Secure Agile Development

With FISMA Compliance

Stop Reacting. Start Securing.

https://www.fyrmassociates.com/

FYRM Overview

Qualifications

- Experience
- Respected Partner
- FedRAMP 3PAO

Performance

- CPAR 4/4
- CMS, DOE
- Fortune 500

Strategy

- Secure Agile
- Knowledge Sharing
- Effective & Efficient

Projects completed: On time Accurately Within budget

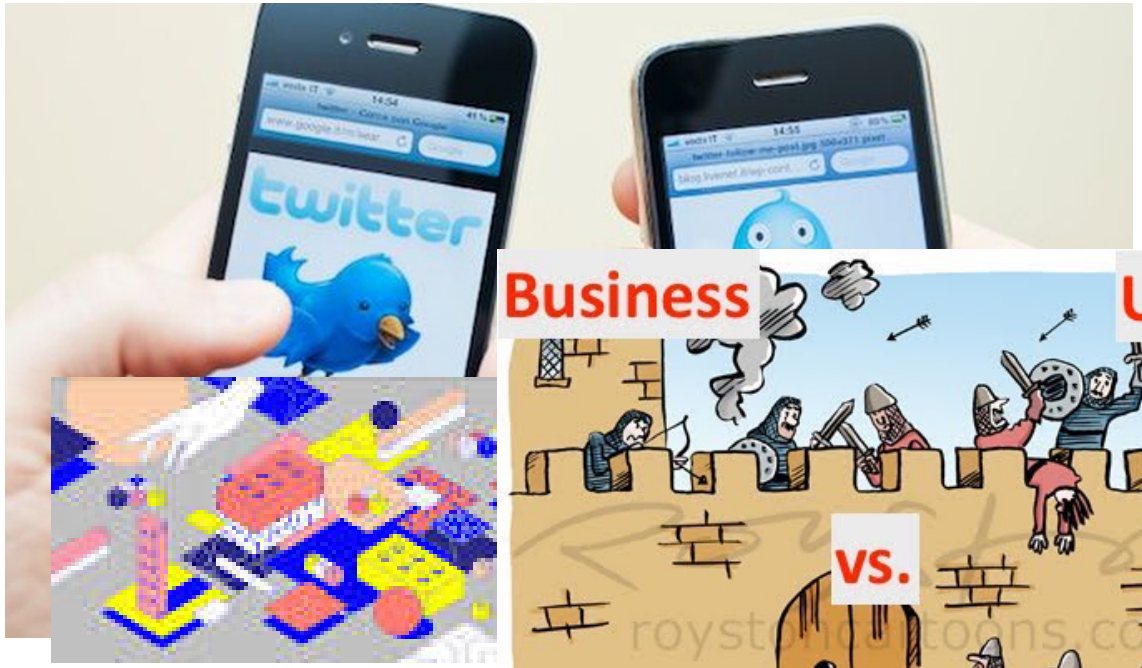
Agenda

- Agile Overview
- Integrating Security into an Agile World
- FISMA Compliance Integration
- Recommendations for success

Agile Overview

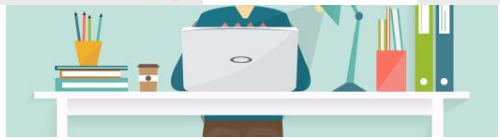
- But first, let's talk about how applications are made.

