Case Study Project

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.: 3

Title of Assessment: Case Study Project

Lecturer: Dr. Tanvir Rahman

Date: Dec 2025

Table of Contents

1. Executive Summary

This report presents the secure system design for **CuraNexus Analytics**, a mid-sized analytics company integrating **hospital** and **retail** data streams into a unified platform. The application accepts user input, writes to and retrieves from a SQL database, and enforces strict access control aligned with ISO/IEC 27001:2022, NIST SP 800-64 Rev.2, and OWASP Secure Coding Guidelines (2024).

The design adopts a **Secure-by-Design (SbD)** philosophy - embedding security from the earliest development phases to ensure confidentiality, integrity, and availability (CIA triad). Controls address input validation, injection prevention, encryption, authentication, and role-based access management. The approach prioritizes human-centric usability while maintaining compliance and resilience.

2. Request Phase – Secure Data Input and Validation

The Request Phase governs how users enter and submit data through the web interface. Insecure data handling is one of the primary sources of software vulnerabilities (Sutton, 2022). Therefore, security begins at the input layer.

All data fields in the CuraNexus platform are subject to length and type validation, ensuring that inputs—such as patient names, retail records, and contact details—adhere to strict formatting standards. For example, name fields are limited to 100 characters, numeric IDs to 10 digits, and emails validated using regex patterns on both client and server sides. This prevents buffer overflow and injection vectors.

To protect against SQL injection, all database interactions employ parameterized queries and stored procedures, preventing malicious manipulation of query strings (OWASP, 2024). Inputs are sanitized using a whitelist model, where only pre-approved characters are permitted.

Authentication follows the NIST SP 800-63B framework, enforcing:

- Multi-Factor Authentication (MFA) for all administrative users.
- Password complexity policies (minimum 12 characters, mixed types).
- Secure hashing and salting via PBKDF2 with HMAC-SHA-256.
- Automatic account lockout after five failed attempts.

Session management is implemented using JWT tokens signed with RSA 2048-bit encryption, with expiry times to limit exposure.

The application is developed in Python (Django), chosen for its memory-safe architecture and broad security libraries. Compared to low-level languages like C/C++, Python mitigates buffer overflow and pointer misuse risks (Steinberg, 2020).

All actions are logged through a centralized SIEM integrated with ACSC Essential Eight monitoring practices to detect anomalies. Logs capture timestamps, user IDs, and IPs for accountability and compliance (ISO/IEC 27001 §12.4).

"Secure coding standards are the foundation of resilience against injection and authentication flaws." (Sutton, 2022)

2.1.Field Specifications and Validation Logic

All input fields are constrained to prevent buffer overflow and injection attacks:

Field	Max Length	Validation Rule	Justification
Name	100 chars	`^[A-Za-z\s'-]{2,100}$`	Accommodates hyphenated surnames and cultural naming (e.g., "O'Brien", "García-López") per Unicode TR36
Street Address	150 chars	`^[A-Za-z\s'-]{5,150}$`	Longest Australian street name is ~60 chars; 150 allows for unit numbers and landmarks
Postal Code	4 chars	`^\d{4}$`	Australian postcodes are exactly 4 digits (NIST SP 800-63B §5.1.3)
State/Suburb	15 chars	`^[A-Za-z\s'-]{5,15}$`	
City	30 chars	`^[A-Za-z\s'-]{5,30}$`	
Phone	15 chars	`^\+?[\d\s()-]{10,15}$`	ITU E.164 international format supports +61 country code + 10 digits
Email	254 chars	RFC 5321 regex	Maximum email length per SMTP standard
Medical Status	ENUM	Dropdown (no free text)	Prevents injection; values: {Sick, Healthy, Cancer, Deceased, Flu, Covid}
Credit Card	19 chars	`^\d{13,19}$` (masked display)	Visa/MC/Amex range; stored encrypted per PCI-DSS 3.2.1

Wildcard Search Security: Name and phone fields support wildcard searches using the SQL `LIKE` operator with parameterized bindings. User input is sanitized to escape `%`, `_`, and `\` characters, preventing pattern injection. Example: searching "O'B%" becomes `LIKE 'O\'B\%'` via prepared statement binding.

Overflow Protection: Server-side validation occurs before ORM processing. Requests exceeding field limits return HTTP 400 with error: "Field [name] exceeds maximum length of [X] characters." Client-side JavaScript provides real-time feedback, but server validation is authoritative (OWASP ASVS 4.0 V5.1.2).

3. Retrieve Phase – Secure Data Retrieval and Encryption

The Retrieve Phase handles SQL queries and database outputs returned to users. CuraNexus employs a tiered encryption strategy—data in transit is protected with TLS 1.3, while data at rest uses AES-256-GCM encryption. The design ensures data confidentiality without compromising performance (Calder, 2020).

