اونيۏرسيتي مليسيا ڤهڠ السلطان عبدالله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

Faculty of Computing
Fakulti Komputeran

PROJECT OF BCY2033

LECTURER'S NAME: DR. MOHD FAIZAL BIN AB RAZAK

TEAM MEMBERS:

NO	MATRIC NUMBER	NAME	SECTION
1	CF23006	SAEED MOHAMMED KHALED ABDULAZIZ	01A
2	CF23005	ALWAHEDI ABDULLAH	01A
3	CF23001	RAMI BENOUAHMENE	01A

Table of Contents

Introduction and Overview

TASK DISTRIBUTION

NO.	MEMBER	TASK

MEETING REPORT

NO.	MEETING DETAILS	RESULTS / REPORT / SCREENSHOT

Appendix C: Assessment Team Members and Functions

Functional Role	Background	Organization	Email	Phone
Risk Assessment Manager	Drives the risk assessment process, coordinates tasks, deliverables, and schedule, composes the report with input from all team members.	XYZ Hospital	risk.manager@xyz.com	(123) 456-7890
System or Network Administrator	Operates and maintains the system from a technical, day-to-day standpoint; usually the "Primary System Contact" in the System Identification table.	XYZ Hospital	sysadmin@xyz.com	(123) 456-7891
Technical Reviewer	Understands the technical components of the system but was not involved in designing, building, or operating the system being assessed.	XYZ Hospital	techreview@xyz.com	(123) 456-7892
System Business Owner	Responsible for the system, or the services it provides, from a business or	XYZ Hospital	business.owner@xyz.com	(123) 456-7893

	customer standpoint; understands the system’s purpose but not necessarily the details of its technical implementation.			
System Technical Owner	Has supervisory responsibility for the operation of the system.	XYZ Hospital	tech.owner@xyz.com	(123) 456-7894
Executive Sponsor	Executive management-level responsibility for the system.	XYZ Hospital	exec.sponsor@xyz.com	(123) 456-7895
Information Security Officer	Responsible for the agency’s security policies and objectives, and its overall risk profile.	XYZ Hospital	security.officer@xyz.com	(123) 456-7896

