Case Study

Design and Creative Technologies

Torrens University, Australia

Student: Luis Guilherme de Barros Andrade Faria - A00187785

Subject Code: SBD 403

Subject Name: Secure By Design

Assessment No.: 2

Title of Assessment: Case Study

Lecturer: Dr. Tanvir Rahman

Date: Nov 2025

Table of Contents

1. Executive Summary

This Secure by Design Implementation Guide defines how the organization, an analytics company serving both Hospital and Retail clients, will protect critical data and maintain service continuity through Secure-by-Design (SBD) principles. The company employs roughly 300 staff divided into **100 Doctors** (hospital analytics, on premise servers) and **200 Retailers** (consumer-behavior analysis, cloud-based).

The proposed strategy integrates **people**, **process** and **technology** to meet compliance obligations under **ISO/IEC 27001, ISO 27017, NIST SP 800-53** and **OWASP Top 10 (2024)**. It balances usability and protection while adding risk management and ensuring that both workgroups can operate safely without unnecessary friction.

The implementation of this strategy will follow a **phased 12-month** roadmap, ensuring that critical security controls, such as MFA, encryption and policy governance are established early, followed by staff training, continuous monitoring and final optimization. Each phase includes defined deliverables, ownership and performance metrics so that security improvements are introduced methodically without disrupting daily operations.

Cybersecurity must be addressed at the organizational level, not as a technical afterthought (Calder, 2020). Embedding secure-by-design principles into governance framework ensures alignment with ISO 27001 controls and NIST SP 800-63B identity standards.

2. Context and Secure-by-Design Principles

The company processes sensitive patient and customer data across two data domains:

- **Hospital data:** stored on-premises, covered by health-privacy legislation and medical-record confidentiality.
- **Retail data:** processed in an Australian cloud environment for commercial insights.

Rather than bolting security onto finished systems, we're embedding it into every development phase, what Shostack (2014) calls 'designing for security' rather than 'securing'. The foundation rests on the CIA Triad:

- **Confidentiality**: information is available only to authorized entities.
- **Integrity**: data remains accurate and unaltered.
- **Availability**: systems and information remain accessible when required.

Complementing the CIA triad, we also have least privilege, defense-in-depth, and human-centred security, designing systems that people can use correctly.

3. User Training and Awareness Program

As emphatically discussed in class by Dr. Tanvir Rahman and reinforced across multiple readings in this course, **human behavior** remains the **biggest risk** in cyber defense. Recent empirical evidence confirms that while phishing-awareness programs improve performance in the short term, their effects decay rapidly without continuous, data-driven reinforcement (Hillman, Harel, & Toch, 2023).

A targeted training program to superpower *the people behind the technology* will include the following:

1. **Phishing awareness**: simulated phishing campaigns every quarter to reduce click-through rates and retrieve feedback on users and departments preparedness for risks.

2. **Data-classification and handling**: clear labelling of confidential, internal, and public information (ISO 27002 §8).
3. **Incident-reporting drills**: tabletop exercises teaching staff how to escalate suspicious activity.
4. **Password and MFA hygiene**: short videos showing how to use passphrases and authenticator apps.
5. **Secure remote work**: VPN use, device locking, and secure Wi-Fi guidance.
6. **HR integration**: engagement programs for performance recognition tied to cyber security certificates.

The training will be mandatory for all new hires and refreshed every six months. Progress will be tracked through a LMS (Learning Management System) and correlated with incident statistics. This aligns with **NIST SP 800-50** on security awareness and **ISO 27002 §7** on personnel controls.

Rather than punishing users for security mistakes, we're creating a culture where reporting suspicious activity is rewarded, and learning is continuous (Tisdale, 2015).

4. Risk Assessment

As Steinberg (2020) highlights, understanding the fundamentals of threats, vulnerabilities, and countermeasures is essential before implementing any Secure-by-Design control. With it, we enable the organization to:

- Prioritize security investments based on actual threat likelihood and business impact.
- Demonstrate due diligence to clients, regulators, and compliance auditors.
- Create a measurable baseline for tracking security posture improvements over time.

- Allocate limited resources (budget, staff) to controls with the highest risk-reduction ROI (Return of Investment).

The CISO team leads this process, re-assessing risks quarterly or after significant system changes, with input from IT Operations, HR, and department heads. The methodology follows ISO 27005 risk management principles, evaluating: *Risk = (Likelihood × Impact) – Mitigation*.

