**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

Copyright © 2025 by Luis G B A Faria

Permission is hereby granted to make and distribute verbatim copies of this document provided the copyright notice and this permission notice are preserved on all copies.

**Table of Contents**

[**1.** **Executive Summary** 3](#_Toc215046480)

[**2.** **Request Phase – Secure Data Input and Validation** 3](#_Toc215046481)

[2.1. Input Validation & Wildcard Handling 3](#_Toc215046482)

[2.2. Authentication & Session Security 4](#_Toc215046483)

[2.3. Secure Transport & Credential Handling 5](#_Toc215046484)

[2.4. Request Integrity, Error Handling and Logging 5](#_Toc215046485)

[2.5. Field Specifications and Validation Logic 5](#_Toc215046486)

[**3.** **Retrieve Phase – Secure Data Retrieval and Encryption** 6](#_Toc215046487)

[3.1. Secure Query Execution 7](#_Toc215046488)

[3.2. Authorization and Record Scoping 7](#_Toc215046489)

[3.3. Encryption in Transit and at Rest 7](#_Toc215046490)

[3.4. Output Encoding & Response Hardening 8](#_Toc215046491)

[3.5. Logging, Backups & High Availability 8](#_Toc215046492)

[3.6. Field-Length Enforcement at Database Layer 8](#_Toc215046493)

[**4.** **Review Phase – Role-Based Access Control and Auditing** 9](#_Toc215046494)

[4.1. Role Definitions and Access Scopes 10](#_Toc215046495)

[4.2. Technical Enforcement 10](#_Toc215046496)

[4.3. Preventing Privilege Escalation 10](#_Toc215046497)

[4.4. Auditing and Log Integrity 11](#_Toc215046498)

[**5.** **Mitigation Methods** 13](#_Toc215046499)

[5.1. General Risk Profile for Web Data Retrieval Applications 14](#_Toc215046500)

[**6.** **Encryption and Key Management** 14](#_Toc215046501)

[**7.** **Integration with ISMS and Business Continuity** 15](#_Toc215046502)

[**8.** **Conclusion** 15](#_Toc215046503)

[**9.** **Appendices** 16](#_Toc215046504)

[9.1. Appendix A – Glossary 16](#_Toc215046505)

[9.2 Appendix B – One-Page Poster 17](#_Toc215046506)

[**10.** **References** 19](#_Toc215046507)

# **Executive Summary**

This report presents a security design guide for web-based data retrieval applications, demonstrated through CuraNexus Analytics—a reference implementation integrating hospital and retail data streams. The guide adopts a Secure-by-Design 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 while maintaining compliance, usability and resilience.

# **Request Phase – Secure Data Input and Validation**

Security begins in the Request Phase, where all incoming data is validated, authenticated, and securely transported before reaching backend systems. Following OWASP ASVS 4.0, validation occurs **server-side** using strict type checks, length limits, and Unicode normalization to prevent spoofing or malicious character manipulation (Sutton, 2022). Client-side checks support usability but never replace enforcement.

# Input Validation & Wildcard Handling

All fields undergo strict allow-list validation and length constraints (Table 2.5). SQL injection is prevented through parameterized queries or stored procedures; raw SQL is never permitted. To safely support wildcard searches:

* UI constrains to **suffix-only** patterns (e.g., term%).
* Backend escapes **%**, **\_**, and **\** in user input and binds patterns as parameters.
* Indexing and pagination prevent enumeration (Xiao & Xiao, 2021)

*Example: entering* ***O'B%*** *becomes a safely escaped* ***O\'B\%*** *parameterized LIKE query.*

# Authentication & Session Security

Authentication follows NIST SP 800-63B:

* MFA is mandatory for admins and privileged actions.
* Passwords require ≥ 12 chars, PBKDF2-HMAC-SHA-256 hashing, and breach screening.
* Brute-force mitigation: progressive delays (1→2→4s) and SIEM alerts
* Lockout: after 5 failed attempts → 30-min lockout + SIEM alert (ISO/IEC 27001 §12.4)
* Sessions: RSA-signed JWTs with short expiry, no sensitive claims, rotation every 15 minutes, invalidated on logout.

**Bot and Automated Attack Prevention:** To prevent automated credential stuffing by bots, the system implements reCAPTCHA v3 (score ≥0.5), rate limiting (10 requests/IP/minute via NGINX), progressive delays after failed attempts, and IP reputation checking against ACSC threat intelligence feeds. This distinguishes legitimate users from automated attacks while maintaining usability per OWASP Automated Threats to Web Applications (2024).