Risk Assessment Process

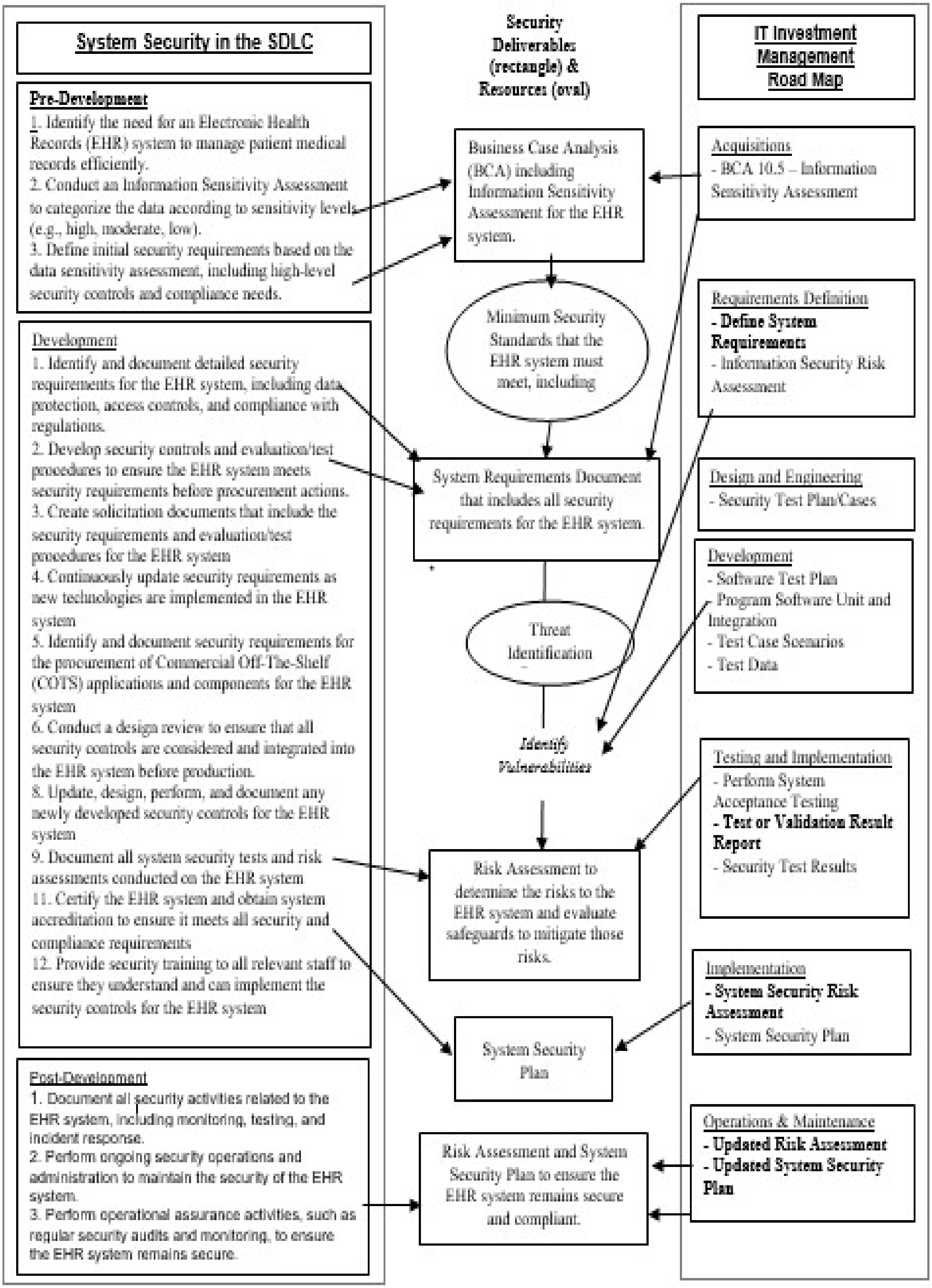
XYZ Hospital, a prominent healthcare institution known for its advanced medical services and state-of-the-art facilities, experienced a significant data breach in early 2023. The breach compromised the hospital's Electronic Health Records (EHR) system, which is designed to store and manage comprehensive patient medical records, including sensitive personal information such as names, addresses, social security numbers, and detailed medical histories. The EHR system is integral to the hospital's operations, facilitating seamless access to patient data for healthcare providers, enhancing the quality of care, and ensuring efficient administrative processes.

The breach was discovered when hospital IT staff noticed unusual activity on the network, prompting an immediate investigation. It was later determined that unauthorized individuals had gained access to the EHR system through a combination of exploiting weak passwords, outdated software vulnerabilities, and a lack of encryption for sensitive data. The incident exposed the personal and medical information of thousands of patients, raising serious concerns about patient privacy and the hospital's information security practices. The breach not only compromised the trust of patients but also highlighted the critical need for robust security measures to protect sensitive healthcare data. In response, XYZ Hospital initiated a comprehensive risk assessment to identify and address the vulnerabilities that led to the breach, aiming to prevent similar incidents in the future and restore confidence in their information security infrastructure.

1.0 Set boundary for selected system

The EHR system boundary encompasses all hardware, software, and network components that are directly involved in the storage, processing, and transmission of patient medical records. This includes:

- ***Core EHR Application:*** The primary software application used by healthcare providers to access and manage patient records. It also includes modules for patient demographics, medical history, diagnoses, treatments, and billing information.
- ***Database Servers:*** Servers that store the EHR data, including patient records, medical images, and administrative information. It also includes both primary and backup databases.
- ***Application Servers:*** Servers that host the EHR application and related services. It also includes web servers, application servers, and middleware components.
- ***Network Infrastructure:*** The internal network that connects the EHR system components, including local area networks (LANs) and wide area networks (WANs). It also includes routers, switches, firewalls, and virtual private networks (VPNs) used for secure remote access.
- ***User Devices:*** Computers, tablets, and other devices used by healthcare providers, administrators, and other authorized users to access the EHR system. It also includes workstations, laptops, and mobile devices.
- ***Integration Points:*** Interfaces and APIs that connect the EHR system with other hospital systems, such as laboratory information systems, radiology information systems, and billing systems. It also includes data exchange protocols and security measures for inter-system communication.
- ***Security Controls:*** Authentication and authorization mechanisms, including user credentials, multi-factor authentication, and access control lists. It also includes encryption protocols for data at rest and in transit, as well as intrusion detection and prevention systems (IDPS).
- ***Physical Components:*** Data centers and server rooms where the EHR system hardware is located. It also includes physical security measures, such as access controls, surveillance cameras, and environmental controls.



