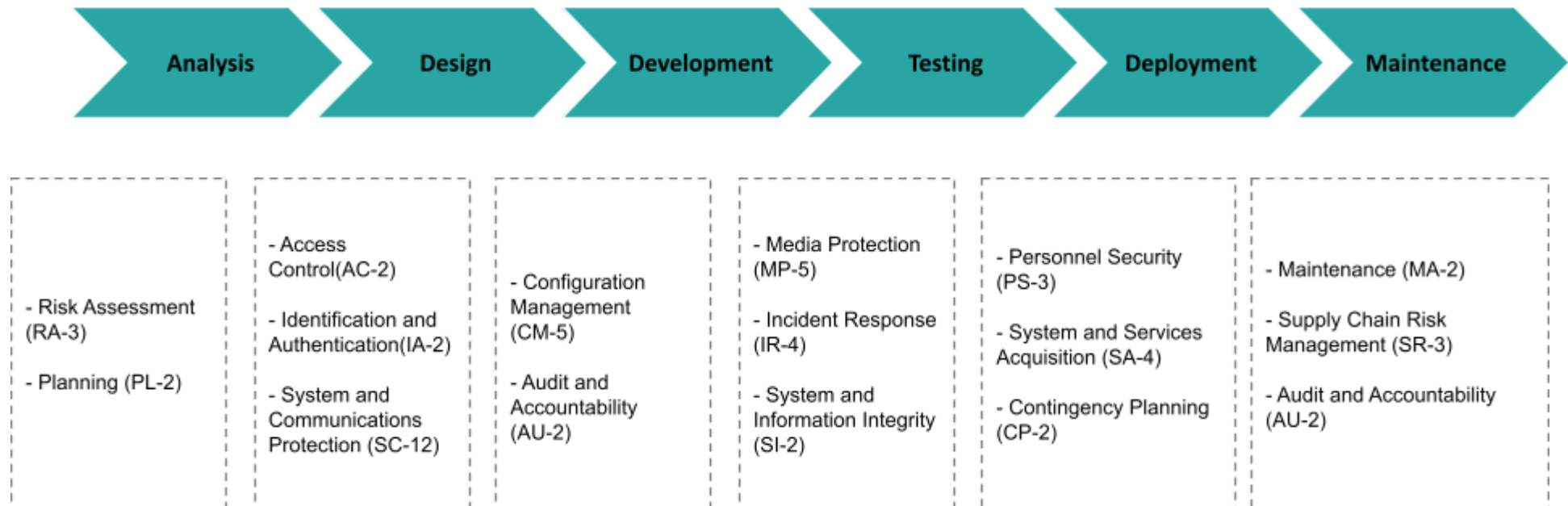


Individual Assignment

A. Please elaborate your understanding in controls embedded throughout the Software Development Life Cycle to protect data.









Picture A: Software Development Lifecycle

B. Please identify applicable risk and controls to data regarding to the following scenarios

| Scenario | Risk | Preventive control | Detective control | On-going monitoring control |
|--------------------------------------|--|---|---|---|
| 1. Ransomware attack | <ul style="list-style-type: none"> - Loss of access to critical data - Financial loss - Data breach due to encryption | <ul style="list-style-type: none"> - Patch management to close vulnerabilities - Endpoint security to block ransomware - Data backup and recovery for restoration | <ul style="list-style-type: none"> - Log monitoring and handling process to detect suspicious activities - Anomaly detection in endpoint behaviors | <ul style="list-style-type: none"> - Regular updates to endpoint security tools - Continuous audit of patch application |
| 2. Data sharing to Third Party | <ul style="list-style-type: none"> - Unauthorized use of shared data - Data leakage due to third-party mishandling | <ul style="list-style-type: none"> - Information classification and handling to define data sharing rules - Data Encryption for shared data - Secured data transmission protocols like TLS | <ul style="list-style-type: none"> - Data Leakage Prevention (DLP) to detect unauthorized sharing - Log monitoring of data access and transmission activities | <ul style="list-style-type: none"> - Third-party audits - Monitoring third-party compliance to data sharing agreements |
| 3. Malicious code attached in e-mail | <ul style="list-style-type: none"> - System infection - Compromised sensitive data | <ul style="list-style-type: none"> - Cybersecurity awareness training for phishing awareness - Multi-Factor Authentication (MFA) to prevent unauthorized access | <ul style="list-style-type: none"> - Log monitoring to detect unusual email attachments - Endpoint security to flag malicious code | <ul style="list-style-type: none"> - Continuous email filtering and threat intelligence updates - Regular phishing simulation tests |