#	Risk	Likelihood	Impact	Mitigation	Owner	Res Risk
1	Phishing compromise of user credentials	High	High	MFA, simulated campaigns, email filter (SPF, DKIM, DMARC)	IT Sec Manager	Low
2	Cloud misconfiguration exposing retail data	High	High	Automated compliance scanner, least-privilege IAM, periodic audits	Cloud Lead	Low
3	Insider misuse or data exfiltration	High	High	DLP software, access-log analytics, HR screening	CISO / HR	Low
4	Ransomware infection	Med	Med	Endpoint EDR, immutable backups, patch management	Sys Admin	Low
5	DDoS/Service Outage	Low	High	WAF, CDN, redundant links, test BCP	IT Ops	Low
6	Unauthorized access to hospital servers	Med	High	Physical access control, CCTV, audit trails	Facilities	Low

Each risk has a designated owner responsible for monitoring controls and reporting into the monthly security dashboard.

4.1 DREAD Threat Scoring for Critical Risks

As Sutton (2022) notes, the modern threat landscape has shifted from isolated malware to complex, multi-stage campaigns that exploit both technology and human behavior - and to

quantify the severity of our top risks, we applied the DREAD framework developed by Microsoft (Howard & LeBlanc, 2003). Each category is scored 1-10, with the average determining priority.

Risk #1: Phishing Compromise of User Credentials

Category	Risk	Justification
Damage potential	9	Full account takeover enables access to sensitive hospital or retail datasets. Financial and reputational damage would be severe.
Reproducibility	8	Phishing kits are readily available; attacks can be launched repeatedly with minimal effort.
Exploitability	7	Requires social engineering but no technical expertise. Success rate averages 30% in untrained populations (Tisdale, 2015).
Affected Users	9	All 300 employees are potential targets; compromise of admin accounts magnifies impact.
Discoverability	8	Email addresses follow predictable patterns (firstname.lastname@company.au), making reconnaissance trivial.
DREAD Score	8.2/10	Critical. Immediate mitigation required.

Risk #3: Insider Misuse or Data Exfiltration

Category	Risk	Justification
Damage potential	10	Insiders already have authorized access; exfiltration of hospital data would violate privacy regulations and destroy client trust.
Reproducibility	6	Requires intent and opportunity; not easily repeatable without detection after initial incident.
Exploitability	8	Authorized users can copy data to USB drives or personal cloud storage with little technical barrier.
Affected Users	7	Primarily impacts the 100-person Doctors group handling sensitive medical records.

Discoverability	4	Insider threats are notoriously difficult to predict; behavioral analytics required for detection.
DREAD Score	7.0/10	High. Continuous monitoring essential.

5. Mitigation Methods

5.1. Technical Controls

- **Next-generation firewall + IDS/IPS**: monitors inbound/outbound traffic in real time (ISO 27002 §13).
- **Encryption**: AES-256 for data at rest; TLS 1.3 for data in transit (NIST SP 800-52 Rev 2).
- **Multi-Factor Authentication (MFA)**: required for all user accounts; app-based rather than SMS.
- **Automated patch management**: weekly checks; critical patches within 48 hours.
- **Endpoint Detection and Response (EDR)**: monitors anomalies and quarantines malware automatically

5.2. Organizational Controls

- **Information Security Policy**: outlines acceptable use, access levels, and incident response steps.
- **Security Governance Committee**: cross-functional body (IT, HR, Legal, Ops) meeting monthly to review metrics.

The table below maps controls in accordance with standards (e.g., MFA → ISO 27001, NIST 800-63B) for enhanced clarity moving forward with the project:

Security Control	NIST Reference	ISO/IEC Reference

Multi-Factor Authentication (MFA)	NIST SP 800-63B Â§5.1	ISO/IEC 27001 Â§9.4.2
AES-256 Encryption	NIST SP 800-57	ISO/IEC 27001 Â§10.1
TLS 1.3 (Data in Transit)	NIST SP 800-52 Rev.2	ISO/IEC 27001 Â§13.2.3
Patch Management	NIST SP 800-40	ISO/IEC 27001 Â§12.6.1
Security Awareness Training	NIST SP 800-50	ISO/IEC 27001 Â§7.2.2
Access Control (RBAC)	NIST SP 800-53 AC-2	ISO/IEC 27001 Â§9.1
SIEM and Logging	NIST SP 800-92	ISO/IEC 27001 Â§12.4
Business Continuity Planning (BCP)	NIST SP 800-34	ISO 22301:2019
Endpoint Detection and Response (EDR)	NIST SP 800-137	ISO/IEC 27001 Â§12.6.2
Cloud Security (SSE, KMS, etc.)	NIST SP 800-144	ISO/IEC 27017
Data Classification	NIST SP 800-60	ISO/IEC 27001 Â§8.2
Physical Security Controls	NIST SP 800-116	ISO/IEC 27001 Â§11.1

Controls are classified as:

- **Mandatory**: MFA, encryption, firewall/IDS, patching.
- **Recommended**: DLP, CASB, and advanced analytics (dependent on budget).

5.3. User Impact Analysis of Security Controls

To ensure security does not stress operations, each control has been evaluated not just for its technical effectiveness but also for its impact on end-users. The organization has adopted ISO 9241-210 (Ergonomics of human-system interaction) principles to design user-friendly security mechanisms that promote compliance without creating resistance. The following table details user impacts and mitigation strategies for each major control.

Control	User Impact	Mitigation / UX Strategy
MFA	Adds login friction (especially for mobile users)	Use app-based push (not OTP); SSO + adaptive MFA reduce frequency
AES-256 Encryption	Transparent to users	Implemented at storage level; no workflow change
Patch Automation	May trigger reboots or service disruption	Scheduled during off-peak; user comms via IT portal
EDR	Potential false positives / system slowdowns	Tuning profiles to user roles; EDR alerts reviewed before lockout
Firewall + IDS/IPS	May block legitimate traffic	False positive handling + exception process documented
Security Policy & Governance	Viewed as bureaucratic	Policy summaries shared via intranet in plain language; staff feedback loop created

Training Modules	Time-consuming; "boring" perception	Gamified phishing tests; 90%+ completion tracked via LMS

6. User Rights and Access Control

Access follows the *Principle of Least Privilege* using *Role-Based Access Control* (RBAC):

Role	Data Access	System Access	Notes
Doctors Group	Hospital dataset only	On-prem analytics servers	Read/Write to medical tables
Retailers Group	Retail dataset only	Cloud tenant (Azure AU-East)	No access to hospital records
Executives & PAs	Reports only (aggregated data)	Dashboard via SSO	No raw data
IT Admins	Temporary elevated privilege ("break-glass")	AD + network infra	Logs audited daily

All access events are recorded in centralized SIEM (Security Information and Event Management). Privileges expire automatically after 30 days unless renewed.

7. Password and Authentication Policy

Aligned with NIST SP 800-63B (2023) and OWASP Authentication Cheat Sheet:

Account Type	Policy	Rationale
Standard Users	≥ 12 characters; no forced expiry if MFA enabled; block known breached passwords; allow passphrases (e.g., "river-sky-coffee-train").	Longer passphrases > complexity rules.
Privileged Accounts	≥ 16 characters; rotate every 90 days; MFA mandatory; no reuse of 5 previous passwords	Protects high-impact accounts.

Failed logins trigger account lockout after 5 attempts for 30 minutes. Audit logs retain credential events for one year.

The rationale for the Password Policy Design choices are:

- Length over complexity: NIST SP 800-63B (2023) demonstrates that longer passphrases provide greater entropy than complex 8-character passwords. A 12-character passphrase like "coffee-river-mountain-12" is both memorable and cryptographically stronger than "P@ssw0rd!".
- No forced expiry with MFA: Research by Taneski et al. (2019) shows that forced password changes lead to predictable patterns (Password1 → Password2). When MFA is enabled, the second factor compensates, making expiration counterproductive (NIST 800-63B §5.1.1.2).
- Breach detection: Integration with Have I Been Pwned API prevents users from selecting compromised credentials.