System Security in the SDLC

Pre-Development

1. Identify the need for an Electronic Health Records (EHR) system to manage patient medical records efficiently.
2. Conduct an Information Sensitivity Assessment to categorize the data according to sensitivity levels (e.g., high, moderate, low).
3. Define initial security requirements based on the data sensitivity assessment, including high-level security controls and compliance needs.

Development

1. Identify and document detailed security requirements for the EHR system, including data protection, access controls, and compliance with regulations.
2. Develop security controls and evaluation/test procedures to ensure the EHR system meets security requirements before procurement actions.
3. Create solicitation documents that include the security requirements and evaluation/test procedures for the EHR system
4. Continuously update security requirements as new technologies are implemented in the EHR system
5. Identify and document security requirements for the procurement of Commercial Off-The-Shelf (COTS) applications and components for the EHR system
6. Conduct a design review to ensure that all security controls are considered and integrated into the EHR system before production.
8. Update, design, perform, and document any newly developed security controls for the EHR system
9. Document all system security tests and risk assessments conducted on the EHR system
11. Certify the EHR system and obtain system accreditation to ensure it meets all security and compliance requirements
12. Provide security training to all relevant staff to ensure they understand and can implement the security controls for the EHR system

Post-Development

1. Document all security activities related to the EHR system, including monitoring, testing, and incident response.
2. Perform ongoing security operations and administration to maintain the security of the EHR system.
3. Perform operational assurance activities, such as regular security audits and monitoring, to ensure the EHR system remains secure.

Security Deliverables (rectangle) & Resources (oval)

Business Case Analysis (BCA) including Information Sensitivity Assessment for the EHR system.

Minimum Security Standards that the EHR system must meet, including

System Requirements Document that includes all security requirements for the EHR system.

Threat Identification

Identify Vulnerabilities

Risk Assessment to determine the risks to the EHR system and evaluate safeguards to mitigate those risks.

System Security Plan

Risk Assessment and System Security Plan to ensure the EHR system remains secure and compliant.

IT Investment Management Road Map

Acquisitions
- BCA 10.5 – Information Sensitivity Assessment

Requirements Definition
- Define System Requirements
- Information Security Risk Assessment

Design and Engineering
- Security Test Plan/Cases

Development
- Software Test Plan
- Program Software Unit and Integration
- Test Case Scenarios
- Test Data

Testing and Implementation
- Perform System Acceptance Testing
- Test or Validation Result Report
- Security Test Results

Implementation
- System Security Risk Assessment
- System Security Plan

Operations & Maintenance
- Updated Risk Assessment
- Updated System Security Plan

1.1 Record system identification information

1.1 System Identification	
Agency Name	XYZ Hospital
Official System Name	Electronic Health Records (EHR) System
System Acronym	EHR
System Business Owner	Dr. Jane Doe, Chief Medical Officer
System Technical Owner	John Smith, IT Director
System Security Owner	Alice Johnson, Information Security Officer
Additional System Stakeholders	Hospital administrators IT staff healthcare providers
System Location Full Address	123 Medical Avenue, Healthville, USA
Contract Number, Contractor names, phone numbers and emails, if applicable	N/A (in-house development)
System type(s) (mainframe, application / database / network / file server, workstation)	Application/database server, network infrastructure, workstations
Primary System Contact(s), Name and Title (usually the system administrator)	John Smith, IT Director
Organization Name	XYZ Hospital
Full Address	123 Medical Avenue, Healthville, USA
Email Address	john.smith@xyzhospital.com
Phone and pager numbers	(123) 456-7890

1.2 Document system purpose and desc.

1.2 System Purpose and Description	
Function and purpose of the system	The EHR system is designed to store, manage, and provide access to patient medical records, facilitating efficient and effective healthcare delivery.

