **Reconnaissance Activities:** Port scans detected from external IPs, SQL injection probe attempts in web logs
- **Social Engineering Attempts:** Employees report suspicious phone calls requesting credentials (vishing), phishing emails bypassing spam filters
- **Credential Leaks:** AcmeTech employee emails appear in public data breach databases (check: Have I Been Pwned API)
- **Dark Web Mentions:** Company name or employee credentials for sale on underground forums (monitor via threat intelligence feeds)
- **Vulnerability Disclosures:** Zero-day vulnerability announced affecting AcmeTech's tech stack (e.g., critical VMware, Microsoft Exchange, AWS service vulnerability)

Incident Escalation Triggers

Severity Thresholds Requiring Immediate Escalation

Critical (Escalate to CTO + ISMS PM within 15 minutes):

- Ransomware encryption detected on any endpoint
- AWS root account accessed without break-glass justification
- Customer database (A-01) unauthorized access or exfiltration
- More than 5 endpoints reporting EDR alerts simultaneously (potential coordinated attack)
- Public S3 bucket exposure containing PII/customer data

- DDoS attack causing production downtime

High (Escalate to IT Security Lead within 1 hour):

- Failed login attempts exceeding 50 in 1-hour window for privileged accounts
- Malware detection on >3 endpoints within 24 hours
- Unauthorized security group changes allowing 0.0.0.0/0 access to production systems
- Data Loss Prevention (DLP) alert for large file transfer to external email
- Phishing campaign targeting >10 employees simultaneously

Medium (Log and investigate within 4 hours):

- Single endpoint malware detection successfully quarantined
- Failed login attempts from known bad IP addresses
- Unauthorized software installation on non-critical endpoint
- Anomalous cloud resource usage (20-50% cost spike without business justification)

Early Warning Checklist (Weekly Review by IT Security Lead):

- Review AWS GuardDuty findings (target: 0 high-severity findings)
- Check Sentinel threat intelligence alerts
- Analyze failed authentication trends (>10% week-over-week increase = investigate)
- Review phishing simulation results (click rate increasing = additional training needed)
- Verify backup completion status (100% success rate required)
- Confirm EDR agent health (>98% endpoints reporting)
- Check for employee departures without completed offboarding (access revocation delays)
- Scan for new CVEs affecting AcmeTech infrastructure (subscribe to NVD, CERT-In feeds)
- Review threat intelligence for industry-specific campaigns (monitor CERT-In advisories for Indian organizations)
- Verify SIEM log ingestion rates (detect potential log deletion or collection failures)

Section 5: Mitigation Strategies for AcmeTech Solutions

Introduction

This section provides actionable mitigation strategies to address AcmeTech's identified gaps and risks. Strategies are organized by control type (technical, policy/process, training) and prioritized into three implementation phases aligned with the ISO 27001 compliance lifecycle.

5.1 Technical Controls with Priority and Cost Estimates

Technical Controls Summary Table

Control	Gap/Risk	Implementation	Cost	Timeline	Priority
Multi-Factor Authentication	A.8.5, R-01	Microsoft Entra ID Conditional Access	Included in M365 E5	1 week	**Immediate**
Endpoint Detection & Response	A.8.7, R-02	Microsoft Defender for Endpoint via GPO	Included in M365 E5	1 week	**Immediate**
Privileged Access Management	A.8.2, R-01	Azure AD PIM with JIT access	$540/year	2 weeks	**Immediate**
Automated Screen Lock	A.7.7	Group Policy 5-minute timeout	Free	Immediate	**Immediate**
Cross-Region Backup	A.8.12, R-04	S3 Cross-Region Replication	$3,000/year	2 weeks	**Short-term**
Network Access Control	A.8.20, R-05	802.1X with Microsoft NPS	$500 one-time	2 weeks	**Short-term**
Automated Offboarding	A.5.18, R-06	Jira + AD/M365/AWS integration	$360/year	2 weeks	**Short-term**
Data Loss Prevention	R-06	Microsoft Purview DLP policies	Included in M365 E5	2 weeks	**Short-term**
SIEM Implementation	A.8.16	Microsoft Sentinel	$15,000/year	3 weeks	**Short-term**
CCTV System	A.7.4	4 IP cameras with NVR	$3,000 one-time	1 week	**Short-term**
Biometric Access	A.7.2	Fingerprint/RFID badges	$4,000 one-time	2 weeks	**Short-term**
Asset Management	A.5.9	Snipe-IT deployment	$180/year	2 weeks	**Long-term**
Infrastructure-as-Code	A.8.9	Terraform with CIS Benchmarks	$1,680/year	3 weeks	**Long-term**
Vulnerability Scanning	A.8.8	AWS Inspector + OWASP ZAP	$1,800/year	2 weeks	**Long-term**
Web Application Firewall	A.8.20	AWS WAF with OWASP rules	$600/year	2 weeks	**Long-term**
Endpoint Web Filtering	A.8.23	Cisco Umbrella DNS filtering	$1,980/year	2 weeks	**Long-term**

