Assignment 1: Design and Demonstration of CMDB

Analysis of ITSM Requirements:

Asset Management

- Tracks and manages IT assets to ensure security (Bannerman, 2008).
  - Asset identification with unique IDs and Ownership tracking to assign accountability.
  - Lifecycle tracking from acquisition to disposal.
  - Documentation of relationships and dependencies among assets.

Vulnerability Tracking

- Identifies and manages weaknesses in systems (Anderson, 2019).
  - Integration with vulnerability scanners for automated updates.
  - Prioritisation based on severity (e.g., CVSS scoring).
  - Real-time status tracking and historical data for trends and recurring issues (Chapple & Seidl, 2017).

Compliance Monitoring

- Ensures processes meet regulatory requirements (ISO/IEC 20000, 2018).
  - Mapping of assets to regulatory standards (e.g., GDPR).
  - Real-time compliance reports and automated compliance checks
  - Continuous monitoring for ongoing compliance (Salehi & Vazife, 2019).

Incident Response

- Manages and resolves incidents to reduce impact (Shameli-Sendi, 2016).
  - Incident tracking with details like impact.
  - Documentation of post-incident actions for future improvement.
  - Escalation processes and timelines responses (Johnson et al., 2019).

Conceptual Data Model:

- **Assets**: Physical or digital items necessary for operations (e.g., Laptop)
- **Vulnerabilities**: Identified security weaknesses within assets
- **Compliance**: Regulatory or organisational standards the assets must comply with (e.g., GDPR)
- **Incidents**: Unplanned events that disrupt operations (e.g., Phishing Attack)
- **Users**: Individuals with authorised access to IT systems (e.g., Administrator).
- **Services:** Business or IT services supported by assets (e.g., CRM).

CI	Attribute	Definition
Assets	Asset ID	Unique identifier
	Asset Type	Classification (e.g., laptop)
	Owner	Individual responsible
	Location	Physical or virtual location
	Criticality	Importance to operations
	Lifecycle Status	Status (e.g., active)
	Configuration	Specifications or setup details
Vulnerabilities	Vulnerability ID	Unique identifier
	CVSS Score	Risk rating based on CVSS
	Affected Asset	Identifying which asset is impacted
	Date Discovered	When the vulnerability was found
	Mitigation Status	Resolution state (e.g., in-progress)
	Vulnerability Source	Origin of the vulnerability (e.g., internal scan)
Compliance	Compliance ID	Unique identifier
	Regulation	Standard or regulation
	Affected Assets	Showing which assets are impacted
	Compliance Status	Compliance level (e.g., non-compliant)
	Last Audit Date	Most recent compliance check date
Incidents	Incident ID	Unique identifier
	Incident Type	Nature of the incident (e.g., security)
	Severity	Impact level
	Affected Assets	Showing which assets are impacted
	Incident Description	Brief details about the incident
	Root Cause	Primary cause of the incident
	Date Detected	When the incident was detected
	Mitigation Actions	Steps taken to resolve the incident
Users	User ID	Unique identifier
	Role	User’s function in the organisation
	Access Level	Permission level
	Affected Assets	Showing which assets access rights
Services	Service ID	Unique identifier
	Dependencies	Assets or services required for this service
	Criticality to Business	Importance of the service to operations
	Associated Incidents	Any incidents or vulnerabilities affecting the service

Table 1: Attributes for each CI (Hamberger, 2024)

Relationship	Definition
Asset - Vulnerability	Links asset to associated vulnerabilities
Asset - Compliance	Connects assets to compliance requirements, ensuring they meet regulations.
Asset - Incident	Links assets to incidents, aiding in impact analysis
Service - Asset	Shows dependencies of services on specific assets
Incident - Vulnerability	Connects incidents to vulnerabilities, enabling root-cause analysis
User - Asset	Access control management
Compliance - Incident	Ensuring regulatory accountability

Table 2: Relationships Between CIs (Hamberger, 2024)

