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

Insecure inputs account for major breaches (Sutton, 2022), so security starts server-side per OWASP ASVS 4.0. All inputs receive type/length checks and Unicode NFC normalization to thwart spoofing—e.g., names ≤100 chars, numeric IDs ≤10 digits, emails per RFC 5321. Client-side aids usability, but server enforcement prevails (ASVS V5.1.2).

Database interactions employ parameterized queries or stored procedures, eschewing raw SQL. Allow-lists and output encoding counter SQLi and XSS (OWASP, 2024).

For wildcard safety in business searches, suffix-only patterns (term%) are used, with % and _ escaped pre-binding. Indexing and pagination avert full-table scans (Xiao & Xiao, 2021). Where wildcards are essential:

- UI constrains to suffix-only patterns (term%) and caps term length.
- Backend escapes **%**, **_**, and \ in user input and binds patterns as parameters.
- Queries use covering indexes and pagination (e.g., limit 100, cursor-based) to avoid table scans and enumeration.
    - Example: user enters O'B% → backend binds O\'B\% to LIKE ?.

Authentication & sessions (NIST SP 800-63B): MFA is mandatory for admins and privileged actions. Passwords require ≥ 12 chars, PBKDF2-HMAC-SHA-256 hashing, and breach screening. Progressive throttling (1 → 2 → 4 s delays) and SIEM alerts block brute-force. JWTs are RSA-signed with short expiry and contain no sensitive claims.

Authentication follows NIST SP 800-63B: MFA mandatory for admins/privileged actions; passwords ≥12 chars with PBKDF2-HMAC-SHA-256 hashing and breach checks. Progressive throttling (1-4s delays) plus SIEM alerts deter brute-force. JWTs are RSA-signed, short-lived, and claim-minimal.

Database accounts (app_reader, app_writer, app_admin) reside in AWS Secrets Manager with AES-256 KMS encryption, rotating every 90 days and runtime-injected—no code-stored credentials (NIST SP 800-53 IA-5).

Request integrity mandates CSRF tokens, SameSite=strict cookies, and origin verification. Generic errors avoid leaks; logs capture user ID/IP/timestamp sans PII/credentials, feeding central SIEM under ACSC Essential Eight (ISO/IEC 27001 §12.4).

Secure coding bolsters resilience against injection/auth flaws (Sutton, 2022), though trade-offs like MFA usability require user training to balance security and efficiency.

2.1. Field Specifications and Validation Logic

All input fields are constrained to prevent 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

These balance global usability with buffer protection (OWASP ASVS V5.1.2). Overflow rejects return HTTP 400; validation precedes ORM for fail-fast.

python Copy

```python
# Safe parameterized search with suffix-only LIKE
term = normalize_to_nfc(clean_user_term(user_input))
term = escape_like(term)  # escapes %, _, \
if not valid_search_term(term): raise BadRequest()
qs = Patient.objects.filter(last_name__istartswith=term)[:100]  # indexed, paginated
```

Figure 1: Python code snippet with parameterized search using suffix-only LIKE.

3. Retrieve Phase – Secure Data Retrieval and Encryption

This phase secures queries and delivery. Transit uses TLS 1.3 with forward secrecy; at-rest employs AES-256-GCM with yearly rotation (Calder, 2020). ORM/stored procedures replace raw SQL; least-privilege accounts govern access (ISO/IEC 27002 §9).

Endpoints enforce filters/record caps (max 100); wildcards suffix-only to safeguard indexes (Xiao & Xiao, 2021). Integrity checks scope queries—e.g., doctors barred from retail data; >10,000 records prompt pagination/SIEM alerts. SHA-256 digests verify responses.

Output escapes HTML; cookies are Secure/HttpOnly/SameSite=Strict. HSTS/certificate pinning maintain HTTPS. Backups: Daily encrypted in AWS S3 Glacier, verified quarterly. Multi-zone replicas ensure uptime; retrievals log session ID/timestamp in WORM Elasticsearch (Vacca, 2014).

Encryption forms trust's core (Calder, 2020), though key management overhead demands automated tools for scalability.