# Secure Transport & Credential Handling

All requests use TLS 1.3 with forward secrecy, HSTS, and certificate pinning. Application and database credentials (*app\_reader, app\_writer, app\_admin*) are stored only in AWS Secrets Manager, encrypted with AES-256 KMS keys and rotated every 90 days—never in source code (NIST SP 800-53 IA-5).

# Request Integrity, Error Handling and Logging

CSRF tokens, SameSite=strict cookies, and origin checks protect request integrity. Errors return sanitized HTTP 400/401 responses with no internal details to avoid information leakage. Logs capture only non-sensitive metadata (user ID, timestamp, IP), forwarded to SIEM for correlation under ACSC Essential Eight requirements.

# 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 |

Validation precedes ORM processing (“fail fast”) to prevent overflow and injection attacks (OWASP ASVS V5.1.2).

A screenshot of a computer code

AI-generated content may be incorrect.

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

# **Retrieve Phase – Secure Data Retrieval and Encryption**

This phase secures queries and delivery. Transit uses TLS 1.3; data 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).

# Secure Query Execution

All retrieval operations use ORM parameterized queries or stored procedures, eliminating raw SQL and preventing injection attacks. Least-privilege database accounts govern access according to ISO/IEC 27002 §9.

Requests that include search filters or wildcards must conform to strict rules:

* Wildcards are suffix-only (term%) to preserve index efficiency.
* Inputs are escaped (%, \_, \) before query binding.
* High-volume queries (>10,000 rows) auto-trigger pagination and generate SIEM alerts to detect abuse or enumeration attempts (Xiao & Xiao, 2021).

# Authorization and Record Scoping

Each retrieval is evaluated against role-based access rules:

* Doctors cannot access retail data.
* Retail analysts cannot query hospital datasets.
* Privileged users require elevated roles with audit logging.

These checks prevent cross-domain exposure and enforce least privilege consistently across application and database layers.

# Encryption in Transit and at Rest

Data protection is maintained end-to-end:

* Transit: TLS 1.3 with forward secrecy, HSTS.
* At Rest: AES-256-GCM encryption with annual key rotation (Calder, 2020).
* Content Integrity: SHA-256 digests validate that responses are untampered.

# Output Encoding & Response Hardening

Returned data is sanitized to prevent client-side attacks:

* HTML output is escaped to block XSS.
* Cookies are set with Secure, HttpOnly, and SameSite=Strict.
* Browsers are forced to use HTTPS via HSTS.

These controls ensure that even if users view or download data, the client environment does not become an attack vector.

# Logging, Backups & High Availability

Retrieval logs store session ID, timestamp, role, and query scope. Logs remain immutable for 12 months (Vacca, 2014).

Availability is ensured through:

* Daily encrypted backups to AWS S3 Glacier (verified quarterly)
* Multi-zone replicas for failover and resilience.

Together, these controls support strong Business Continuity and Disaster Recovery alignment.

# Field-Length Enforcement at Database Layer

Database column definitions mirror the constraints from the *Request Phase* (e.g., Name 100 chars, Address 150 chars). This prevents buffer overflows, reduces storage waste, and maintains consistency with Australian formats (e.g., postcode = 4 digits, +61 phone structure).

These retrieval controls depend directly on the input validation defined in the *Request Phase* and will ensure secure access to stored data.

A diagram of a computer

AI-generated content may be incorrect.

*Figure 2: Data Retrieval and Encryption Flow*

# **Review Phase – Role-Based Access Control and Auditing**

*CuraNexus* applies **Role-Based Access Control** (RBAC) to ensure users access only the data required for their role. Permissions are explicitly defined, enforced through PostgreSQL role groups, and audited quarterly. These RBAC rules govern access *after* users pass the secure login and validation controls defined in the Request Phase.

# Role Definitions and Access Scopes

A close-up of a list

AI-generated content may be incorrect.

# Technical Enforcement

Access is enforced in the database using PostgreSQL roles (*doctors\_group, retailers\_group, accounting\_group*) and Row-Level Security. Only authenticated users who passed brute-force protection, MFA checks, and secure session validation reach this phase.

* Standard Users see only limited columns.
* Accounting roles can access encrypted credit card fields.
* Admin roles see all datasets.

This database-native enforcement prevents application-layer bypasses and aligns with ISO/IEC 27002 §9.2.