8. Storage Security Controls

8.1. Technical Controls

The on-premises hospital servers reside in a Tier 3-equivalent data center with layered physical controls meeting NIST SP 800-116 requirements for sensitive health data:

- **Physical security**: Biometric key-card entry (two-factor: card + fingerprint), 24/7 CCTV monitored by security personnel, FM-200 fire suppression to protect against thermal damage without water damage to electronics, and locked server racks preventing unauthorized device tampering or USB-based exfiltration.
- **Network segmentation**: The hospital data VLAN is isolated from corporate LAN and internet-facing systems using firewall rules that default-deny all traffic except

explicitly approved analytics application ports. This reduces the blast radius if the corporate network is compromised (ISO 27001 §13.1.3).

- **Encryption**: AES-256 full-disk encryption with keys stored in a FIPS 140-2 Level 2 Hardware Security Module (HSM). The HSM prevents key extraction even if physical hardware is stolen, aligning with ISO 27001 §10.1.1 cryptographic controls.
- **Backup and recovery**: Nightly incremental backups and weekly full backups to air-gapped offline storage following the 3-2-1 rule (3 copies, 2 media types, 1 offsite). Restoration drills occur monthly to validate RPO targets, as required by ISO 27001 §12.3.1.

8.2. Cloud

- Hosted on ISO 27017-compliant provider with data residency in Australia.
- Server-Side Encryption (SSE) with customer-managed keys in KMS.
- Access: via federated SSO using Azure AD conditional access.
- Monitoring: continuous compliance scanner against CIS Benchmarks.

9. Plan of Action (Information Security Management System)

The organization will implement an **ISMS** using the **ISO 27001 PDCA** cycle. KPIs include phishing click-rate < 5 %, mean time to detect < 1 hour, and patch compliance > 95 %.

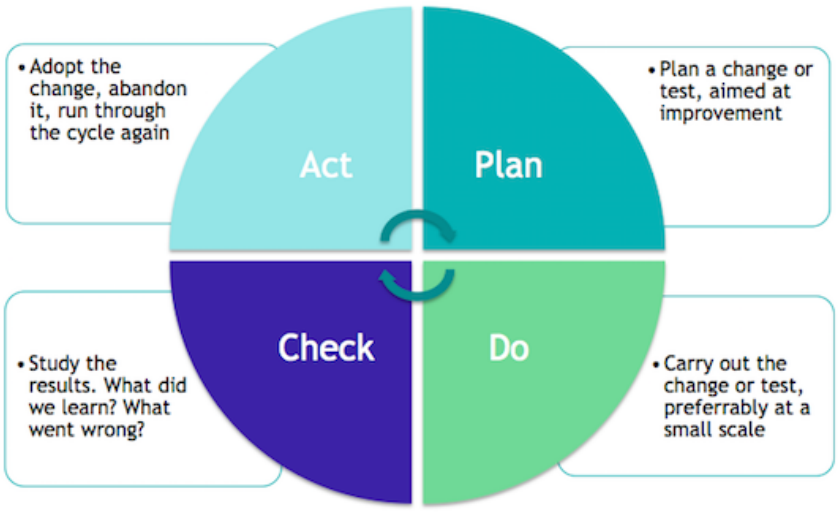

Figure 1: Information Security and PDCA

- **Plan**: identify assets, assess risks, establish controls.
- **Do**: implement training, MFA, encryption, and monitoring.
- **Check**: quarterly audits, monthly metrics, annual penetration tests.
- **Act**: update policies, patch emerging vulnerabilities, review incidents.

To operationalize the ISMS and ensure rapid containment of threats, an Incident Response Plan (IRP) will define detection, analysis, containment, eradication, recovery, and post-incident review stages (NIST SP 800-61 Rev. 2). Each incident type (phishing, malware, data-loss, or insider misuse) has a corresponding playbook outlining immediate actions, responsible teams, and communication protocols. The escalation chain moves alerts from the SOC to the CISO, then to the Executive Team if impact thresholds are exceeded. This structure complements the PDCA cycle by turning “Check” findings into actionable lessons, strengthening resilience and compliance with ISO 27035:2023 Information Security Incident Management. See Appendix B for an incident-response flowchart and escalation model.

