بنك العز الإسلامي
alizz islamic bank

Cybersecurity by Design in Banking: A Critical Need

Muscat, 17 December 2024

Speaker: Dr Mohamed Chahine GHANEM CISSP FCIISec
Associate Professor
Director- Cyber Security Research Centre | CSbD Advisor
London Metropolitan University (UK) | Scotia Bank (Canada)

Agenda

1. Introduction
2. Cybersecurity Threats in Digital Banking
3. Cyber Security by Design (CSbD)
4. Key CSbD Strategies in Banking
5. Best Practices
6. Challenges and Future

About me

- Engineer Degree (MoD), MSc in Digital Forensics and PhD in Cyber Security Engineering from City, University of London
- 19 years in the Cyber Security Industry (Law Enforcement and Corporations)
- Certified Expert (CISSP, CPCI, Multi-GIAC Cert.)
- Currently Associate Professor and Director of the Cyber Security Research Centre at Londonmet
- Senior Advisor on Cyber Resilience (CSbD) in Banking (prev. Associate Director in Security Auditing at Kroll LLC)

Rapidly Expanding Banking Threat

Increased Cyber Threats: In 2023, 70% of global financial institutions reported being targeted by cyberattacks, a trend expected to grow in 2024.

Digital Transformation Drives Complexity: Global banks spend over $1.3 trillion on digital transformation, with cybersecurity a key focus.

High Stakes for Financial Systems: Cyber breaches cost financial services $265 million in ransomware damages alone in 2023.

“Authorised” Fraud in Banking

The global authorized fraud losses in the banking sector are estimated to be in the **hundreds of billions** of dollars

United States: The Federal Trade Commission (FTC) estimated scam-related losses at approximately **$158 billion** in 2023.

United Kingdom: Authorized push payment (APP) fraud accounted for a significant proportion of banking fraud losses, with figures nearing **£900 million** annually. Total Fraud is about **£2 billion.**

Middle East Context !

Emerging Cybersecurity Threats

Ransomware & Phishing: Ransomware caused $265M in damages in 2023. Phishing remains a top vector for data breaches.

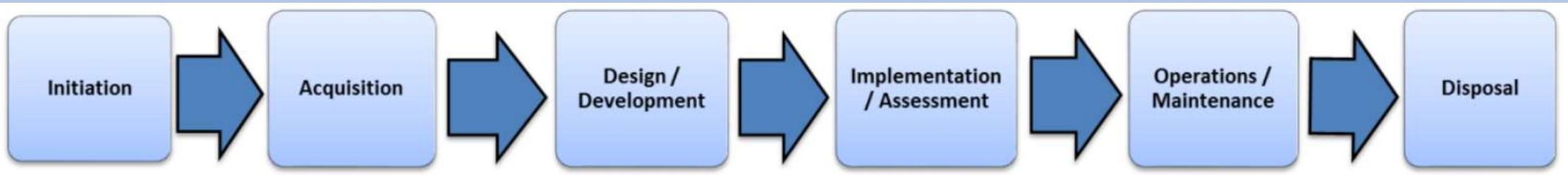
Evolving Malware Techniques: A dramatic 333% rise in malware targeting security controls was noted in 2024.

AI-Driven Cyber Hacking: AI automates attacks, exploits vulnerabilities, and bypasses banking security systems.

AI in Fraud: AI enables deepfakes, synthetic identities, and automated fraud to mimic legitimate transactions and evade detection.