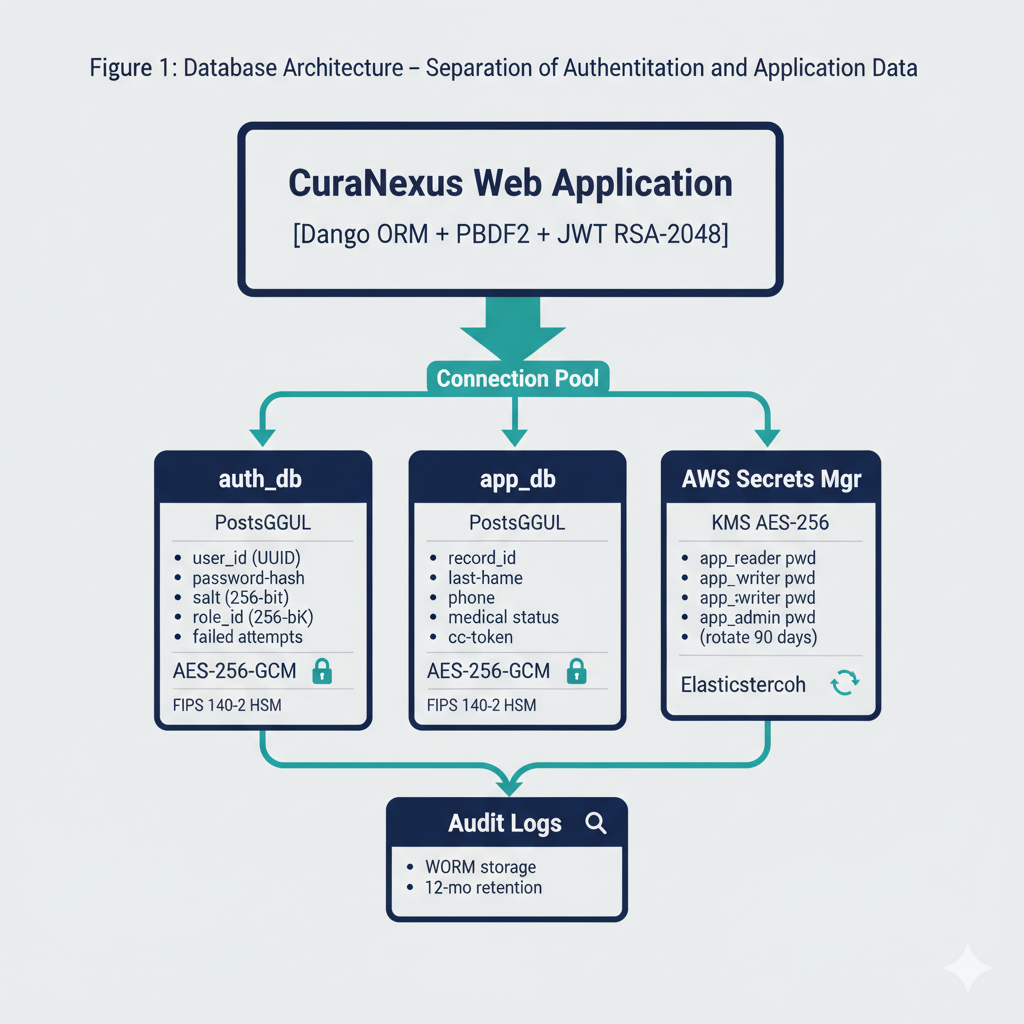
# Preventing Privilege Escalation

Administrative boundaries follow strict controls:

* Separation of Duties (SoD) prevents self-modification of roles.
* Privilege changes require dual approval and cannot occur through the UI.
* Sessions expire after 20 minutes.

# Auditing and Log Integrity

All critical actions (logins, role changes, high-risk queries) are logged immutably in WORM storage for 12 months, correlated in SIEM, and reviewed within 24 hours to support compliance and forensic readiness under NIST SP 800-64 Rev.2. Quarterly access attestation ensures users retain only minimum privileges required (ISO/IEC 27005).



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



*Figure 4: RBAC sequence diagram for CuraNexus request, authorization, and logging flow.*