1. Planning



3. Design

2. Requirements

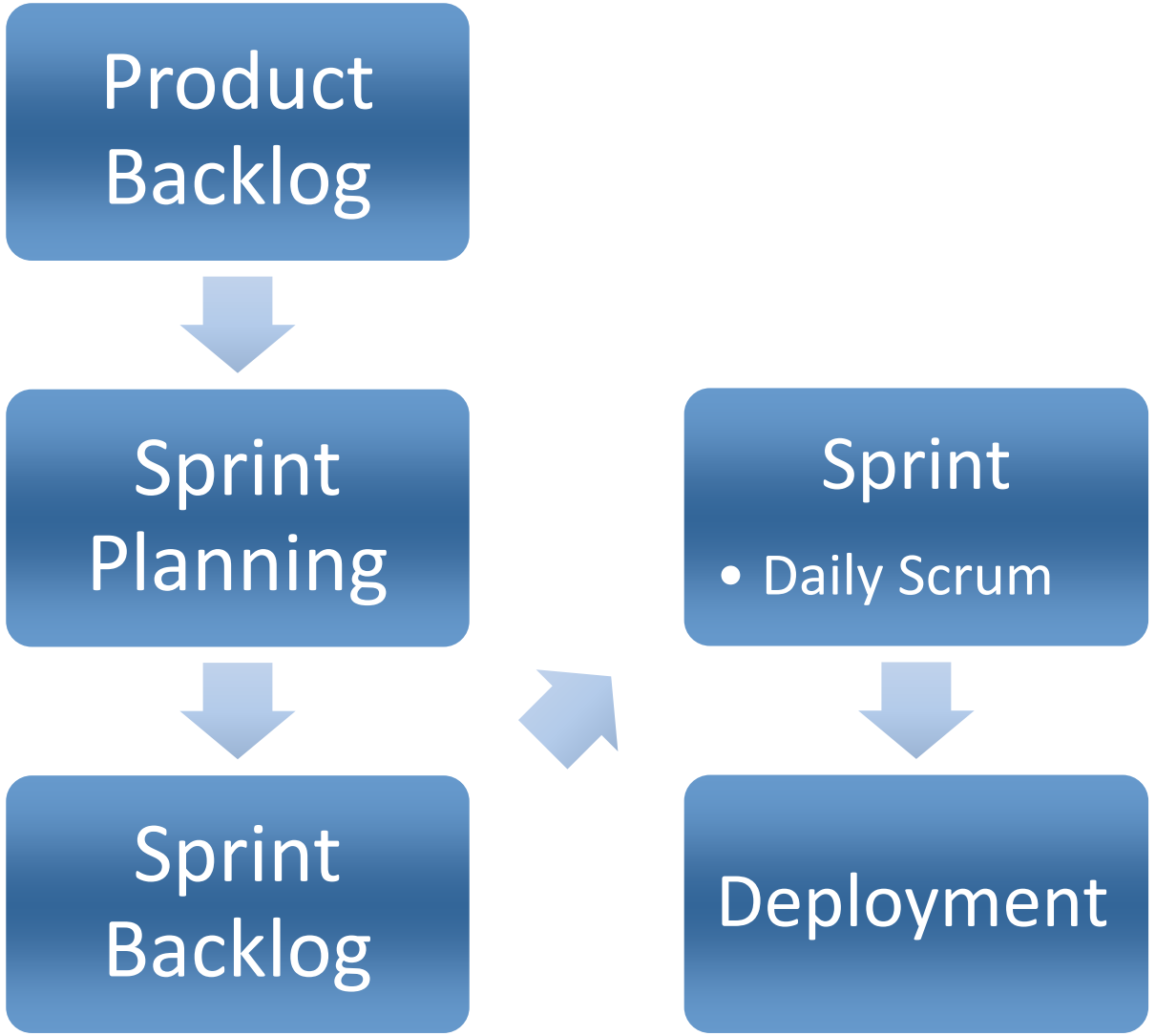


4. Coding / Implementation

ng
AT, Security)

6. Implementation

Agile Overview



Rules of Agile Development:

1. You don't speak about the rules of Agile development
2. There are no rules of Agile Development

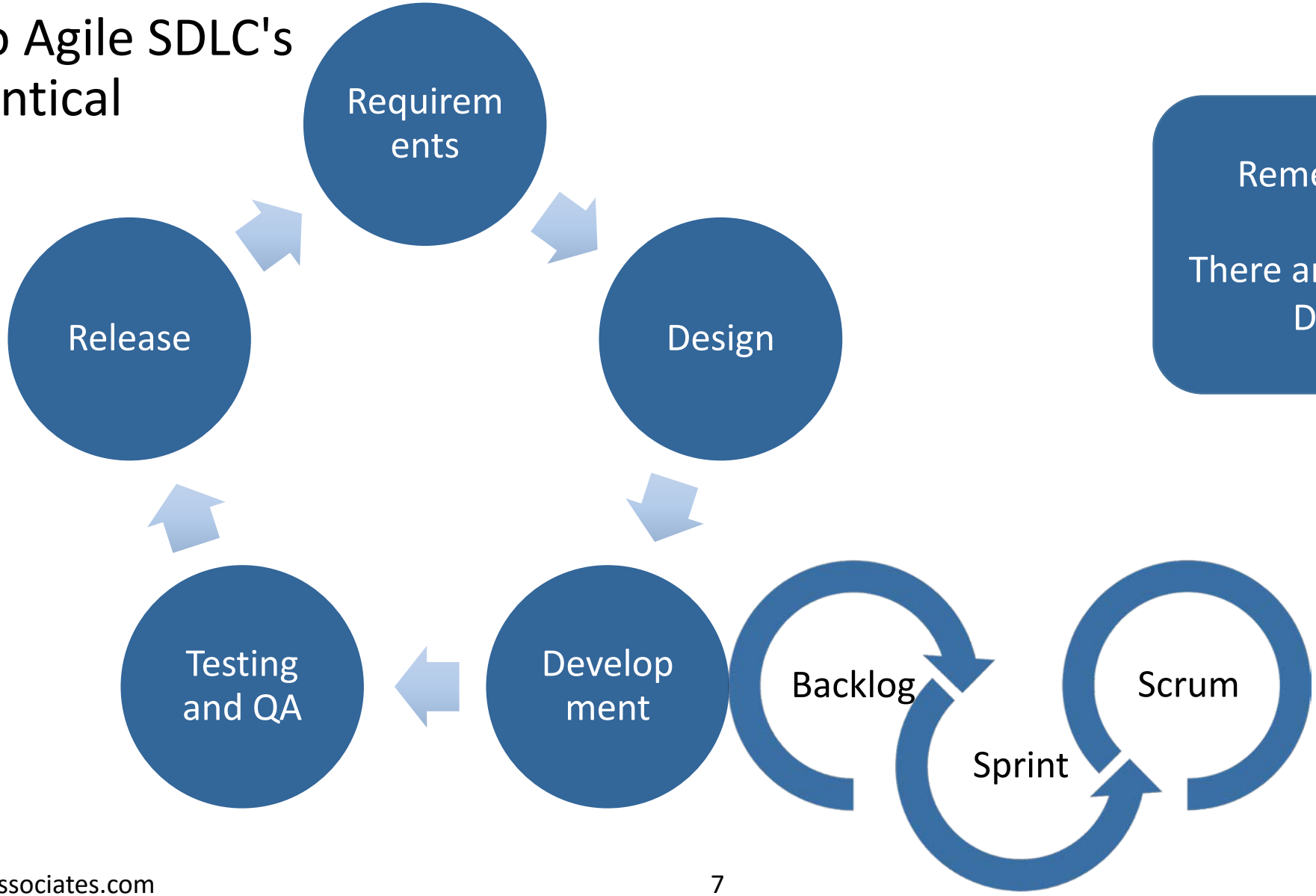
Agile Overview

Mapping Non-Security Tasks to an Agile SDLC:

Product Backlog	• Requirements • Design • Use Cases / Stories
Sprint Planning	• Development goals for sprint • Use Cases / Stories for sprint
Sprint Backlog	• Goal breakdown into tasks • Development tasks for use cases / stories
Sprint	• Coding • Unit Testing, Functional Testing, Code Review • Scrum: Design, Planning
Deployment	• QA • Testing