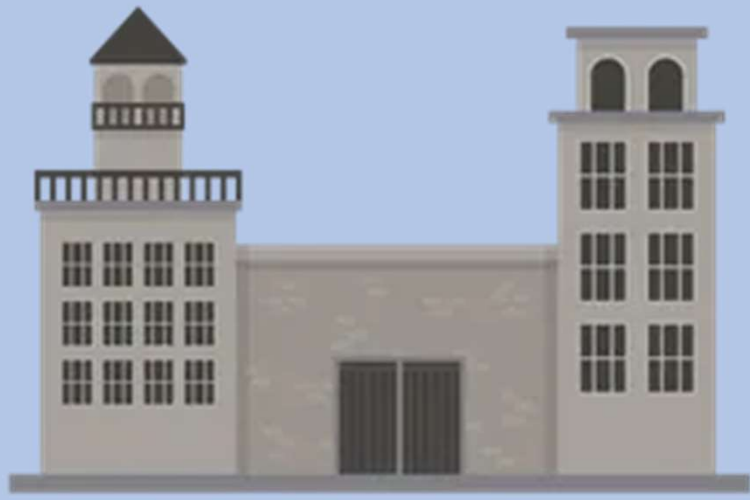
Systems Development Lifecycle

- Most organisations including Banks adopt a Systems Development Lifecycle (SDLC) methodology
- SDLC is multi-step lifecycle process and quite effective to protect computer systems against cyber threats is to integrate
- Costs and business performance often take precedence over security.
- Limited view on the asset's security before implementation stage



Cyber Security by Design (CSbD)

Hospital



Jail

What is the difference in term of design ?

Cyber Security by Design (CSbD)

- New approach to integrate security into every aspect of a systems design and development process with the aim of creating a secure final product.

- Relies on other stakeholders, including its contractors, technology developers and security experts to identify vulnerabilities within delivered capabilities and design effective controls to protect against exploitation.

- CSbD increased accountability will bring cyber security to the forefront of everyone's minds and help ensure that defence receives more resilient products

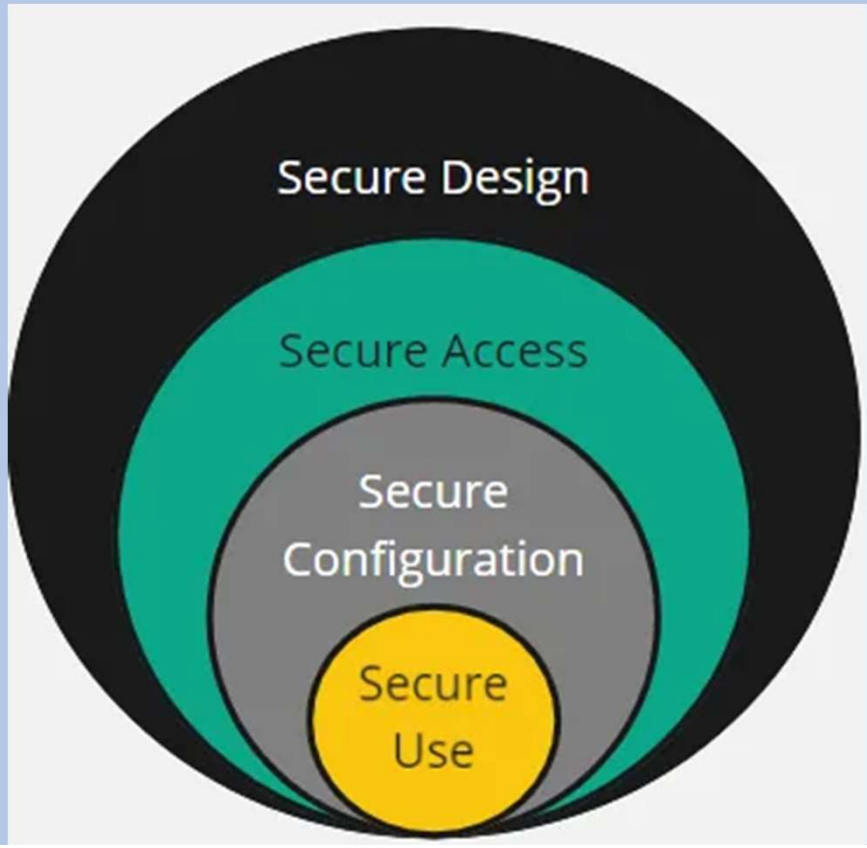
CSbD: The bigger picture

Secure Design: Strategies, tools, and processes to ensure secure design and deployment of banking systems, including digital platforms, customer applications, and internal systems for financial services.