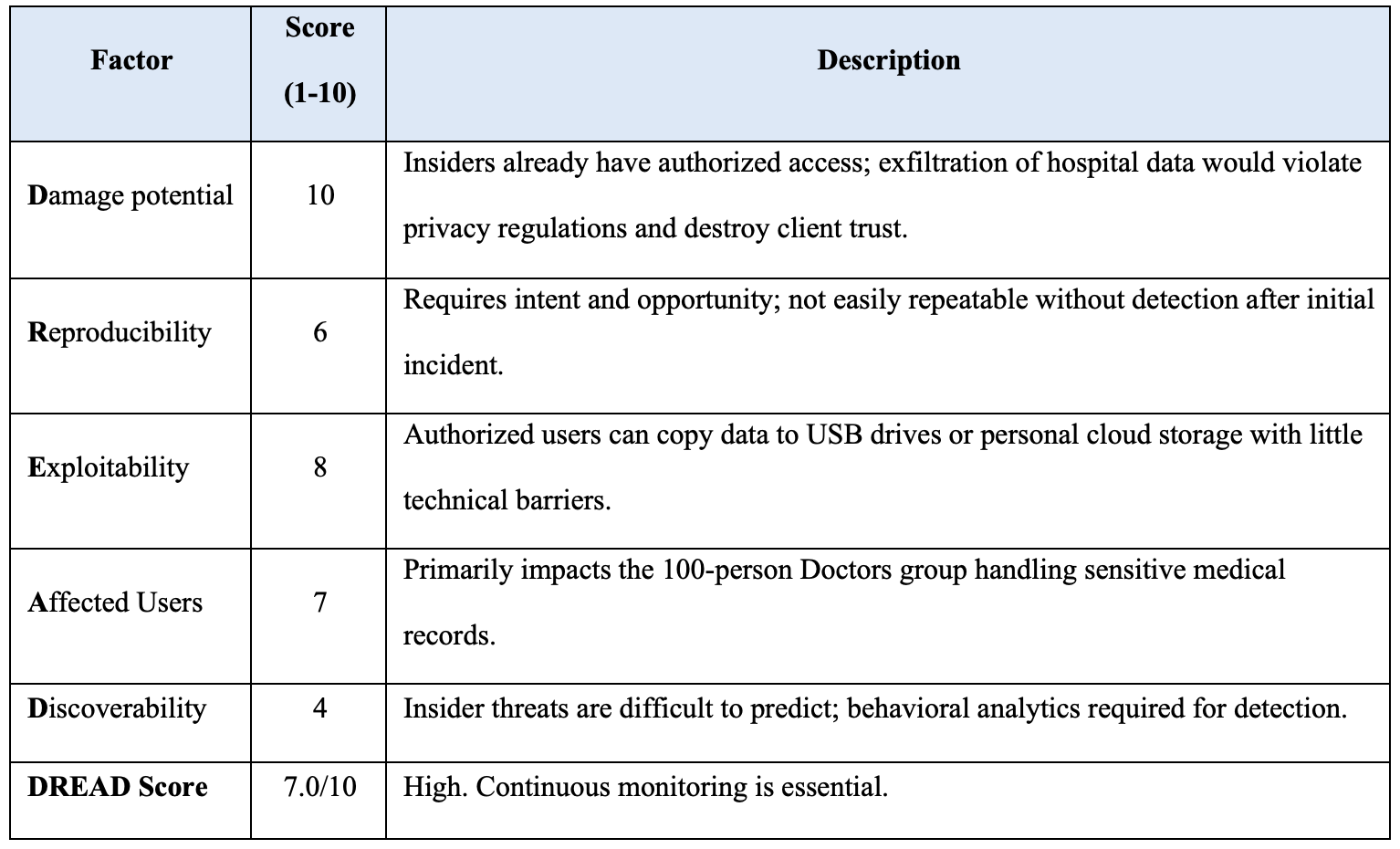
A diagram of a software

AI-generated content may be incorrect.

*Figure 5: RBAC use case diagram showing role-based permissions for CuraNexus users.*

# **Mitigation Methods**

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



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.”

# General Risk Profile for Web Data Retrieval Applications

Beyond CuraNexus-specific threats, all web-based data retrieval applications face common OWASP Top 10 (2024) vulnerabilities:

|  |  |  |
| --- | --- | --- |
| **Factor** | **DREAD Score** | **Mitigation Priority** |
| SQL Injection (OWASP #3) | 8.2/10 | Critical – Parameterized queries mandatory |
| Broken Authentication (OWASP #1) | 7.5/10 | Critical – MFA + session management |
| Sensitive Data Exposure (OWASP #2) | 8.0/10 | Critical – Encryption at rest/transit |
| Broken Access Control (OWASP #5) | 7.8/10 | High – RBAC + least privilege |

**Application-Type Risk Factors:**

Healthcare data retrieval systems face heightened privacy regulations (Privacy Act 1988, Australian Privacy Principles). Financial/retail systems require PCI-DSS compliance for payment data. Multi-tenant architectures risk data leakage between clients. Web interfaces expose larger attack surfaces than internal tools. This risk framework applies across medical, financial, or retail contexts, with scores adjusted based on data sensitivity classification per ISO 31000:2018.”

# **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).

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).

# **Integration with ISMS and Business Continuity**

This security design integrates with the **ISMS** **framework** from *Assessment 2*, particularly the PDCA cycle, SIEM monitoring cadence, incident response playbooks (ISO 27035), and business continuity plans ensuring 4-hour RTO through encrypted cloud backups (ISO 22301).

# **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.

# **Appendices**

## 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. |

## Appendix B – One-Page Poster

**A white and blue text on a white background

AI-generated content may be incorrect.**

*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.

# **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.

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). *Automated threats to web applications.* https://owasp.org/www-project-automated-threats-to-web-applications/

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

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

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.