9.1. ISMS Monitoring and Review Cadence

The PDCA cycle operates at multiple time horizons to balance operational responsiveness with strategic oversight:

- Daily Operations:
    - Automated SIEM correlation rules trigger alerts for anomalous access patterns
    - EDR agents report suspected malware to SOC analysts for triage
    - Automated backup validation checks confirm data integrity
- Weekly Reviews (IT Operations):
    - Patch compliance dashboard reviewed against >95% target
    - Phishing simulation results analyzed (targeting <5% click-through rate)
    - Help desk tickets tagged "security incident" escalated to CISO team
- Monthly Governance (Security Committee):
    - KPI trend analysis presented to IT leadership
    - Risk register reviewed for newly discovered vulnerabilities (CVE tracking)
    - Budget allocation decisions for emerging security tools
- Quarterly Deep Dives (CISO + Department Heads):
    - Full risk re-assessment using ISO 27005 methodology
    - Training effectiveness measured: LMS completion rates correlated with incident reduction

    - Tabletop exercises simulating ransomware or data breach scenarios

- Annual Strategic Reviews (Executive Team + Board):

    - Third-party penetration testing validates perimeter defenses
    - Internal audit confirms ISO 27001 compliance readiness - Maturity assessment using frameworks like NIST CSF or ACSC Essential Eight.

This multi-layered rhythm ensures that tactical issues (like a suspicious login) surface within minutes, while strategic decisions (like adopting zero-trust architecture) benefit from months of trend analysis. As Calder (2020) emphasizes, "information security management is a continuous process, not a project with an end date" (p. 15).

10. Business Continuity Plan (BCP)

Business continuity complements the ISMS by ensuring resilience.

- Recovery Time Objective (RTO): 4 hours.
- Recovery Point Objective (RPO): 15 minutes.
- Redundancy: hot-site replica for on-prem servers; multi-zone cloud replication.
- Backup: encrypted off-site storage with quarterly restore tests.
- Communication: predefined escalation chain and crisis-comms template.

BCP testing will be tested at least twice yearly, coordinated by IT Operations and audited by Internal Audit. This aligns with ISO 22301(2019).

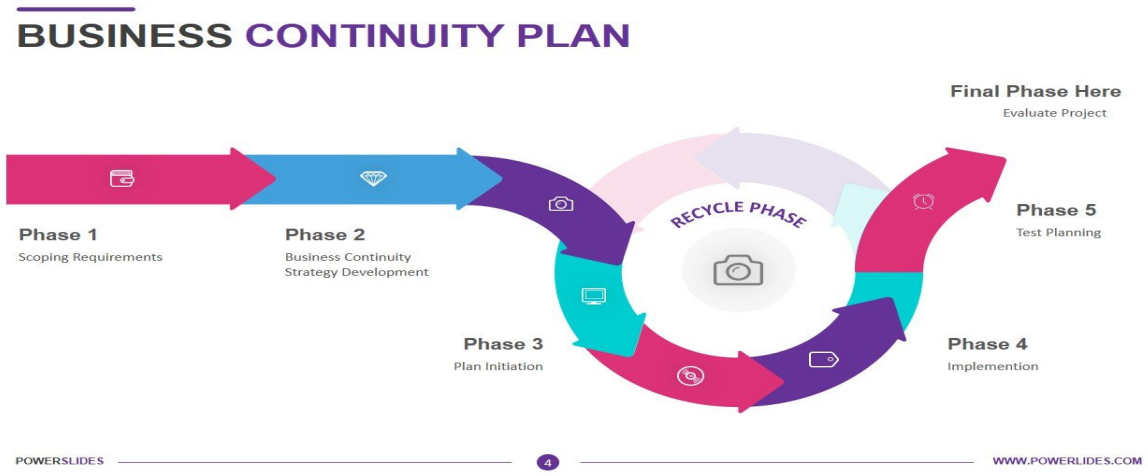

Figure 2: Business Continuity Plan

11. Balancing Service Quality and Security

Security that frustrates users fails in practice. Doctors need rapid access to medical dashboards, and Retailers require uninterrupted data-visualization tools.

11.1. Usability challenges

- Excessive authentication prompts slow down clinical workflows.
- Over-segmentation may block legitimate cross-team collaboration.

11.2. Solutions

- Single Sign-On (SSO) with adaptive MFA: low-risk logins stay frictionless; anomalies trigger extra verification.
- Transparent encryption: AES at storage layer, invisible to end-users.
- Automated patching: done off-peak to avoid downtime.
- User feedback loop: post-incident reviews collect usability insights.