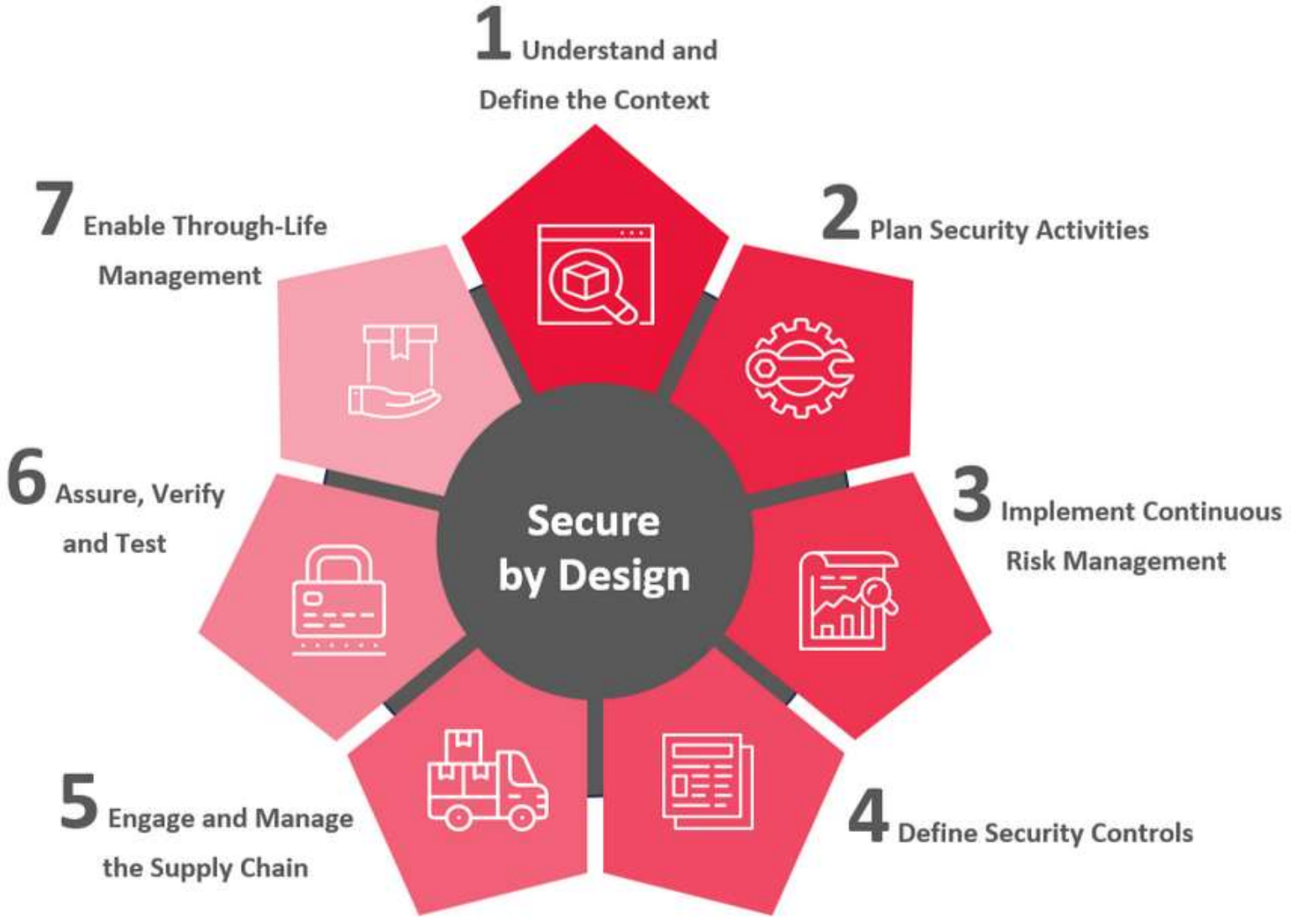
Secure Access: Protocols and tools to secure access to sensitive resources like customer data and transaction systems, regardless of location or access state.

