Exercise 2

1.

2. Security and Privacy by Design:

- Integrating security and privacy considerations into the entire software development lifecycle. This involves conducting security risk assessments and defining security requirements during the initial planning stages. Adopt secure coding practices and conduct regular security reviews throughout the development process.

Example Actions:

- Include security experts in the requirements gathering phase.
- Use threat modeling to identify potential security risks.
- Implement coding standards that prioritize secure coding practices.
- Perform regular security reviews and code audits.

Access Control:

- Implementing robust access control mechanisms to ensure that only authorized users can access and manipulate safety-critical functions. This involves user authentication, role-based access control (RBAC), and detailed logging for accountability.

Example Actions:

- Enforce strong authentication measures, such as multi-factor authentication.
- Implement role-based access control RBAC.
- Monitor and log user activities to detect and respond to unauthorized access.
- Regularly review and update access permissions based on personnel changes.

Compliance with Legislation (e.g., GDPR):

- Implementation: Establish a thorough understanding of relevant regulations and incorporate compliance measures into the software development process. Develop and maintain documentation to demonstrate compliance with legal requirements.

Example Actions:

- Conduct an analysis to identify applicable regulations.
- Design data handling processes to comply with data protection laws.
- Implement mechanisms for obtaining and managing user consent where necessary.
- Keep policies and procedures up-to-date with evolving regulations.

Design with the Enemy in Mind (Threat Modeling):

- Implementation: Actively identify potential threats and vulnerabilities by conducting threat modeling exercises. Use this information to inform the design and implementation of security controls that address specific risks.

Example Actions:

- Identify potential threat actors and their motivations.
- Prioritize potential attack vectors based on impact and likelihood.

- Develop and implement security controls to mitigate identified risks.
- Regularly update threat models to adapt to evolving threats.