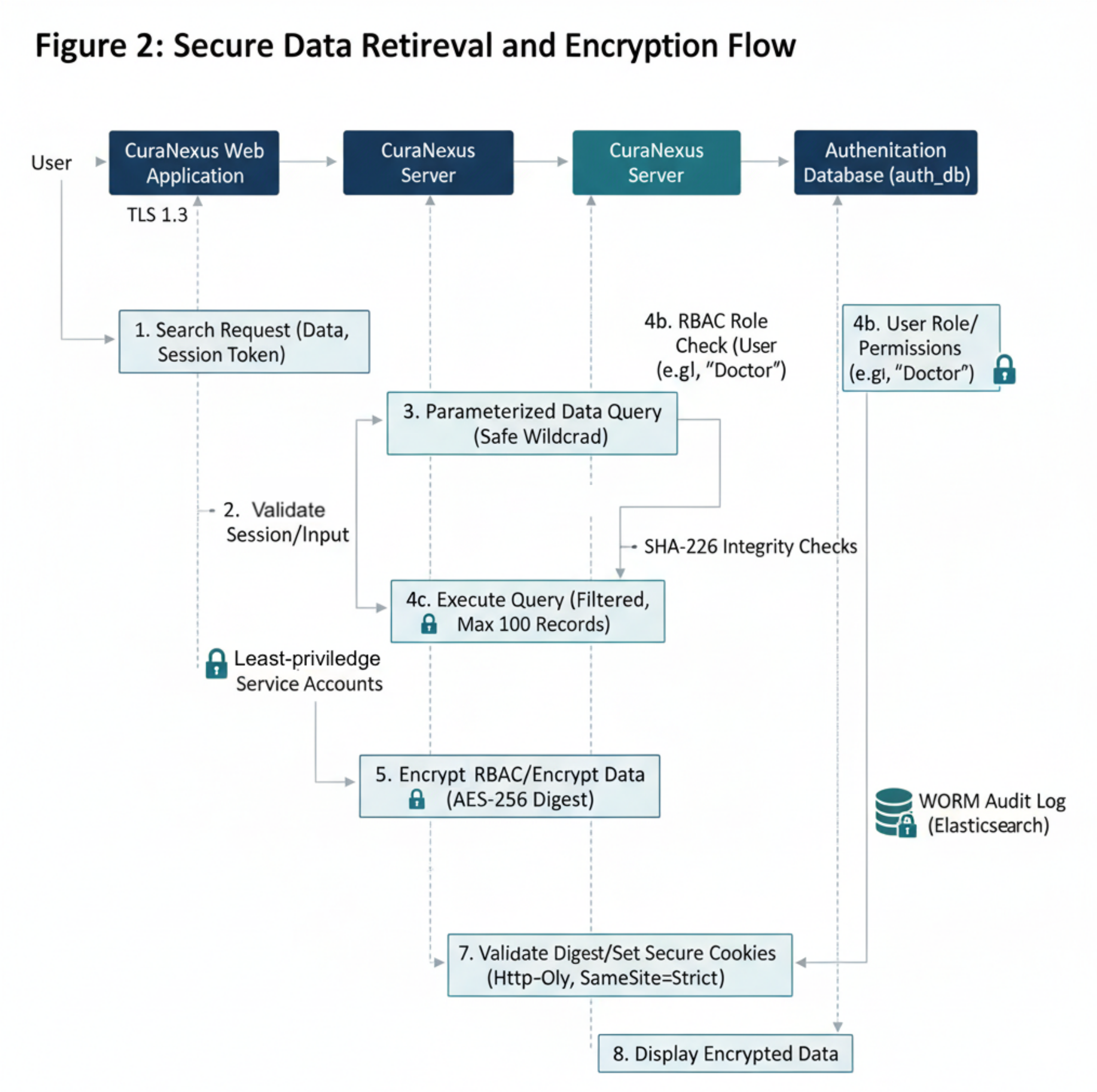

Figure 2: Data Retrieval and Encryption Flow (User → Input Validation → DB Query → RBAC Check → Encrypted Response).

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

CuraNexus enforces **Role-Based Access Control** (RBAC) to translate organizational policy into technical enforcement, with roles and scopes explicitly defined and audited quarterly.