Secure Configuration: Measures and tools to establish and maintain secure configurations for systems, applications, and network infrastructure across the enterprise.

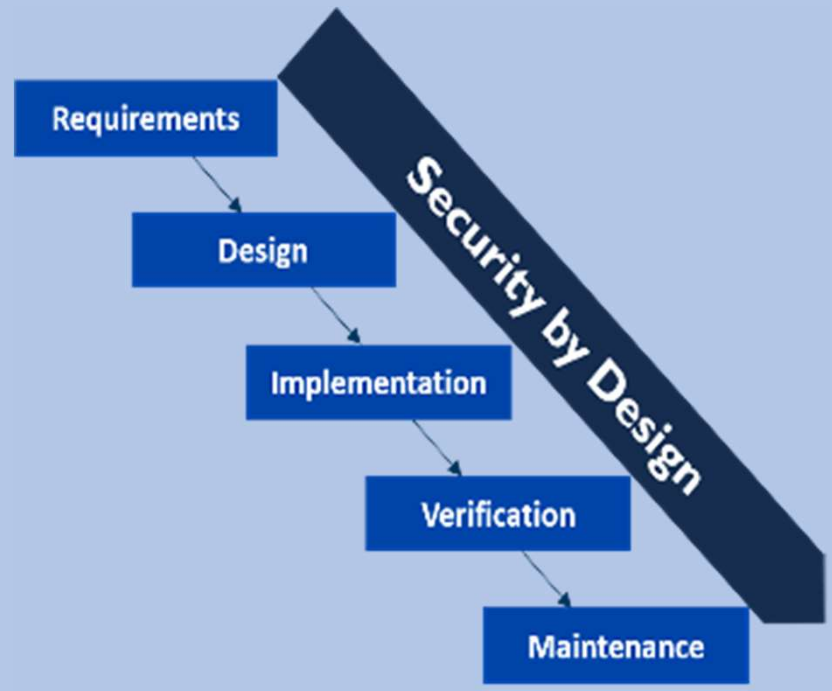
Secure Use: Procedures and tools to safeguard real-time use of data and systems, including transaction processing, data analytics, and customer interactions.