All SQL statements are executed through ORM abstractions rather than direct raw queries, significantly reducing injection risk. Least Privilege Access is applied to all database accounts—each role has its own credentials, and connections are audited via service accounts (ISO/IEC 27002 §9).

For cross-site protection, output data is HTML-encoded to prevent Cross-Site Scripting (XSS), and cookies are set as HttpOnly and Secure. Sensitive responses, such as medical reports or sales analytics, are transmitted only over HTTPS with HSTS enabled.

Retrieval responses undergo additional plausibility checks before rendering. For instance, a doctor requesting retail data will receive a denial message since their scope is limited to medical

analytics. Similarly, accounting users accessing medical databases will trigger an alert within the SIEM environment for review.

System reliability is further supported by daily encrypted backups stored offsite in AWS S3 Glacier, using separate encryption keys. Database queries and read operations are load-balanced to preserve availability during peak access periods (Vacca, 2014).

"Encryption is not an afterthought—it is the backbone of trust in digital systems." (Calder, 2020)

4. Review Phase – Role-Based Access Control and Auditing

CuraNexus enforces Role-Based Access Control (RBAC), defining permissions aligned with organizational functions:

Role	Access Scope	Privileges
Standard Users (Doctors, Retail Analysts)	Read-only to relevant data domain	View reports and analytics dashboards
Accounting / Management Users	Read & Write	Upload transaction or medical billing data
Privileged IT / Admin Users	Full control	Manage roles, monitor logs, perform maintenance

Each access token carries embedded claims (role, department, validity) and is verified using RSA signatures. Separation of Duties ensures that privileged accounts cannot modify audit logs or their own permissions (ISO/IEC 27001 §9.2).

User sessions automatically expire after 20 minutes of inactivity, mitigating hijacking risks. Audit logs capture every role-based access decision and are stored in immutable format within an internal Elasticsearch cluster for compliance tracking.

The RBAC model follows the Principle of Least Privilege, supported by ISO/IEC 27005 (risk-based controls) and NIST SP 800-64 Rev.2.

"Role-based control systems translate business policy into enforceable technical boundaries." (Vacca, 2014)

5. Mitigation Methods

A DREAD-based analysis quantifies CuraNexus's high-priority risks.

Factor	Score (1-10)	Description
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.

Mitigation measures:

- Parameterized queries prevent injection attempts.
- Least privilege limits exposure to compromised accounts.

- MFA reduces credential theft success rates.
- Automated alerts and SIEM correlation rules detect anomalies in real time.

According to Vellani (2007), “quantified risk frameworks like DREAD enable prioritisation of remediation efforts and security investment.”

Residual risk remains low after applying compensating controls and continual improvement under the Plan-Do-Check-Act (PDCA) model.

6. Encryption and Key Management

Encryption keys are centrally managed using an HSM (Hardware Security Module) with periodic rotation every 12 months or after any breach event.

- Data Encryption: AES-256-GCM for all SQL tables containing personally identifiable information (PII).
- Key Exchange: RSA-2048 for secure key transfer and handshake.
- Secure Hashing: SHA-256 applied to sensitive identifiers (e.g., Medicare IDs).

Keys are separated by environment (production/test) and stored outside application containers. Only the Information Security Manager can approve key rotation cycles.

TLS configurations disable legacy protocols (SSL, TLS 1.2) and weak ciphers. HSTS headers ensure encrypted continuity between user and system. Periodic key audits and penetration testing validate the integrity of the encryption ecosystem (Erbschloe, 2005).

7. Integration with ISMS and Business Continuity

CuraNexus aligns this software design with its Information Security Management System (ISMS) from Assessment 2. Incident response (IRP) and business continuity (BCP) are connected:

- IRP triggers when anomaly thresholds in SIEM exceed limits.
- BCP ensures data restoration within 4 hours (RTO) using encrypted cloud backups.
- Post-incident reviews update security playbooks per ISO 22301 and ISO/IEC 27035.

This ensures not only protection against breaches but rapid containment and learning cycles, hallmarks of Secure-by-Design resilience (Mead & Woody, 2017).

8. Conclusion

Through proactive design, CuraNexus Analytics embeds security into every development layer - people, process, and technology. From validated input to encrypted storage and risk-based access control, the system exemplifies Secure-by-Design principles guided by international standards. By continuously auditing, encrypting, and training, CuraNexus reduces risk exposure, builds trust, and ensures operational resilience in handling sensitive hospital and retail data.

9. Appendices

9.1. 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

9.2 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.

