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 3
2. Context and Secure-by-Design Principles 3
3. User Training and Awareness Program 4
4. Risk Assessment 5
5. Mitigation Methods 6
5.1. Technical Controls 6
5.2. Organizational Controls 6
6. User Rights and Access Control 8
7. Password and Authentication Policy 8
8. Storage Security Controls 9
8.1. Technical Controls 9
8.2. Cloud 9
9. Plan of Action (Information Security Management System) 10
10. Business Continuity Plan (BCP) 10
11. Balancing Service Quality and Security 11
11.1. Usability challenges 11
11.2. Solutions 12
12. Continuous Improvement and Next Steps 12
13. Implementation Plan and Timeline 13
13.1. Key Milestones 14
13.2. Prioritization rationale 14
13.3. Implementation Oversight 15
14. Conclusion 15
15. Appendices 16
15.1. Appendices A - Glossary 16
16. References 18

Secure By Design Implementation Guide

1. Executive Summary

This guide defines how the organization, which happens to be 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.

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.

Secure-by-Design means integrating protection at every phase of the system life cycle rather than adding controls after deployment (Shostack, 2014). The foundation rests on the CIA Triad:

- **Confidentiality**: information is available only to authorised 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 largest variable in cyber defense. 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 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.

4. Risk Assessment

Risk management follows ISO 31000 and ISO 27005, evaluating likelihood × impact – mitigation. The organization re-assesses risk quarterly or after major change.

#	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	SysAdmin	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.

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.

8. Storage Security Controls

8.1. Technical Controls

- Physical security: key-card entry, CCTV, fire suppression, locked racks.
- Segmentation: hospital network separated from corporate LAN by firewall VLANs.
- Encryption: AES-256 via full-disk encryption; keys in hardware security module (HSM).
- Backup: nightly incremental + weekly full backups to offline storage; tested monthly.

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 Plan-Do-Check-Act (PDCA)** cycle.

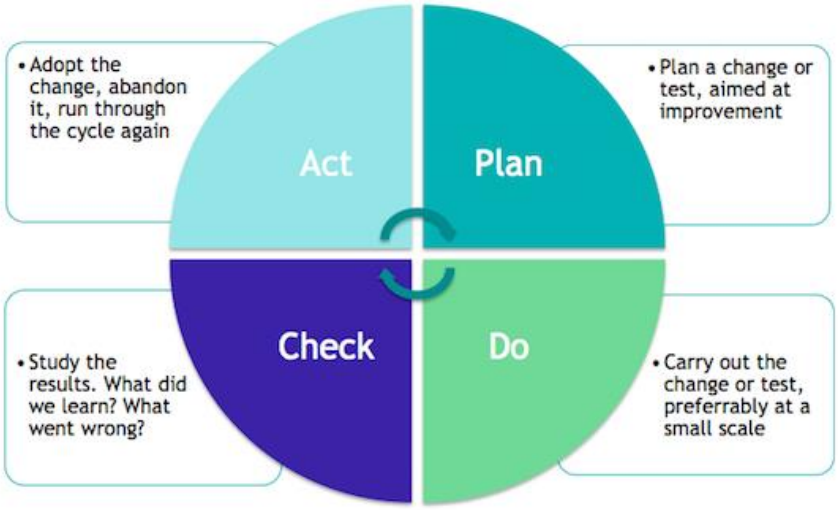

Figure 1: Information Security and PDCA

- **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.

Key performance indicators (KPIs) include phishing click-rate < 5 %, mean time to detect < 1 hour, and patch compliance > 95 %.

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).

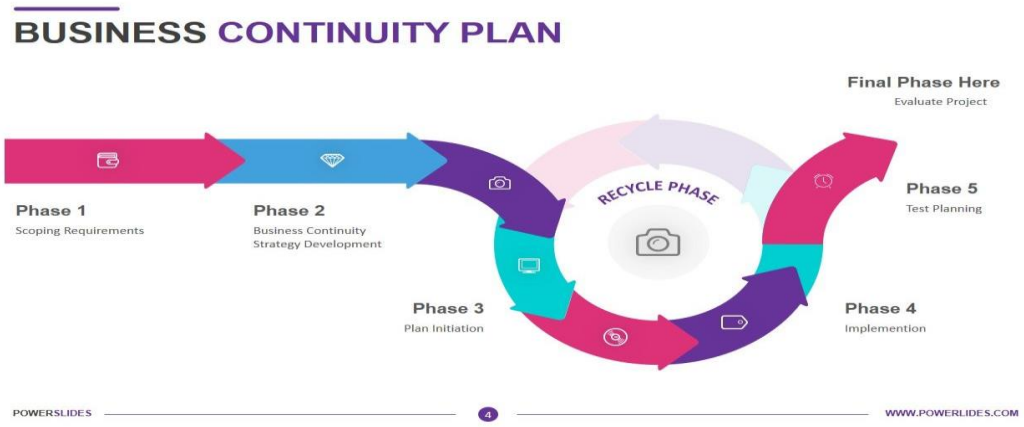

Figure 2: Business Continuity Plan

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.

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. Appendices 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.

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/

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). (2021). ISO/IEC 27017:2021 Code of practice for information security controls for cloud services. ISO.

National Institute of Standards and Technology (NIST). (2023). Special Publication 800-63B: Digital Identity Guidelines. U.S. Department of Commerce.

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.

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.