



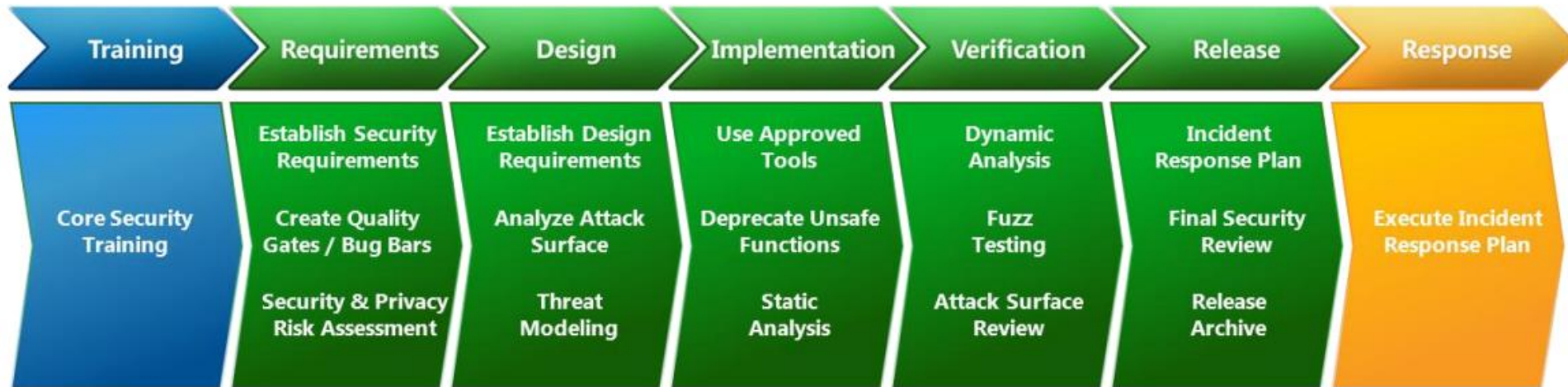
HM Government

Secure Development

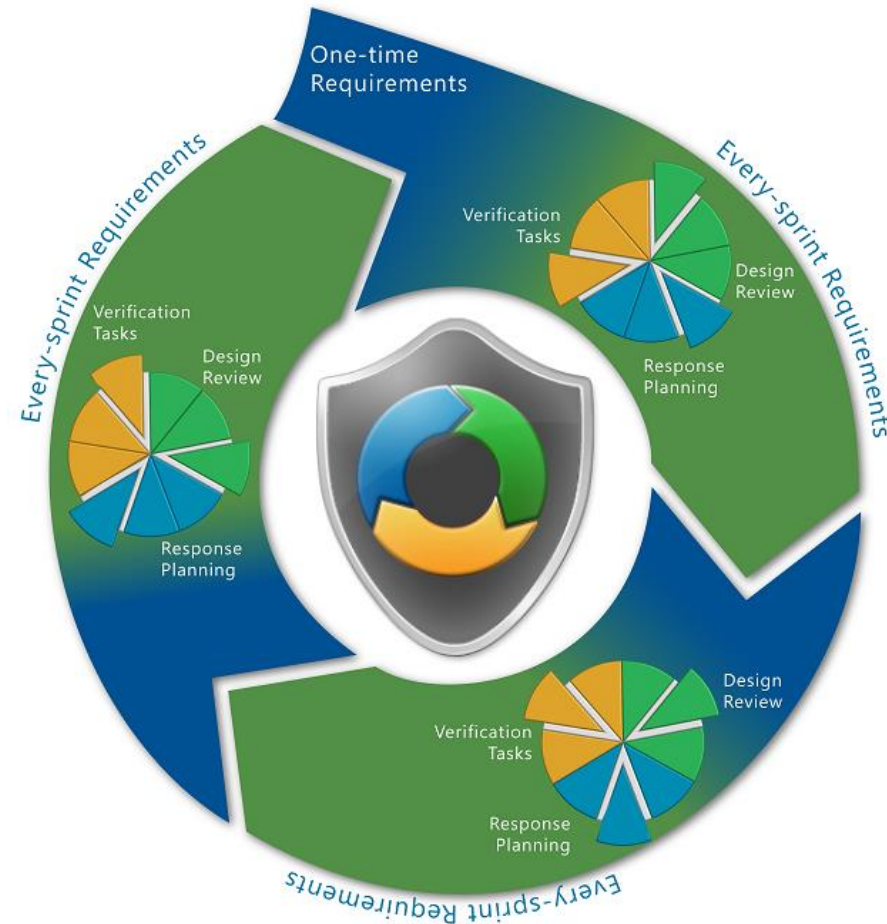
Secure Development Lifecycle Overview



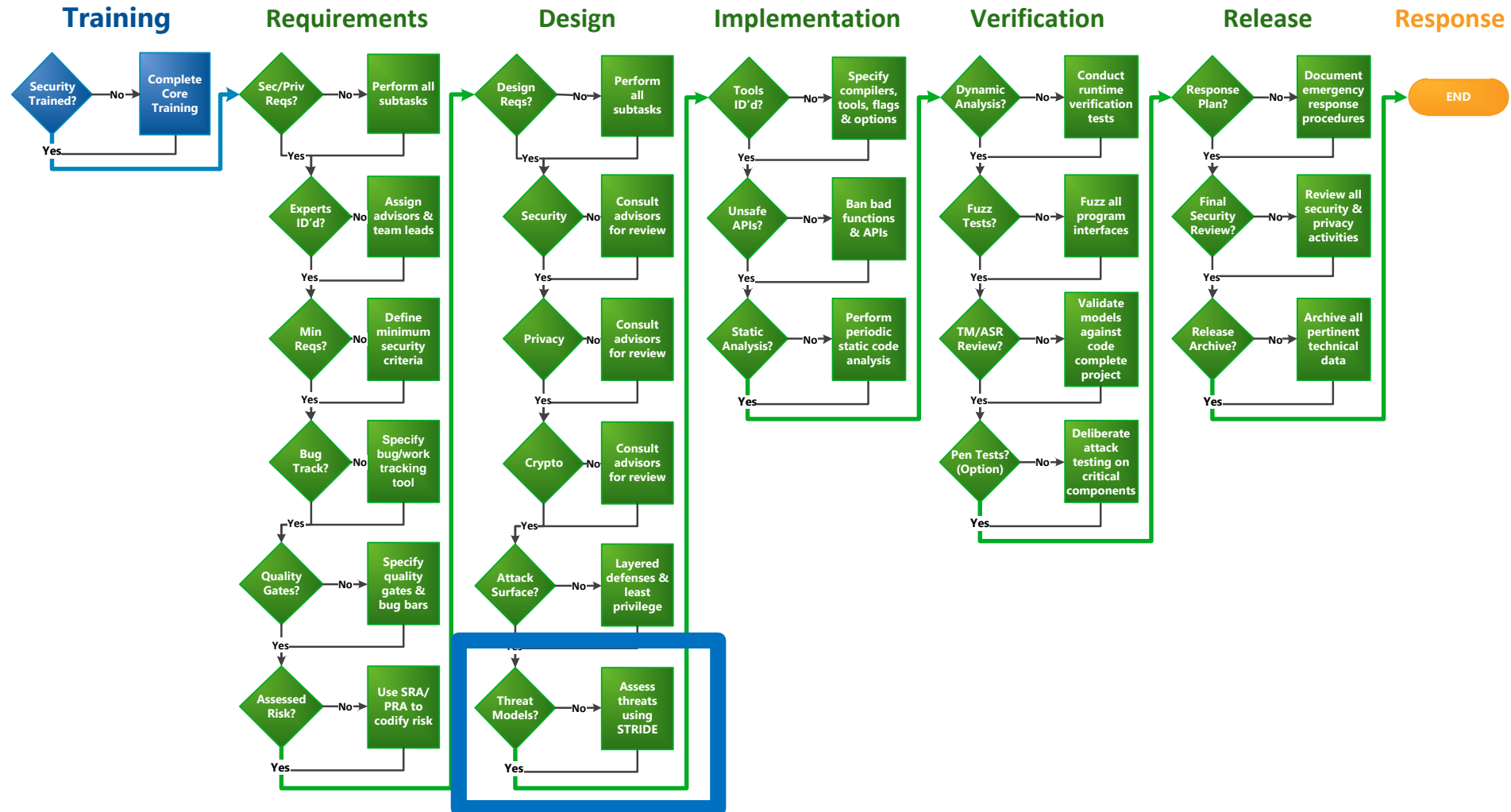
Secure Development Lifecycle



Agile Secure Development Lifecycle



SDL exploded



Secure Development Lifecycle

Training

Training – Basic

- Security
- Privacy
- Threat Modelling
- Secure Design, Development and Testing



Training - Advanced

- Secure Design
 - Attack Surface Reduction
 - Threat Modelling
- Secure Development
 - Secure Coding & Defensive Coding
 - Web Applications
 - Secure Database Access
- Secure Testing
 - Fuzzing & Penetration Testing
 - Code Review & Threat Model Verification



Secure Development Lifecycle

Requirements

Requirements

- Establish Security Requirements
- Create Bug Bars / Quality Gates
 - Definition of Done
- Perform Security and Privacy Risk Assessments



Secure Development Lifecycle

Design

Design

- Establish Design Requirements
- Perform Attack Surface Analysis & Reduction
- Create Threat Models



Secure Development Lifecycle

Implementation

Implementation

- Use Approved Tools
- Perform Static Analysis
- Follow Secure Coding Guidelines



Secure Development Lifecycle

Verification

Verification

- Perform Dynamic Analysis
- Perform Fuzz Testing
- Perform Penetration Testing
- Conduct Code Reviews
- Conduct Threat Model Verification
- Conduct Attack Surface Review



Secure Development Lifecycle

Release

Release

- Create Incident Response Plan
- Conduct Final Security Review
- Certify Release and Archive



Secure Development Lifecycle

Response

Response

- Execute Incident Response Plan



Secure Development Lifecycle Summary

- Do it.
- No, really. Do it! 😊