Agile Overview

No two Agile SDLC's are identical

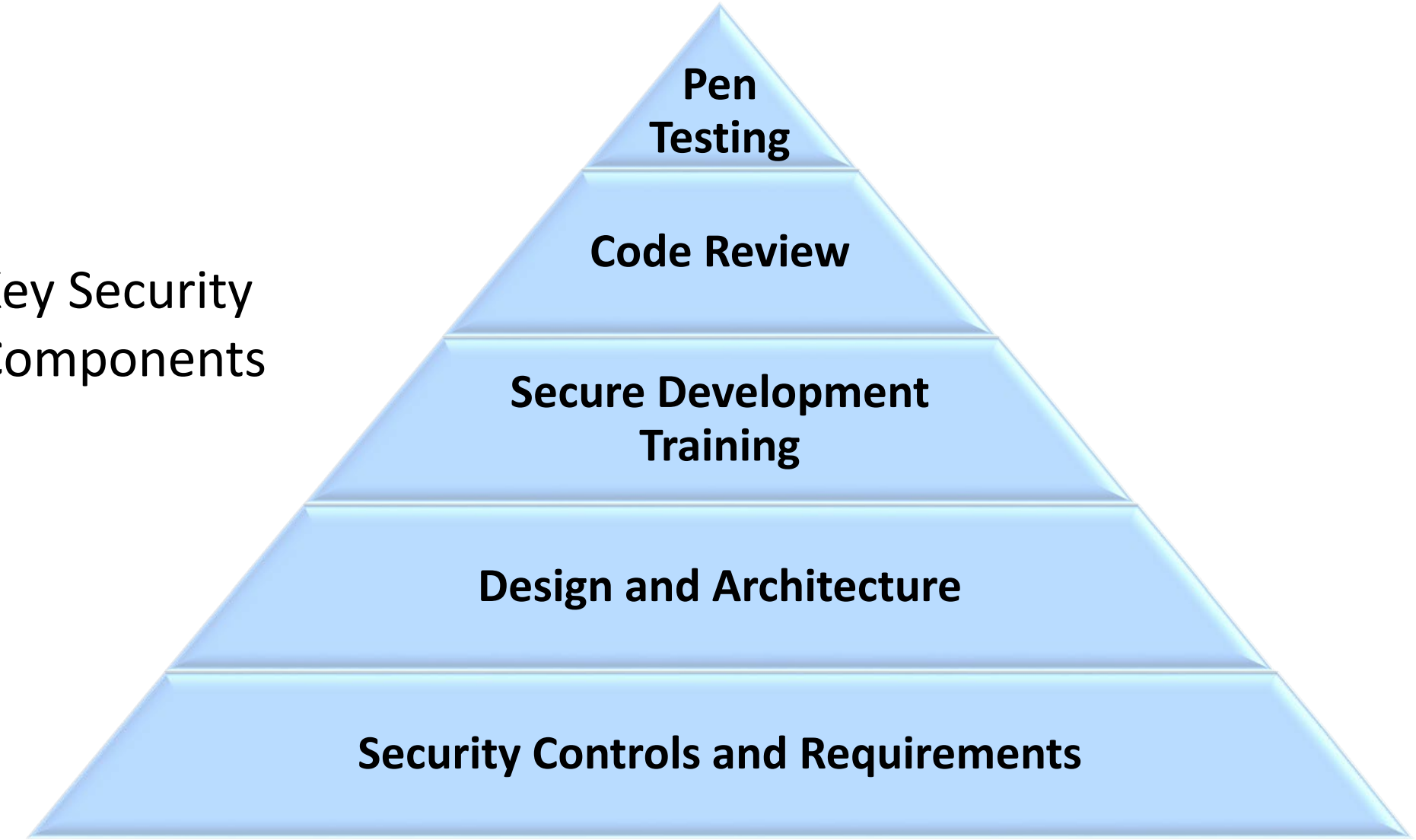


Remember Rule # 2:

There are no rules of Agile Development

Integrating Security into an Agile World

Key Security Components

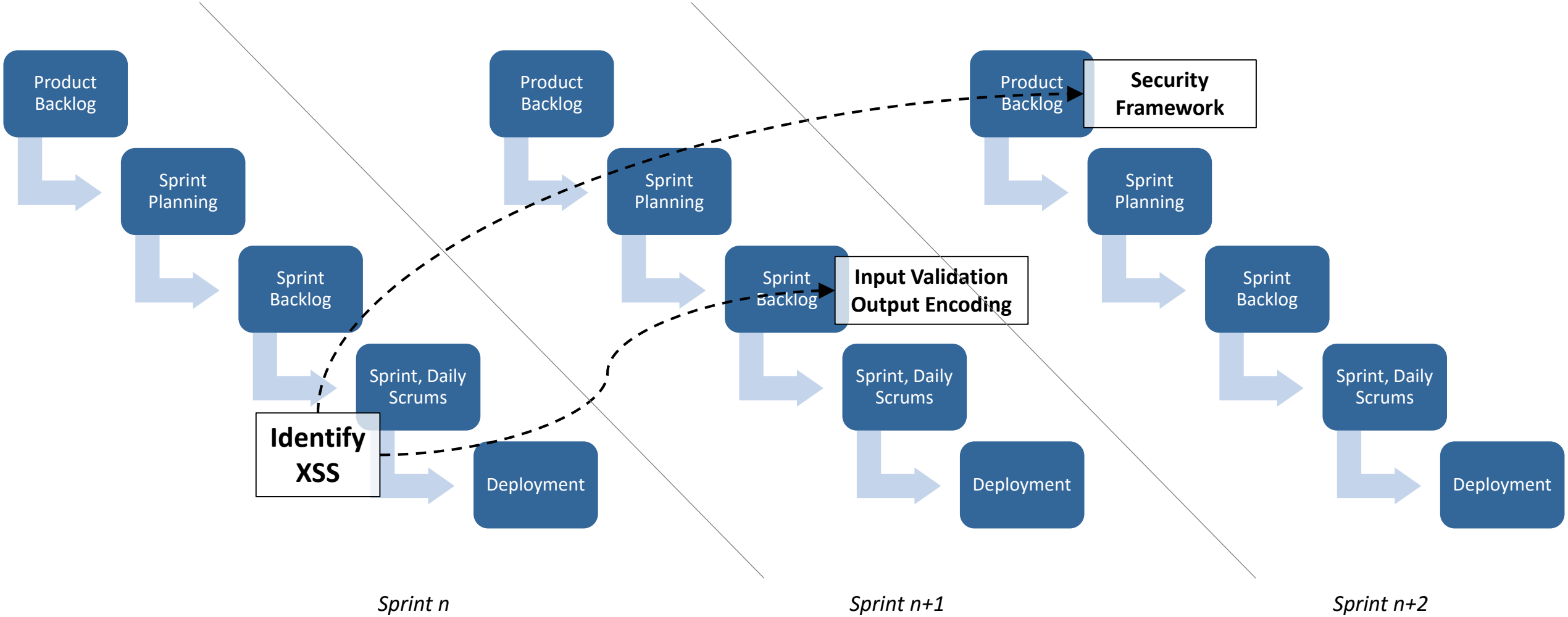


Integrating Security into an Agile World

Mapping Security Tasks to an Agile SDLC:

Product Backlog	• Security Controls and Requirements • Secure Design • Abuse Cases / Malicious User Stories
Sprint Planning	• Security goals for sprint • Abuse Cases / Malicious user stories for sprint
Sprint Backlog	• Security goal breakdown into tasks • Security components for development tasks and security task development
Sprint	• Secure Coding • Security Testing • Scrum: Secure Design, Security Planning
Deployment	• Security Testing

Integrating Security into an Agile World



Integrating Security into any SDLC

Design, Requirements

- Security controls & requirements
- Design and architecture
- Secure development training

Development

- Security controls & requirements
- Design and architecture
- Code review
- Penetration testing

Testing, Deployment, Operations

- Code review
- Penetration testing
- Control assessment

FISMA Compliance Integration

Align activities and schedules

- Development activities, control testing
- Information Security activities, goals, projects
- FISMA requirements, reporting/ATO deadlines