- Transparent Data Encryption (TDE): storage-layer encryption rather than application-level encryption. This means analysts interact with data normally, no decryption prompts, no workflow interruption, while all hospital records remain AES-256 encrypted at rest. The encryption is invisible to users but visible to auditors, satisfying both ISO 27001 §10.1 compliance requirements and the usability principle from ISO 9241-210 that "security controls should not impede the user's primary task."

Metrics such as Mean Time to Authenticate, Incident Closure Rate, and Employee Satisfaction with IT security will measure this balance.

Following ISO 9241-210 (Ergonomics of Human-System Interaction) ensures human-centred design remains part of security decisions.

12. Continuous Improvement and Next Steps

1. Conduct annual third-party penetration testing to validate resilience.
2. Introduce behavioral analytics in IAM to flag anomalies without intruding on workflow.
3. Extend Secure by Design into DevSecOps pipelines, embedding static code analysis and dependency scanning for all applications.
4. Participate in the Australian Cyber Security Centre (ACSC) partnership program for threat intelligence sharing.

This approach aligns with the Secure Development Lifecycle (SDLC) principles defined by Microsoft (2022) and NIST SP 800-64 Rev.2, ensuring that security is embedded in requirements, design, implementation, verification, and maintenance stages.

13. Implementation Plan and Timeline

The Secure-by-Design framework will be rolled out over a 12-month roadmap, divided into four main phases. Each phase has clear deliverables, owners, and priorities. This ensures progressive implementation without disrupting daily operations.

Phase	Time	Key deliverables	Priority	Owners	Notes / Dependencies
1 - Foundation	Months 1 - 2	Establish Security Governance Committee; Approve Information Security Policy; Perform full Risk Assessment (ISO 27005); Define RBAC roles for Doctors/Retailers.	Critical	CISO / IT Sec Manager	Must be completed before system-level controls are applied.
2 - Technical Hardening	Months 3 - 5	Deploy MFA across all systems; Configure Firewall + IDS/IPS; Implement Endpoint Detection and Response (EDR); Apply AES-256 encryption and TLS 1.3; Begin patch automation.	Critical	IT Infra Lead	MFA rollout and encryption are prerequisites for data compliance.
3 - Organizational Enablement	Months 6 - 8	Deliver company-wide training program; Conduct phishing simulation #1; Launch internal security portal; Document BCP	High	HR / Training Lead / CISO	Training outcomes feed into ISMS KPIs.

		procedures; Initiate quarterly ISMS audit cycle.			
4 - Monitoring and Optimization	Months 9 - 12	Deploy SIEM integration; Conduct penetration test; Test disaster recovery failover; Evaluate metrics (MTTD, MTTD, phishing rate); Present "Year-One Security Review."	Medium	CISO / Internal Audit / Ops	Use results to refine PDCA cycle for Year Two.

13.1. Key Milestones

- Month 2: Policy approval and risk register finalized.
- Month 5: MFA + encryption live across both domains.
- Month 8: Training completion ≥ 90 % staff certified.
- Month 12: Pen test passed, residual risk below threshold.

13.2. Prioritization rationale

Controls are ranked by business impact and risk reduction efficiency.

- Critical: required to prevent major compliance or data-breach risk (e.g., MFA, encryption).
- High: supports governance, awareness, and detection.
- Medium: optimizes monitoring and maturity.

13.3. Implementation Oversight

The Security Governance Committee will track progress through monthly reports to the Executive Team. Each control will be mapped to the relevant ISO/NIST clause to ensure traceability during audits

14. Conclusion

The plan translates Secure-by-Design from concept to operational reality. By combining user education, risk-based technical controls, and continuous monitoring, the organization can protect both hospital and retail data without degrading service.

Cyber-security is not a one-time project but a continuous practice of anticipating, adapting, and improving. When people, processes, and technology align, the result is trust from clients, regulators, and employees alike.