General functional requirements	The system must support the creation, storage, retrieval, and updating of patient records, as well as integration with other hospital systems.
Business processes, applications and services supported	Patient registration, medical history management, appointment scheduling, billing, laboratory results, radiology images, clinical decision support.
System components	Primary EHR database, application servers, network infrastructure, workstations, backup systems, integration interfaces.
Environmental factors	The system operates in a secure data center with controlled access, redundant power supplies, and environmental controls.
Network diagram with system boundaries (attach)	[Insert Network Diagram Here]
General information flow	Patient data is entered and accessed by healthcare providers and administrative staff, with integration interfaces facilitating data exchange with other hospital systems.
Technical and business users (list)	Healthcare providers (doctors, nurses), administrative staff, IT staff, hospital administrators.
System ownership (shared or dedicated)	Dedicated

1.3 Document the system security level

1.3 Information Security Levels and Overall System Security Level	
Information Category	Patient personal information, medical history, diagnostic results, treatment plans
Information Security Level	High
Information Category	Medical history, diagnostic results, treatment plans
Information Security Level	High

Information Category	Billing information, insurance details
Information Security Level	Moderate
Overall System Security Level	High

Explanation:

- *Patient personal information:* This includes names, addresses, and social security numbers. Given the sensitivity of this data, it is classified as High.
- *Medical history, diagnostic results, treatment plans*: This information is critical to patient care and privacy, thus classified as High.
- *Billing information, insurance details*: While important, this information is less sensitive than personal and medical data, thus classified as Moderate.

Overall System Security Level:

Given that the EHR system handles highly sensitive patient personal and medical information, the overall system security level is classified as High.

This table ensures that the security levels are appropriately assigned based on the sensitivity and criticality of the information handled by the EHR system, aligning with the organization's information security policy.

2.0 System Risk Determination Phase

2.0 Risk Determination Table							
Item No.	**Threat Name**	**Vulnerability Name**	**Risk Description**	**Existing Controls**	**Likelihood of Occurrence**	**Impact Severity**	**Risk Level**
1	Unauthorized Access	Weak Password	Unauthorized users exploit weak passwords to access sensitive EHR data.	Multi-factor authentication, password policy	High	High	Critical
2	Data Breach	Outdated Software	Hackers exploit vulnerabilities in outdated software to gain access to the system.	Regular software updates, firewalls	Medium	High	High
3	Insider Threats	Lack of Monitoring	Employees misuse their access to view or steal patient data.	Role-based access control, logging	Medium	High	High
4	Data Loss	No Encryption	Data is intercepted during transmission due to lack of encryption.	Encrypted communications, VPN	Low	High	Moderate
5	System Downtime	Lack of Redundancy	Critical system downtime due to hardware failure or cyberattacks.	Backup systems, disaster recovery plan	Low	High	Moderate

2.1 I identify threats and vulnerabilities

- Weak passwords were exploited, leading to unauthorized access.
- Outdated software vulnerabilities were used as an attack vector.
- Lack of encryption increased the risk of data interception.
- Insider threats were identified due to insufficient monitoring.
- Redundancy measures were noted as critical but lacking in certain areas.

2.2 Describe risks

- Unauthorized Access: Allows attackers to compromise sensitive patient data.

- Data Breach: Exposes patient and hospital information, leading to legal and reputational damages.

- Insider Threats: Enables employees to misuse data, compromising patient trust.

- Data Loss: Results in permanent loss or leakage of sensitive data during transmission.

- System Downtime: Disrupts hospital operations, affecting patient care.

2.3 Identify existing controls

- Multi-factor authentication (MFA) and password policies to mitigate unauthorized access.
- Regular updates and firewalls to reduce software vulnerabilities.
- Role-based access control and activity logging to deter insider threats.
- VPNs and encrypted communication protocols to protect data in transit.
- Backup systems and disaster recovery plans to handle system downtimes.

2.4 Determine likelihood of occurrence

- High Likelihood: Weak passwords, given past breaches

- Medium Likelihood: Outdated software and insider threats, based on current controls

- Low Likelihood: Data loss and system downtime due to implemented backup and encryption

2.5 Determine severity of impact

- High Impact: Breaches, insider misuse, and system downtimes due to sensitive patient data
- Moderate Impact: Encrypted data loss mitigated by controls

2.6 Determine risk levels

- Risk levels are calculated based on likelihood and impact severity:
- Critical: High likelihood and high impact.