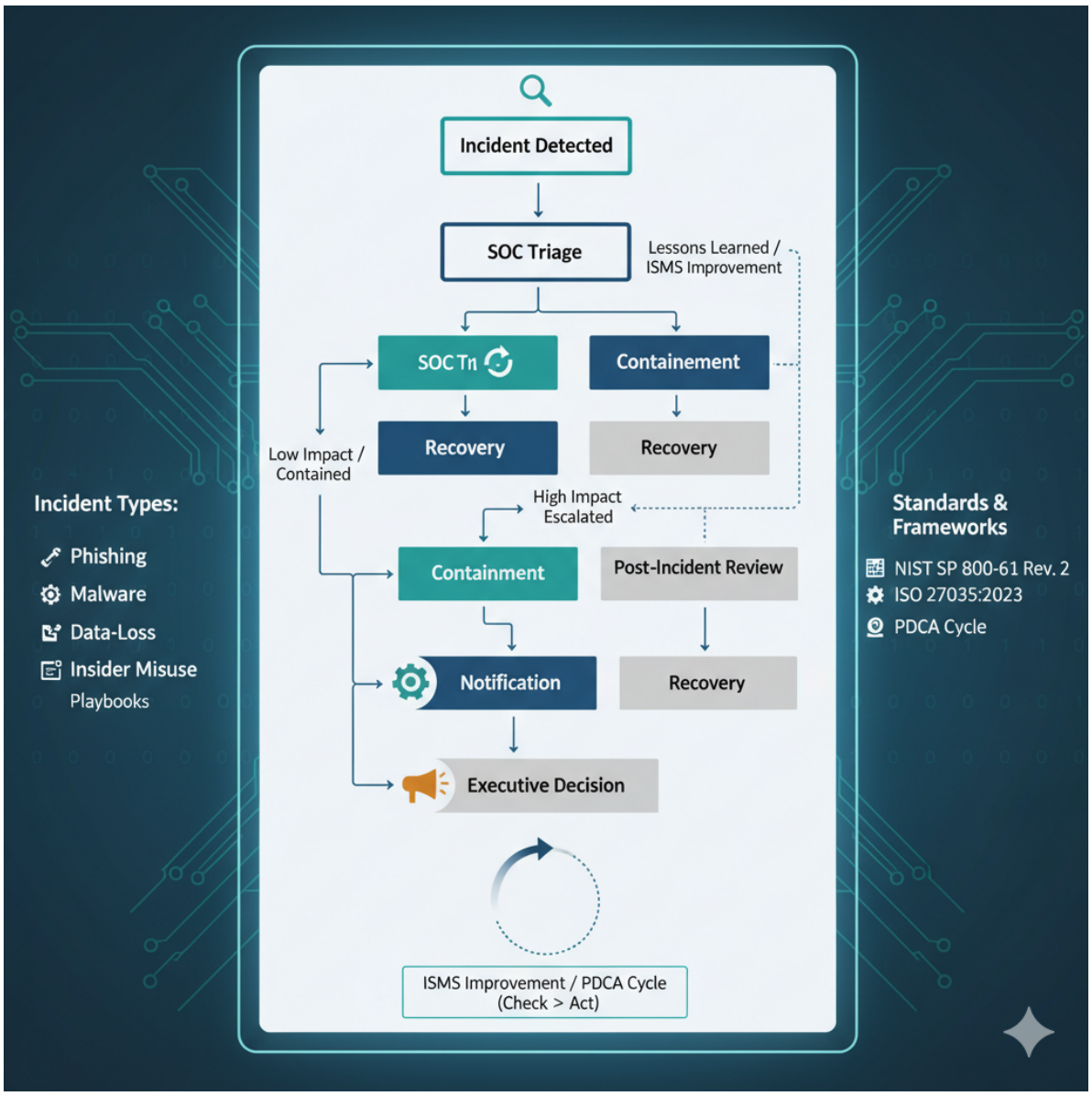

Figure 3: Incident Response Flowchart and Escalation Chain. Adapted from NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide and ISO/IEC 27035:2023 Information Security Incident Management. The diagram illustrates detection, triage, containment, notification, and post-incident review aligned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

10. 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.

Erbschloe, M. (2005). *Physical security for IT.* Digital Press.

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.

Mead, N. R., & Woody, C. C. (2017). *Cyber security engineering: A practical approach for systems and software assurance*. Addison-Wesley.

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.

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.

Vacca, J. R. (2014). *Cyber security and IT infrastructure protection.* Syngress.

Vellani, K. H. (2007). *Strategic security management: A risk assessment guide for decision makers*. Butterworth-Heinemann.