15. Appendices

15.1. Appendix A - Glossary

Term	Definition
RBAC	Role-Based Access Control - method of regulating access to systems and data based on the roles of individual users.
MFA	Multi-Factor Authentication - security system that requires more than one method of authentication from independent categories.
SIEM	Security Information and Event Management - software that provides real-time analysis of security alerts generated by applications and network hardware.
IAM	Identity and Access Management - framework for managing digital identities and controlling user access to critical information.
EDR	Endpoint Detection and Response - system to monitor end-user devices for signs of malicious activity.
TLS	Transport Layer Security - cryptographic protocol for secure communication over a computer network.
AES-256	Advanced Encryption Standard with 256-bit keys - widely used encryption standard for securing data.
ISMS	Information Security Management System - a systematic approach to managing sensitive company information so that it remains secure.
PDCA	Plan-Do-Check-Act - a four-step management method used for continuous improvement of processes and products.
CIA Triad	Confidentiality, Integrity, Availability - the core principles of information security.
BCP	Business Continuity Plan - strategy that outlines procedures and instructions an organization must follow in the face of disaster.
HSM	Hardware Security Module - a physical device that safeguards and manages digital keys for strong authentication and encryption.
DLP	Data Loss Prevention - strategy to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.
CASB	Cloud Access Security Broker - security policy enforcement point between cloud service consumers and providers.
KMS	Key Management Service - a service that manages cryptographic keys for your cloud services.
CDN	Content Delivery Network - a system of distributed servers that deliver pages and other web content to users based on their geographic locations.
SPF/DKIM/DMARC	Email authentication protocols that are used to protect against spoofing and phishing.
IRP	Incident Response Plan

15.2 Appendix B – Incident Response Plan (IRP)

The organization's IRP is operationalized through structured playbooks for each attack vector (phishing, malware, data-loss, insider misuse). The flowchart below shows the escalation chain from the Security Operations Center (SOC) to executive decision-making, following NIST SP 800-61 Rev. 2 and ISO 27035:2023. Each event concludes with a post-incident review feeding lessons into the ISMS improvement cycle. Incident playbooks are reviewed semi-annually and updated following each post-incident review.