Design Document

The CMDB is designed as a centralised repository accessible through role-based permissions, while maintaining overall security (ISO/IEC 20000, 2018). The architecture below includes integration with existing tools to ensure real-time data:

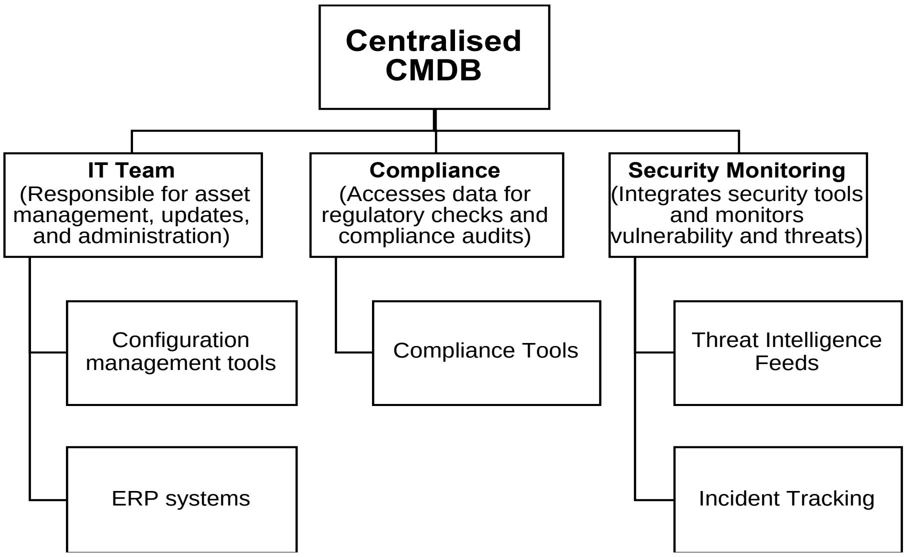
Centralised CMDB
IT Team (Responsible for asset management, updates, and administration)
Compliance (Accesses data for regulatory checks and compliance audits)
Security Monitoring (Integrates security tools and monitors vulnerability and threats)
Configuration management tools
ERP systems
Compliance Tools
Threat Intelligence Feeds
Incident Tracking

Figure 1: CMDB Architecture (Hamberger, 2024)

Entity	Attributes
Assets	ID, Asset Type, Owner, Location, Criticality, Lifecycle Status, Configuration
Vulnerabilities	ID, CVSS Score, Affected Asset, Date Discovered, Mitigation Status, Source
Compliance	ID, Regulation, Affected Assets, Compliance Status, Last Audit Date
Incidents	ID, Type, Severity, Affected Assets, Description, Root Cause, Date, Mitigation
Users	ID, Name, Surname, Role, Access Level, Affected Assets
Services	ID, Dependencies, Criticality, Associated Incidents

Table 3: Data Schema (Hamberger, 2024)

Validation Rules

Effective data validation is crucial for reliability and accuracy (Johnson et al., 2019).

- ID format checks
- Date format validation
- Field completeness of mandatory fields
- Role-based access
- Risk and criticality levels adhere to predefined ranges

User Interface

The CMDB is designed to provide clear views, enabling quick access to information and efficient IT security management (Weed-Schertzer, 2019).

- **Dashboard**: Displays KPIs for quick insights into e.g., asset status.
- **Asset View**: A detailed view that lists all assets, including information on criticality, location, and owner.
- **Incident Management**: A module to record and monitor incidents, view affected assets, and track mitigation steps.
- **Compliance Monitoring**: A compliance dashboard shows regulatory status and audit results.
- **Search and Reporting**: Advanced search capabilities allow users to query e.g. specific assets. Customisable reports offer insights into compliance statuses, aiding strategic decision-making.

<u>Demonstration Phase</u>

Adding New Asset:

1. Open the CMDB dashboard and navigate to the asset management module.
2. Create New Asset Entry
3. Assign attributes such as Criticality and Lifecycle Status.
4. Link the new asset to related CIs, such as associated users.
5. Validate and save the asset entry.