Control	Gap/Risk	Implementation	Cost	Timeline	Priority
SAST Tool	A.8.28	SonarQube in CI/CD pipeline	$360/year	2 weeks	**Long-term**

Total Year 1 Investment: ~$30,700 (one-time + first-year recurring)

Annual Recurring Costs: ~$26,800/year

5.2 Policy and Process Controls

Critical Policies (Immediate - Week 10-11)

1. **Information Security Policy (A.5.1)**
    - **Purpose:** Establish management commitment and ISMS framework
    - **Components:** Security objectives, roles/responsibilities, compliance requirements, annual review cycle
    - **Approval:** CTO signature with board acknowledgment
    - **Distribution:** SharePoint + mandatory employee acknowledgment via DocuSign
2. **Acceptable Use Policy (A.5.10)**
    - **Gap Addressed:** No formal AUP exists
    - **Key Rules:** Email usage limits, prohibited activities (torrenting, crypto-mining), BYOD requirements, software installation restrictions
    - **Enforcement:** HR disciplinary process for violations
3. **Access Control Policy (A.5.15, A.5.18)**
    - **Principles:** Least privilege, separation of duties, need-to-know
    - **Procedures:** Jira-based access requests with manager approval, quarterly access reviews, automated revocation within 1 hour of offboarding
4. **Remote Working Policy (A.6.7)**
    - **Requirements:** MFA mandatory for remote access, VPN usage required, endpoint encryption enabled, clear desk policy at home offices
    - **Security Controls:** EDR on all remote devices, web filtering for remote workers, prohibit public Wi-Fi without VPN
5. **Cloud Governance Policy (A.5.23)**
    - **Gap Addressed:** No AWS governance, shadow IT risk
    - **Requirements:** IT Security Lead + CTO approval for new cloud services, maintain approved services list, CASB monitoring
    - **Enforcement:** Web filtering blocks unapproved cloud services

Supporting Procedures (Short-term - Week 11-16)

6. **Incident Response Procedure (A.8.35)**
    - **Gap Addressed:** No formal procedure, ad-hoc Jira tracking (R-08)
    - **Components:** Severity classification (P1-P4), escalation matrix, communication templates, evidence collection guidelines

- **Tools:** TheHive for incident tracking, documented playbooks for common scenarios

7. **Backup and Recovery Procedure (A.8.12)**
    - **Gap Addressed:** No formal backup policy
    - **Components:** Daily incremental + weekly full backups, cross-region replication, quarterly restore testing with documented results, 90-day retention
    - **RPO/RTO Targets:** RPO 24 hours, RTO 4 hours for critical systems
8. **Data Retention and Deletion Procedure (A.8.10)**
    - **Compliance:** DPDP Act 2023, GDPR (if applicable)
    - **Retention Schedule:** Customer data (3 years post-contract), employee records (7 years), audit logs (1 year), backups (90 days)
    - **Deletion:** Automated lifecycle policies, quarterly verification audits
9. **Secure Development Procedure (A.8.28)**
    - **Gap Addressed:** No secure coding guidelines
    - **Components:** OWASP Top 10 compliance, code review checklist, SAST scanning in CI/CD, developer secure coding training
    - **Enforcement:** No pull request merge without security approval
10. **Business Continuity Procedure (A.8.36)**
    - **Components:** Business Impact Analysis (BIA), documented recovery procedures for AWS infrastructure, communication plan, annual tabletop exercises
    - **Critical Processes:** Customer database (RTO 4 hours), production application (RTO 8 hours), email (RTO 24 hours)