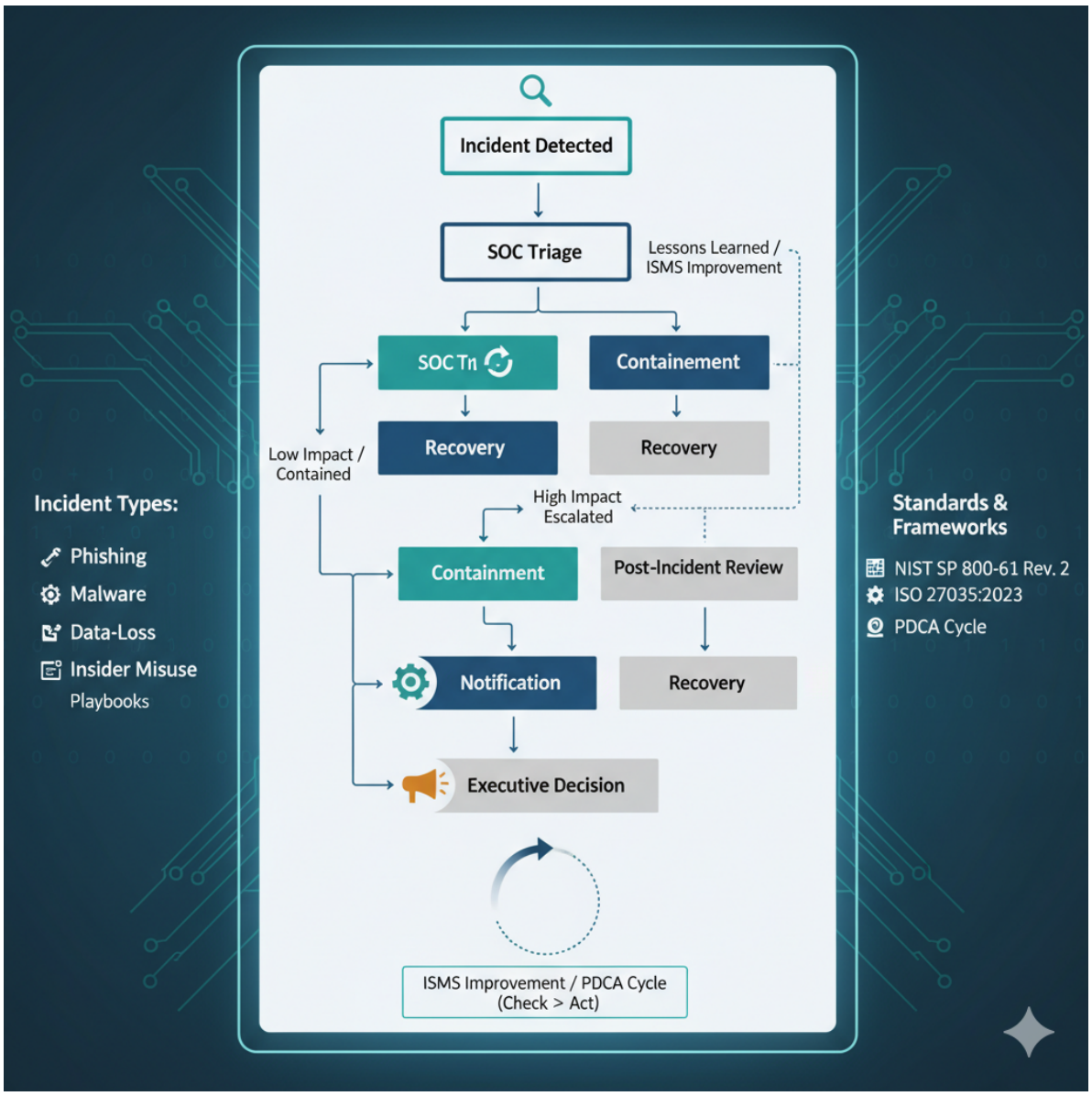

Figure 3: Incident Response Flowchart and Escalation Chain. Adapted from NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide and ISO/IEC 27035:2023 Information Security Incident Management. The diagram illustrates detection, triage, containment, notification, and post-incident review aligned with the PDCA improvement cycle.

Statement of Acknowledgment

I acknowledge that I have used the following AI tool(s) in the creation of this report:

- OpenAI ChatGPT (GPT-5): Used to assist with outlining, refining structure, improving clarity of academic language, and supporting with APA 7th referencing conventions.

I confirm that the use of the AI tool has been in accordance with the Torrens University Australia Academic Integrity Policy and TUA, Think and MDS's Position Paper on the Use of AI. I confirm that the final output is authored by me and represents my own critical thinking, analysis, and synthesis of sources. I take full responsibility for the final content of this report.

16. References

Australian Cyber Security Centre (ACSC). (2023). Essential Eight Maturity Model. https://www.cyber.gov.au/

Calder, A. (2020). *Information security management: The organizational context.* In IT Governance: An International Guide to Data Security and ISO27001/ISO27002 (7th ed., pp. 12-28). IT Governance Publishing.

Hillman, D., Harel, Y., & Toch, E. (2023). *Evaluating organizational phishing awareness training on an enterprise scale*. Computers & Security, 132, 103364.

Howard, M., & LeBlanc, D. (2003). *Writing secure code* (2nd ed.). Microsoft Press.

International Organization for Standardization (ISO). (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. ISO.

International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems. ISO.

International Organization for Standardization (ISO). (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. ISO.

International Organization for Standardization (ISO). (2018). ISO 31000:2018 Risk management – Guidelines. ISO.

International Organization for Standardization (ISO). (2022). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on managing information security risks. ISO.

International Organization for Standardization (ISO). (2019). ISO 9241-210:2019 Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems. ISO.

National Institute of Standards and Technology (NIST). (2023). Special Publication 800-63B: Digital Identity Guidelines. U.S. Department of Commerce. https://pages.nist.gov/800-63-3/sp800-63b.html

National Institute of Standards and Technology (NIST). (2020). Special Publication 800-52 Rev. 2: Guidelines for the Selection and Use of Transport Layer Security (TLS). U.S. Department of Commerce.

National Institute of Standards and Technology (NIST). (2017). Special Publication 800-92: Guide to Computer Security Log Management. U.S. Department of Commerce.

National Institute of Standards and Technology (NIST). (2022). Special Publication 800-64 Rev. 2: Security Considerations in the System Development Life Cycle. U.S. Department of Commerce.

OWASP Foundation. (2024). *OWASP Top 10: Web application security risks*. https://owasp.org/Top10/

Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley.

Steinberg, J. (2020). *Cybersecurity for Dummies*. Wiley.

Sutton, M. (2022). *The Complete Guide to Cyber Threats*. Springer.

Taneski, V., Heričko, M., & Brumen, B. (2019). *Systematic overview of password security problems*. Acta Polytechnica Hungarica, 16(3), 143-165.

Tisdale, S. M. (2015). *Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks.* Journal of Information Systems Education, 26(2), 65–73.