Possible controls for your selection are listed as below

1. Patch management 
2. End point security 
3. User identification and authentication
4. Information access restriction
5. Privilege ID management
6. Multi-Factor Authentication (MFA) 
7. Data backup and recovery 
8. Data Leakage Prevention (DLP) 
9. Cyber security awareness training
10. Information classification and handling 
11. Network security management
12. Data Encryption 
13. Secured data transmission 
14. Log monitoring and handling process 

C. Provide 3 examples of controls that will assure the data privacy risk.

1. Encryption of Data (Data Protection in Transit and at Rest)

ใช้การเข้ารหัสข้อมูลในระหว่างการส่ง (Data in Transit) และจัดเก็บข้อมูลอยู่ในระบบ

(Data at Rest) เพื่อป้องกันการดักจับข้อมูลหรือการเข้าถึงโดยไม่ได้รับอนุญาต

Data in Transit คือ การเข้ารหัสข้อมูลระหว่างการส่งผ่านเครือข่าย ป้องกันข้อมูลจากการถูกดักจับหรือ
โจมตีระหว่างการส่ง ตัวอย่างการใช้งาน

- VPN (Virtual Private Network)

การเข้ารหัสการเชื่อมต่อเครือข่ายระหว่างอุปกรณ์และเครือข่ายส่วนกลาง เพื่อป้องกันข้อมูล
จากการถูกดักฟัง

Data at Rest คือ การเข้ารหัสข้อมูลที่เก็บไว้ในฐานข้อมูลหรือในอุปกรณ์จัดเก็บข้อมูลต่าง ๆ เพื่อป้องกันการ
การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ตัวอย่างการใช้งาน

- Database Encryption:

เข้ารหัสข้อมูลในฐานข้อมูล เช่น การใช้ Transparent Data Encryption (TDE) ในฐานข้อมูลเชิงพาณิชย์ เช่น Microsoft SQL Server หรือ Oracle เพื่อป้องกันการเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาต เป็นข้อกำหนดในมาตรฐาน NIST Privacy Framework (PR.DS-P3) และ ISO 27701

2. Data Minimization

จำกัดการเก็บรวบรวมและประมวลผลข้อมูลเฉพาะที่จำเป็นต่อวัตถุประสงค์ เพื่อลดความเสี่ยงที่อาจเกิดจากการจัดการข้อมูลที่ไม่จำเป็น ตัวอย่างการใช้งาน

การเก็บข้อมูลการสมัครสมาชิกในรูปแบบฟอร์ม (Form Data Collection) เก็บเฉพาะข้อมูลที่ต้องใช้ เช่น ชื่อและอีเมล ไม่เก็บข้อมูลส่วนตัวที่ไม่เกี่ยวข้องกับวัตถุประสงค์ เช่น วันเกิด หรือหมายเลขบัตรประชาชน

เป็นข้อกำหนดในมาตรฐาน NIST Privacy Framework (ID.IM-P4) และ ISO 27701

3. Access Control (RBAC - Role-Based Access Control)

ควบคุมการเข้าถึงคือ การกำหนดสิทธิ์ในการเข้าถึงระบบหรือข้อมูล โดยอิงตามบทบาทหน้าที่ (Role-Based Access Control หรือ RBAC) เพื่อให้แน่ใจว่าข้อมูลสำคัญจะถูกเข้าถึงเฉพาะผู้ที่มีสิทธิ์เท่านั้น

ตัวอย่างการใช้งาน เช่น ระบบภายในองค์กร คือกำหนดสิทธิ์พนักงานในระบบ พนักงานฝ่ายขายสามารถเข้าถึงเฉพาะข้อมูลลูกค้าที่เกี่ยวข้องกับทีมของตน แต่ไม่สามารถดูข้อมูลทางการเงินที่จัดการโดยฝ่ายบัญชีได้

เป็นข้อกำหนดในมาตรฐาน NIST Privacy Framework (PR.AC-P1) และ ISO 27701