Technical security testing

- Review security control design
- Code review
- Penetration testing

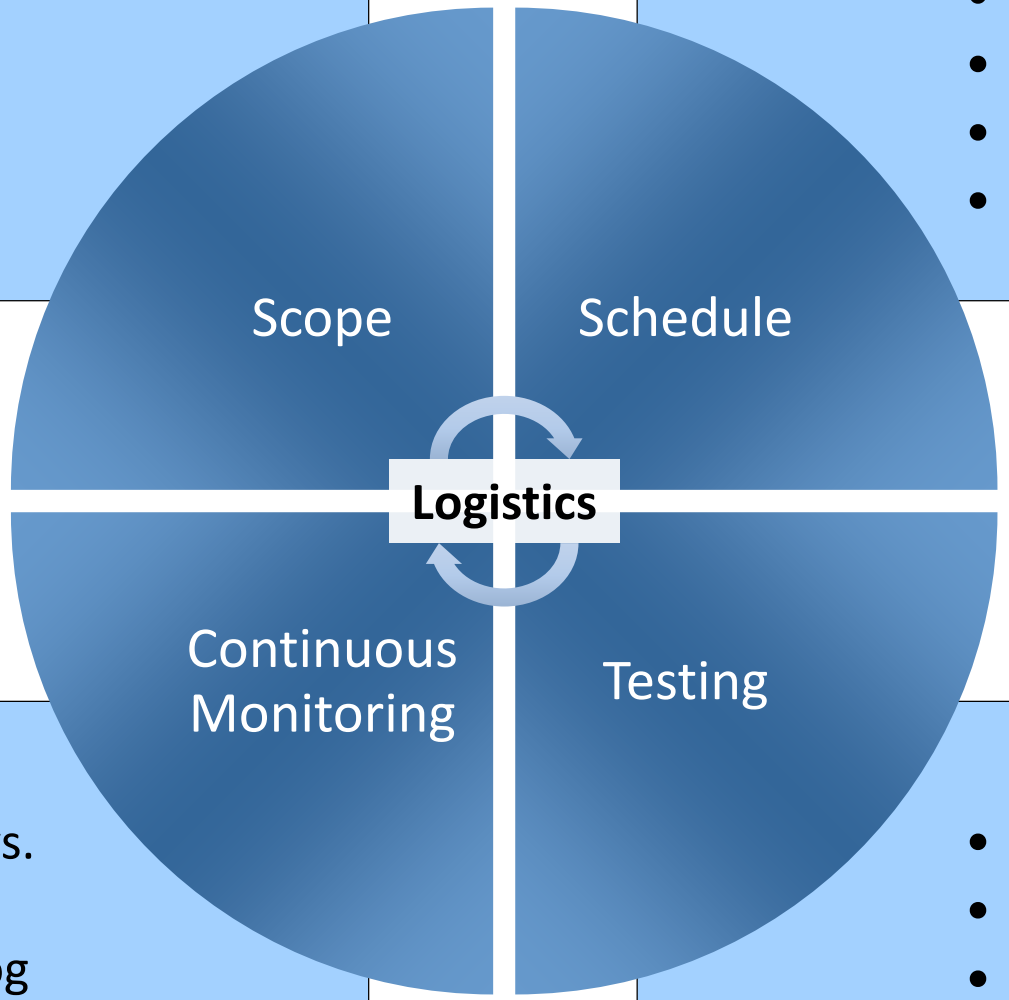
Security controls assessment

- Obtain evidence for non-technical controls during development
- Align with annual testing requirements

FISMA Compliance Integration

- Security Controls
- Sprint Backlog
- In-development testing vs. Annual SCA

- Scrum
- Development meetings
- Release dates
- ATO deadline



- Reporting security issues vs. FISMA findings
- Add remediation to Backlog

- Test environment, accounts
- Application testing scope
- Other evidence

Secure Agile Development

Pros and Cons with Secure Agile Development

Cons

- No security testing in "Pure" Agile
- More security issues more frequently
- Difficulty with security integration

Pros

- "Pure" Agile is not very common
- Well suited for quicker remediation
- Improved security and compliance once integrated

Secure Agile Development

Subject Matter Experts

- Secure Development SME
- Application Security SME
- Key POC's for each team

Security testing logistics

- Environment, accounts, etc.
- Integrate security recommendations
- Integrate security remediation

Recommendations to improve success

Team Integration

- Developers learn security
- IS/Compliance learn development
- Bridge the gap

Development artifacts

- Anti-agile
- Diagrams, data flow and definitions
- Security requirements, abuse cases

Presenter

Matthew Flick

Managing Principal

matt.flick@fyrmassociates.com

Stop Reacting. Start Securing.

https://www.fyrmassociates.com/