CSbD in Banking and beyond



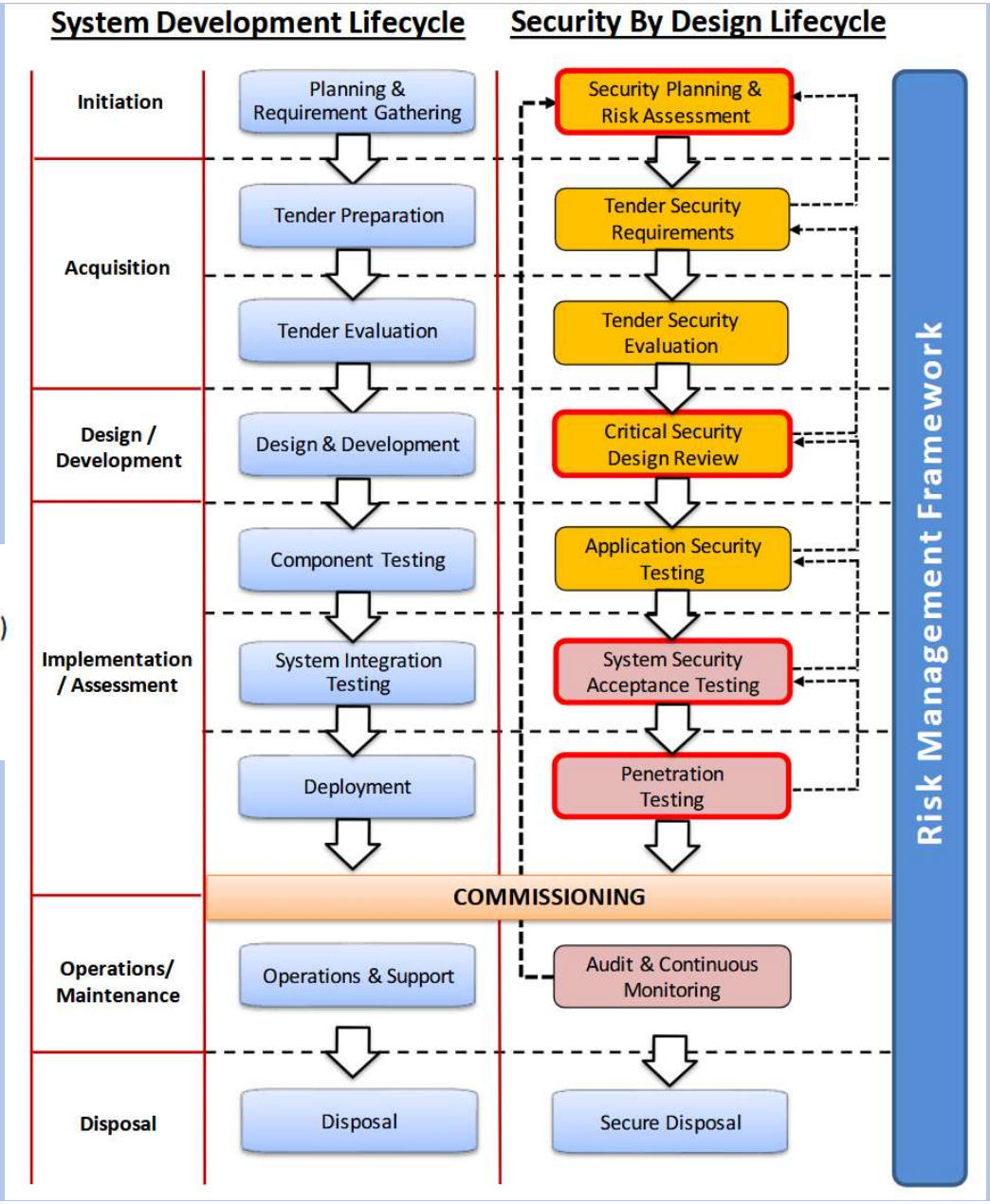
Principles (Consequences) of CSbD



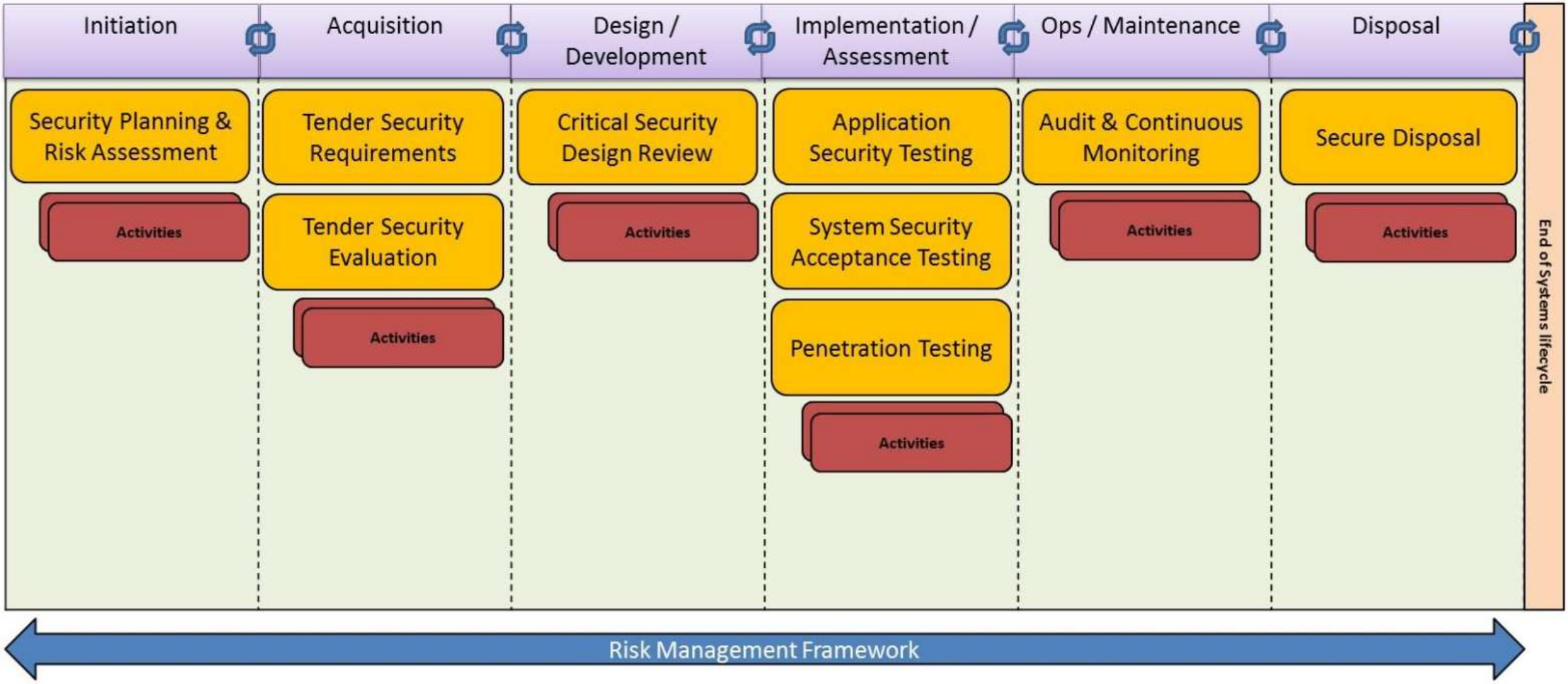
I. **Take ownership** of security outcomes
II. Embrace **transparency** and **accountability**
III. **Adapt (re-build)** organisational IT and product development

CSbD in Practice

- Performed by Project Team
- Performed by Security Officers (Security Consultants if project team does not have expertise)
- Performed by Independent Third-Party Assessor
- Milestones / Deliverables to Steering Committee



Implementing CSbD



Key Strategies for Security by Design in Banking

Benefits of Secured by Design

- Assurance that is **embedded** within capability process
- Addressing **new threat** more regularly
- Improving security awareness by incorporating far **more stakeholders**
- **Holistic view** on the capability thus more vulnerabilities being identified
- **Reducing** the requirement for new projects (saving precious resources)
- **Quality, Trust and Confidence** in internal capabilities

Challenges and considerations in CSbD

1. **Balancing** security with usability
2. Increased development **costs**
3. **Resource** constraints
4. Keeping pace with **evolving** threats
5. **Legacy** systems and Technical debt

How Artificial Intelligence can contribute ?

Automated Risk Assessment: AI analyzes system architectures to predict risks and recommend secure design improvements.

Secure Code Development: AI-powered tools identify and fix security flaws in code, ensuring secure software development.

Adaptive Security Measures: AI enables dynamic, self-learning security protocols that adapt to evolving cyber threats in banking systems.

Enhanced Access Controls: AI strengthens authentication, like biometric verification and behavior-based access monitoring, during system design.

Compliance and Monitoring: AI ensures banking systems comply with security standards and continuously monitors for design vulnerabilities.

Future of CSbD in Banking

Late Technology Adoption: Delayed digital transformation can be advantageous for **Cyber Security by Design (CSbD)**, as newer systems can integrate advanced security measures from inception, avoiding legacy vulnerabilities.

Secure Communication: Implement secure-by-design protocols and AI-optimized encryption techniques to ensure safe and efficient transfer of sensitive financial data.

Robust Defenses: AI-driven frameworks proactively detect, prevent, and mitigate cyberattacks during system design, ensuring system resilience and integrity.

Scalable Frameworks: Adaptive AI-based systems, such as federated and reinforcement learning, enable secure and scalable solutions to support growing and diverse banking infrastructures

Thank You

Questions ?