- Data Accuracy
- Linking assets supports root cause analysis and dependency tracking

Potential Enhancement: Automated Asset Discovery

Updating Data

1. Search or select the specific asset requiring updates.
2. Edit Configuration Attributes

3. Log changes for audit purposes, detailing previous values and update reason
4. Save the changes and send notifications to relevant stakeholders.

- Change Management maintains a history for auditing and compliance.
- Data Integrity

Potential Enhancement: Real-Time Integration

Vulnerability Assessments

1. Run vulnerability scan
2. Identify and link vulnerabilities to affected assets.
3. Record the risk level, and update attributes like CVSS Score and mitigation status.
4. Notify Relevant Teams

- Risk Assessment
- Traceability

Potential Enhancement: Automated Risk Scoring

Compliance Reports:

1. Open the compliance management module
2. Choose parameters, such as regulatory standard and date range.
3. Run the report
4. Export the report in the desired format and share with stakeholders.

- Regulatory Alignment
- Audit Preparedness

Potential Enhancement: Automated Reporting

Key Discussion Points

Rationale Behind Design Decisions:

- The CMDB supports security functions, aligning with organisational and regulatory goals (ISO/IEC 20000, 2018).
- CIs are included for their security relevance. Compliance CIs ensure regulatory alignment (Salehi & Vazife, 2019).
- Attributes like CVSS help prioritise responses and risks (Johnson et al., 2019).
- Links between CIs facilitate root-cause analysis and align with ITIL 4 Foundation (2019).

Design Challenges:

- Standardising across departments is crucial but requires a structured approach and coordination across teams.
- Integrating with systems like ERP is complex and requires customisation for real-time data updates (Chapple & Seidl, 2017).
- CMDB upkeep needs resources, which small IT teams may lack (ISO/IEC 20000, 2018).
- Ensuring the CMDB can scale with new data inputs can add complexity.

Potential Enhancements:

- Automated updates
- Advanced analytics for threat prioritisation (Salehi & Vazife, 2019).
- Granular access controls (ITIL 4 Foundation, 2019).

Wordcount: 1088

References:

Hamberger, G. (2024) Assignment 1. *ITSM November 2024*. Essay submitted to the University of Essex Online.

Anderson, R. (2019) *Security Engineering: A guide to building Dependable Distributed Systems*. John Wiley & Sons.

Bannerman, P. L. (2008) Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, *81*(12), 2118–2133. https://doi.org/10.1016/j.jss.2008.03.059

Chapple, M., & Seidl, D. (2017) *CompTIA CYSA+ Study Guide: Exam CS0-001*. John Wiley & Sons.

ISO/IEC 20000. (2018) Information Technology – Service Management. Available from: https://www.iso.org/standard/70636.html [Accessed 08.11.2024]

ITIL 4 Foundation. (2019) IT Service Management Certification. Available from: https://www.axelos.com/certifications/itil-service-management/itil-4-foundation [Accessed 10.11.2024]

Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2019) Guide for security-focused configuration management of information systems. In *NIST Special Publication 800-128*. DOI: https://doi.org/10.6028/nist.sp.800-128

Salehi, A., & Vazife, Z. (2019) The effect of the implementation of Information Security Management System (ISMS) and Information Technology Infrastructure Library (ITIL) on the promotion of information systems and information technology services continues. *Public Management Researches 12*(43): 225–249. DOI: https://doi.org/10.22111/jmr.2019.4751

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2015) Taxonomy of information security risk assessment (ISRA). *Computers & Security 57*: 14–30. DOI: https://doi.org/10.1016/j.cose.2015.11.001

Weed-Schertzer, B. (2019) *Delivering ITSM for Business Maturity*. Available from: https://books.emeraldinsight.com/resources/pdfs/chapters/9781789732542-TYPE23-NR2.pdf [Accessed 08.11.2024]