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 to financial or billing modules	Upload transaction or medical billing data
Privileged IT / Admin Users	Full control with elevated audit accountability	Manage roles, monitor logs, perform maintenance

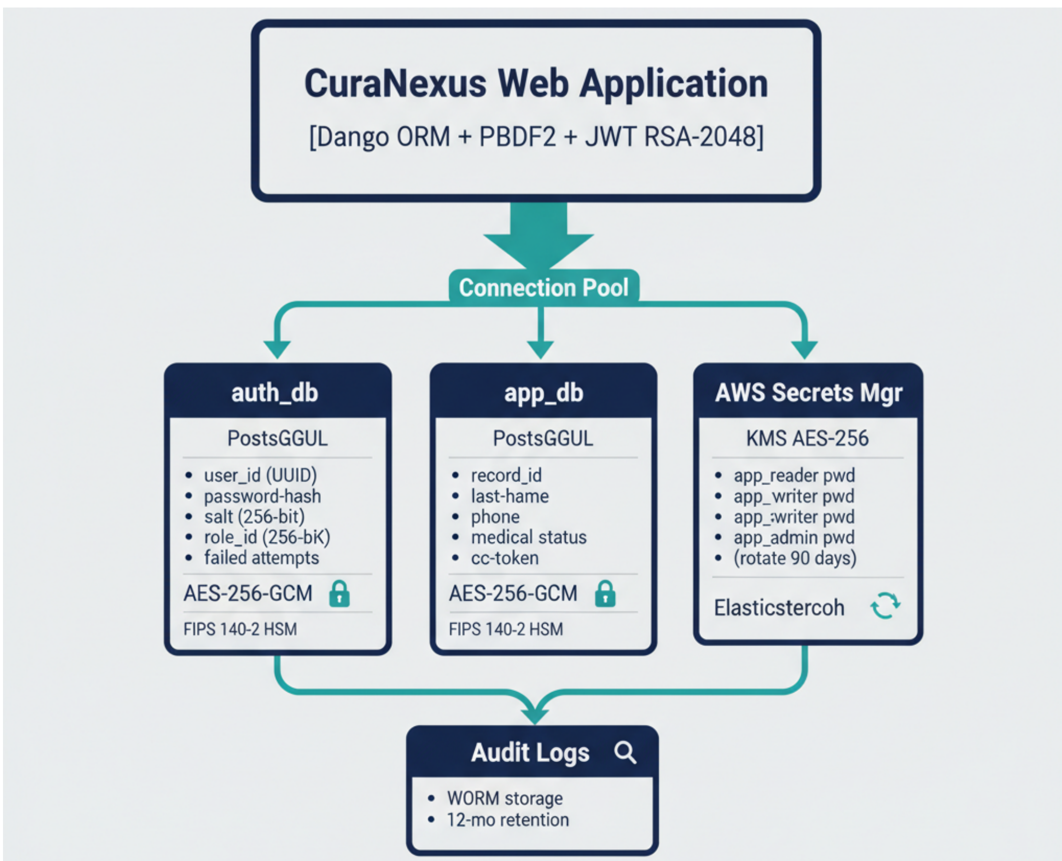

Figure 3: Database Architecture – Separation of Authentication and Application Data.

Tokens embed RSA-2048-signed claims (role/dept/expiry). SoD prevents admin self-modification (ISO/IEC 27001 §9.2); sessions expire after 20min idle/network shift. JML lifecycle: Provision/modify/revoke access with dual approval for privileged roles; quarterly attestation ensures least-privilege (ISO/IEC 27005).

Logs hash-chain events stored immutably 12 months; SIEM correlates/alerts reviewed <24hrs. This supports continuity/forensics per NIST SP 800-64 Rev. 2, though RBAC rigidity may require hybrid ABAC for dynamic environments.

RBAC translates policy into boundaries (Vacca, 2014).