5.3 Training Recommendations

Immediate Training (Week 10-12)

1. **Security Awareness Foundation Training - All 55 Employees**
    - **Duration:** 90 minutes (self-paced modules)
    - **Platform:** KnowBe4 Security Awareness Training
    - **Modules:**
        - Module 1: Information Security Basics (30 min) - CIA triad, data classification, acceptable use
        - Module 2: Phishing & Social Engineering (20 min) - Recognizing suspicious emails, vishing, pretexting
        - Module 3: Password Security & MFA (15 min) - Strong password creation, MFA enrollment, password manager usage
        - Module 4: Data Handling & Privacy (15 min) - PII protection, DPDP Act basics, clean desk policy
        - Module 5: Incident Reporting (10 min) - What to report, how to report, escalation process
    - **Assessment:** 10-question quiz (80% passing score required)
    - **Completion Target:** 100% within 2 weeks of policy publication
    - **Cost:** Included in $1,375/year KnowBe4 license
2. **MFA Enrollment Training - All 55 Employees**
    - **Duration:** 15 minutes

- **Format:** Live webinar + recorded video for reference
- **Content:** Microsoft Authenticator app installation, QR code enrollment, passwordless setup, backup codes
- **Timeline:** Week 9 (concurrent with MFA rollout)
- **Trainer:** IT Security Lead

Short-Term Training (Week 13-20)

3. **Phishing Simulation Program - All 55 Employees**
    - **Frequency:** Monthly automated simulations
    - **Platform:** KnowBe4 Phishing Security Test
    - **Approach:**
        - Month 1: Easy template (obvious phishing indicators) - establish baseline
        - Month 2-3: Medium difficulty (realistic phishing scenarios)
        - Month 4+: Advanced templates (spear-phishing, CEO fraud)
    - **Remedial Training:** Employees who click phishing links automatically assigned 5-minute training module
    - **Success Metric:** Achieve <5% click rate by Month 6 (down from estimated 15-20% baseline)
    - **Reporting:** Monthly dashboard shared with management showing click rates, department comparisons, improvement trends
4. **Role-Based Security Training**
    - **IT Team (5 staff) - Secure Administration Training**
        - **Duration:** 4 hours
        - **Content:** Privileged access best practices, PAM usage, secure AWS configuration, incident response procedures, log review techniques
        - **Format:** Instructor-led workshop (external consultant or SANS OnDemand)
        - **Timeline:** Week 15
        - **Cost:** $2,500 (SANS Securing the Human workshop) or free (internal delivery by consultant)
    - **Developers (15 staff) - Secure Coding Training**
        - **Duration:** 4 hours
        - **Content:** OWASP Top 10 deep-dive, input validation, authentication/authorization, cryptography, dependency management, SAST tool usage
        - **Format:** Hands-on workshop with code examples
        - **Timeline:** Week 18
        - **Trainer:** External security consultant or senior developer with secure coding certification
        - **Cost:** $3,000 (external trainer) or free (internal if qualified trainer available)
    - **HR & Finance (5 staff) - Data Privacy Training**
        - **Duration:** 2 hours
        - **Content:** DPDP Act 2023 compliance, PII handling, HRMS access controls, employee data retention, breach notification procedures
        - **Format:** Instructor-led session

        - **Timeline:** Week 16
        - **Trainer:** Legal/compliance consultant or DPO
        - **Cost:** $1,500 or free (internal legal team)
    - **Management (5 executives) - Risk Management Training**
        - **Duration:** 2 hours
        - **Content:** ISO 27001 management responsibilities, risk assessment methodology, incident escalation, management review process, compliance obligations
        - **Format:** Executive briefing
        - **Timeline:** Week 20
        - **Trainer:** ISO 27001 consultant
        - **Cost:** Included in consultant retainer