3.0 Safeguard Determination Phase

The Safeguard Determination Phase for XYZ Hospital's Electronic Health Records (EHR) system addresses the identified risks by recommending controls and safeguards, assessing their effectiveness, and determining the residual risk levels. These measures aim to enhance the overall security posture of the EHR system.

Item No.	Recommended Safeguard Description	Residual Likelihood of Occurrence	Residual Impact Severity	Residual Risk Level
1	Implement multi-factor authentication (MFA), enforce strict password policies, require password rotation, and conduct	Medium	High	High

	periodic security awareness training for staff.			
2	Regularly update all EHR-related software, perform routine vulnerability scans, use automated patch management tools, and implement an emergency update protocol.	Low	High	Moderate
3	Deploy advanced activity logging, establish real-time monitoring systems, conduct periodic security audits, and enforce stringent access controls.	Medium	Moderate	Moderate
4	Enforce end-to-end encryption for data in transit and at rest, implement encryption standards across all sensitive data stores, and conduct regular	Low	Moderate	Low

	encryption audits.			
5	Develop and test a disaster recovery plan, implement redundant servers and failover systems, and ensure backup power supplies and network redundancy.	Very Low	Low	Low

3.1 Recommend controls and safeguards

Item No.	Threat Name	Vulnerability Name	Recommended Safeguard Description
1	Unauthorized Access	Weak Password	Implement multi-factor authentication (MFA), enforce strict password policies, require password rotation, and conduct periodic security awareness training for staff.
2	Data Breach	Outdated Software	Regularly update all EHR-related software, perform routine vulnerability scans, use automated patch management tools,

			and implement an emergency update protocol.
3	Insider Threats	Lack of Monitoring	Deploy advanced activity logging, establish real-time monitoring systems, conduct periodic security audits, and enforce stringent access controls.
4	Data Loss	No Encryption	Enforce end-to-end encryption for data in transit and at rest, implement encryption standards across all sensitive data stores, and conduct regular encryption audits.
5	System Downtime	Lack of Redundancy	Develop and test a disaster recovery plan, implement redundant servers and failover systems, and ensure backup power supplies and network redundancy.

3.2 Determine residual likelihood of occurrence

Item No.	Threat Name	**Residual Likelihood of Occurrence**
1	Unauthorized Access	Medium
2	Data Breach	Low
3	Insider Threats	Medium
4	Data Loss	Low
5	System Downtime	Very Low

3.3 Determine residual severity of impact

Item No.	**Threat Name**	**Residual Impact Severity**

1	Unauthorized Access	High
2	Data Breach	High
3	Insider Threats	Moderate
4	Data Loss	Moderate
5	System Downtime	Low

3.4 Determine residual risk level

Item No.	Threat Name	Residual Risk Level
1	Unauthorized Access	High
2	Data Breach	Moderate
3	Insider Threats	Moderate
4	Data Loss	Low
5	System Downtime	Low

4.0 Report presentation, archiving and sign-off

4.1 Report Presentation

The findings of this risk assessment have been compiled into a comprehensive report to assist in improving the security of the XYZ Hospital EHR system. The report includes:

1. A summary of the EHR system architecture and its security requirements.
2. Identified threats, vulnerabilities, and existing controls.
3. Detailed risk levels and recommended safeguards.
4. The residual risks after safeguard implementation.

This report is intended to guide decision-making for system improvement and to ensure compliance with applicable security policies and standards.

4.2 Archiving

The report will be securely archived within XYZ Hospital's information repository. The repository will:

- Ensure authorized access for future reference.
- Support periodic audits and reviews.
- Serve as a resource for updating risk management and business continuity plans.

4.3 Sign-Off

By signing this document, all parties acknowledge the findings, recommendations, and actions outlined in the risk assessment.

Signatures

Submitted by: ______________________ Date: ________

Risk Assessment Manager

Reviewed by: _______________________ Date: _________

[Title]

Approved by: _______________________ Date: _________

[Title]