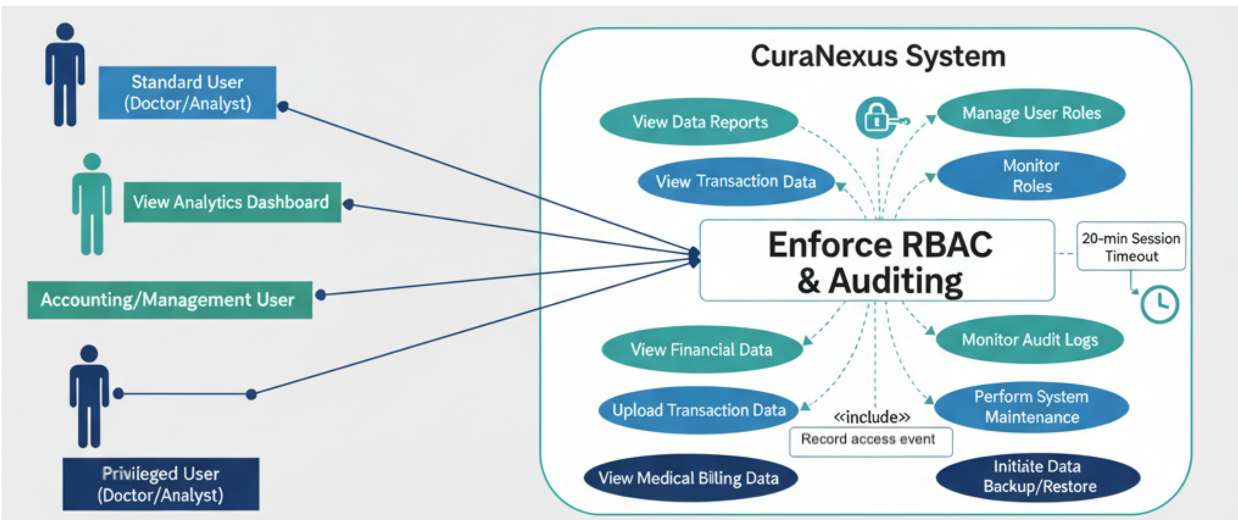

Figure 4: Use Case Diagram with RBAC.

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 prioritization 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 SBD 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	Meaning	Description
AES-256 (GCM)	Advanced Encryption Standard	Uses 256-bit keys in Galois/Counter Mode; protects data at rest.
BCP	Business Continuity Plan	A strategy defining how critical systems and data are restored following a disruption.
CIA Triad	Confidentiality, Integrity and Availability	Core security model comprising Confidentiality, Integrity and Availability.
CSRF	Cross-Site Request Forgery	Attack that tricks a user into performing unwanted actions on a trusted web application.
HSM	Hardware Security Module	Dedicated hardware device used to generate, store and manage cryptographic keys securely.
ISMS	Information Security Management System	ISO/IEC 27001 framework governing information-security policies, procedures and continual improvement.
JWT	JSON Web Token	Signed token format for securely transmitting authentication claims between client and server.
MFA	Multi-Factor Authentication	Login control requiring two or more independent factors to verify user identity.
RBAC	Role-Based Access Control	Authorization model assigning permissions to roles rather than individuals.
SIEM	Security Information and Event Management	Centralized platform that aggregates, correlates and analyses logs for threat detection.
TLS 1.3	Transport Layer Security	Cryptographic protocol securing data in transit with forward secrecy and modern cipher suites.
PDCA	Plan-Do-Check-Act	Continuous-improvement cycle used in ISO management systems to maintain and enhance controls.