Long-Term Training (Ongoing)

5. **Annual Refresher Training - All 55 Employees**
    - **Duration:** 60 minutes
    - **Content:** Updates on new threats, policy changes, lessons learned from incidents, compliance requirements
    - **Format:** Self-paced online modules with annual mandatory completion
    - **Timeline:** Every 12 months from initial training
    - **Assessment:** 10-question quiz (80% passing)
    - **Cost:** Included in KnowBe4 annual license
6. **New Hire Security Onboarding - All New Employees**
    - **Duration:** 30 minutes (Day 1 orientation)
    - **Content:** Information Security Policy overview, AUP acknowledgment, MFA enrollment, password manager setup, incident reporting contacts
    - **Format:** Live orientation session + digital acknowledgment
    - **Delivery:** HR + IT Security Lead
    - **Timeline:** Day 1 of employment (part of standard onboarding)
    - **Cost:** Free (internal delivery)
7. **Specialized Certifications (Optional - Career Development)**
    - **For IT Security Team:**
        - Certified Information Systems Security Professional (CISSP) - $699 exam
        - Certified Ethical Hacker (CEH) - $1,199 course + exam
        - AWS Certified Security - Specialty - $300 exam
        - ISO 27001 Lead Implementer - $2,500 5-day course
    - **Budget:** $5,000/year for certifications (2-3 team members)
    - **Timeline:** Year 2-3 (post-certification)

Training Metrics and Reporting

Key Performance Indicators:

- Training completion rate: 100% target (within 2 weeks of assignment)
- Phishing simulation click rate: <5% target (by Month 6)
- Assessment pass rate: >95% (80% passing score)
- Time-to-complete for new hires: <24 hours
- Annual refresher completion: 100% (within 30 days of assignment)

Quarterly Training Report (to Management):

- Completion statistics by department
- Phishing simulation performance trends
- Repeat offenders requiring additional coaching
- Training gaps and recommendations
- Budget utilization

Training Total Cost Estimate:

- **Year 1:** $8,375 (KnowBe4 $1,375 + role-based training $7,000)
- **Annual Recurring:** $1,375 (KnowBe4 license) + $5,000 (optional certifications) = $6,375/year

5.4 Prioritized Implementation Roadmap

Immediate Actions (0-30 Days)

Week 1-2: Critical Foundation

- ☐ Enable MFA on all 55 Microsoft 365 accounts (A.8.5, R-01) - **Cost: $0 (included)**
- ☐ Deploy EDR to all 55 endpoints via Group Policy (A.8.7, R-02) - **Cost: $0 (included)**
- ☐ Enforce 5-minute screen lock via GPO (A.7.7) - **Cost: $0**
- ☐ Implement PAM with Azure AD PIM for database admins (A.8.2, R-01) - **Cost: $540/year**
- ☐ Conduct MFA enrollment training webinar - **Cost: $0 (internal)**

Week 3-4: Policy Framework

- ☐ Develop and publish 5 critical policies (A.5.1, A.5.10, A.5.15, A.6.7, A.5.23) - **Cost: $0 (internal or included in consultant fees)**
- ☐ Distribute policies via SharePoint with DocuSign acknowledgment - **Cost: $0**
- ☐ Launch foundation security awareness training (90 min, all staff) - **Cost: $1,375/year (KnowBe4)**
- ☐ Baseline phishing simulation (establish click rate) - **Cost: Included**

Immediate Phase Total Cost: $1,915 Year 1 ($540 PAM + $1,375 training)

Critical Risks Mitigated:

- R-01: Weak credentials → **Residual Risk: 4 (Low)** - MFA + PAM deployed
- R-02: Malware/ransomware → **Residual Risk: 6 (Medium)** - EDR deployed to 100% endpoints
- A.7.7: Clear screen → **Compliant** - Auto-lock enforced

Expected Outcomes:

- 100% MFA enrollment within 1 week
- 100% EDR coverage within 1 week
- 100% policy acknowledgment within 2 weeks
- Baseline phishing click rate established (likely 15-20%)

Short-Term Actions (1-3 Months)

Month 1 (Week 5-8): Detection & Monitoring

- ☐ Deploy CCTV system at HQ (A.7.4) - **Cost: $3,000 one-time**
- ☐ Install biometric access control with RFID badges (A.7.2) - **Cost: $4,000 one-time**
- ☐ Enable AWS GuardDuty for cloud threat detection - **Cost: $120/year**
- ☐ Contract 3rd party background verification vendor (A.6.1) - **Cost: $50-100 per check**
- ☐ Conduct role-based training: HR/Finance data privacy (2 hours) - **Cost: $1,500**

Month 2 (Week 9-12): Infrastructure Hardening

- ☐ Implement cross-region S3 backup replication (A.8.12, R-04) - **Cost: $3,000/year**
- ☐ Deploy 802.1X network access control (A.8.20, R-05) - **Cost: $500 one-time**
- ☐ Automate offboarding workflow in Jira (A.5.18, R-06) - **Cost: $360/year**
- ☐ Configure Microsoft Purview DLP policies (R-06) - **Cost: $0 (included)**
- ☐ Quarterly backup restore test (document results) - **Cost: $0**
- ☐ Conduct role-based training: IT team secure administration (4 hours) - **Cost: $2,500**

Month 3 (Week 13-16): Advanced Detection

- ☐ Deploy Microsoft Sentinel SIEM (A.8.16) - **Cost: $15,000/year**
- ☐ Configure 20+ detection rules for critical use cases - **Cost: Included**
- ☐ Deploy FIDO2 security keys for 15 privileged users (R-07) - **Cost: $750 one-time**
- ☐ Implement asset management tool (Snipe-IT) with tagging (A.5.9) - **Cost: $280 (EC2 + tags)**
- ☐ Conduct role-based training: Developers secure coding (4 hours) - **Cost: $3,000**
- ☐ Month 3 phishing simulation - track improvement - **Cost: Included**

Short-Term Phase Total Cost: $33,010 Year 1 (one-time + recurring)

Risks Mitigated:

- R-04: Single-region backup → **Residual Risk: 3 (Low)** - Cross-region replication deployed
- R-05: Visitor network access → **Residual Risk: 4 (Low)** - 802.1X + guest VLAN segregation
- R-06: Offboarding delays → **Residual Risk: 4 (Low)** - Automated within 1 hour
- R-07: Phishing → **Residual Risk: 6 (Medium)** - Training + simulations ongoing, FIDO2 for privileged users

Expected Outcomes:

- 100% backup redundancy achieved (multi-region)
- Offboarding access revocation <1 hour (down from 3-5 days)
- Phishing click rate reduced to 8-10% (from 15-20% baseline)
- Centralized SIEM with 90-day log retention operational
- All 55 assets tracked with physical ID tags

Long-Term Actions (3-12 Months)

Month 4-6 (Week 17-28): Operational Maturity

- ☐ Subscribe to threat intelligence feeds (CERT-In, CISA) (A.5.7) - **Cost: $0 (free)**
- ☐ Implement cloud governance policy with CASB (A.5.23) - **Cost: Included in M365 E5**
- ☐ Deploy Terraform Infrastructure-as-Code with CIS Benchmarks (A.8.9) - **Cost: $1,680/year**
- ☐ Develop data retention policy aligned with DPDP Act (A.8.10) - **Cost: $0**
- ☐ Deploy AWS Inspector vulnerability scanning (A.8.8) - **Cost: $1,800/year**
- ☐ Implement AWS WAF with OWASP rules (A.8.20) - **Cost: $600/year**
- ☐ Deploy endpoint web filtering (Cisco Umbrella) (A.8.23) - **Cost: $1,980/year**
- ☐ Integrate SonarQube SAST in CI/CD pipeline (A.8.28) - **Cost: $360/year**
- ☐ Develop and test Business Continuity Plan (A.8.36) - **Cost: $0**
- ☐ Conduct BCP tabletop exercise - **Cost: $0**
- ☐ Monthly phishing simulations (Month 4-6) - **Cost: Included**

Month 7-9 (Week 29-36): Documentation & Internal Audit

- ☐ Complete Statement of Applicability (all 93 controls) - **Cost: $0**