9.2 Appendix B – One-Page Poster

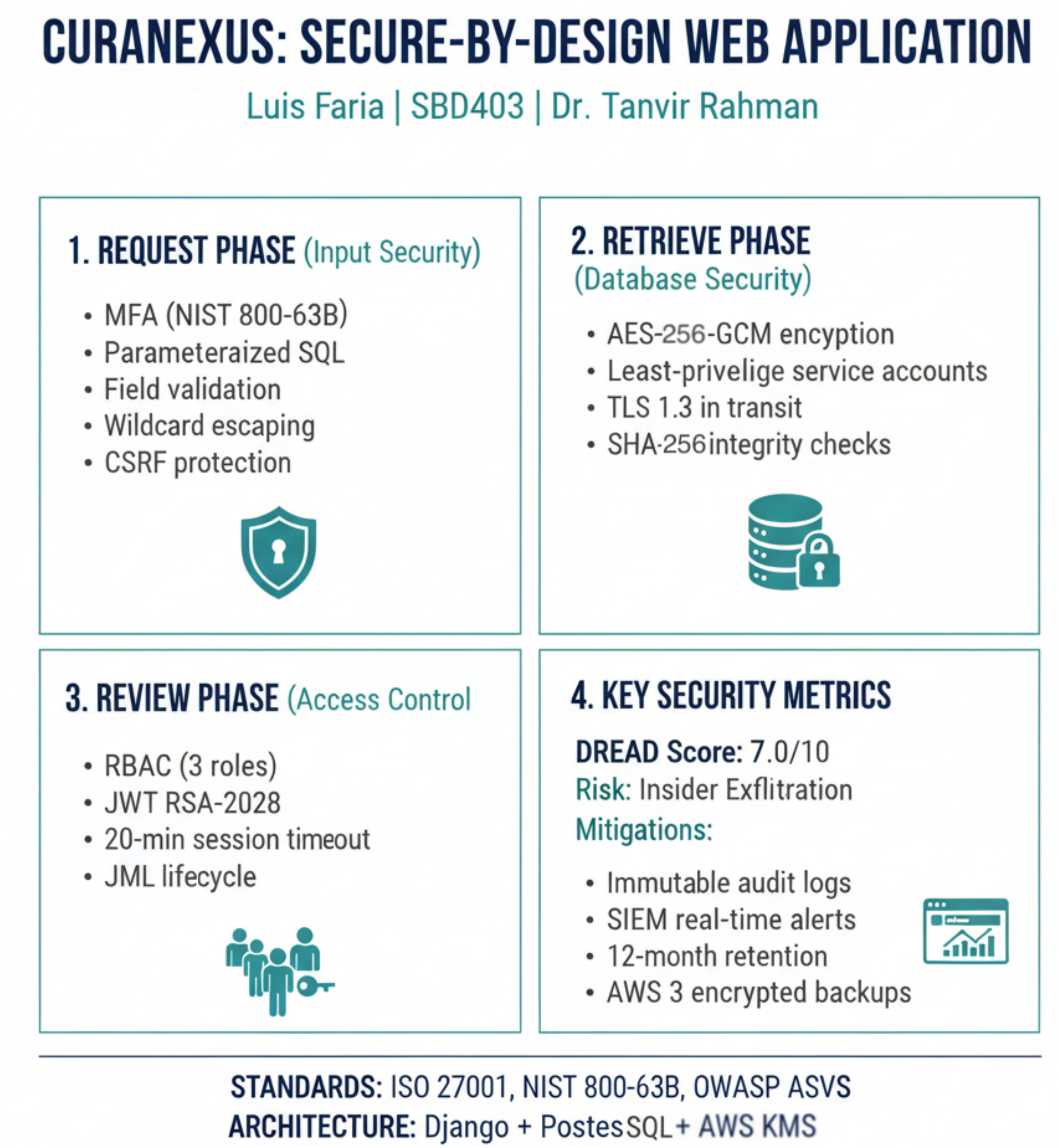

Figure 5: One-Page Poster with CuraNexus Web App's details.

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). (2018). ISO 31000:2018 Risk management – Guidelines. ISO.

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

International Organization for Standardization. (2023). ISO/IEC 27035:2023: Information security incident management. ISO.

National Institute of Standards and Technology. (2012). Special Publication 800-61 Rev. 2: Computer security incident handling guide (NIST SP 800-61). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2

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

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). (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. (2020). Special Publication 800-53 Rev. 5: Security and privacy controls for information systems and organizations (NIST SP 800-53). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

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.

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

OWASP Foundation. (2024). Application security verification standard (ASVS) 4.0. https://owasp.org/www-project-application-security-verification-standard/

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.

Xiao, X., & Xiao, S. (2021). *Database security: Concepts, approaches, and challenges.* IEEE Transactions on Dependable and Secure Computing, 18(3), 1324-1339.