INCOSE Healthcare Working Group

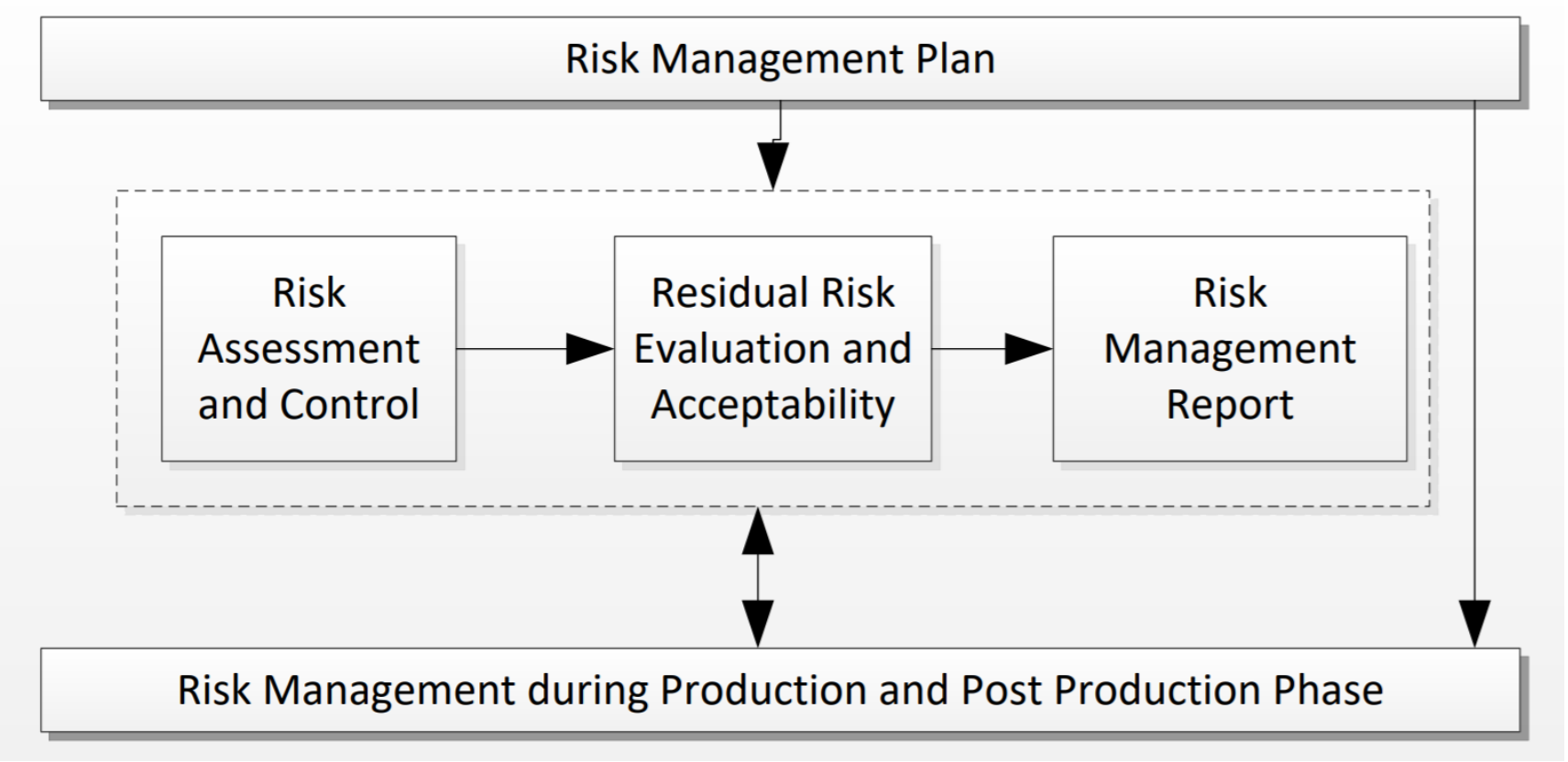
4th Annual Systems Engineering in Healthcare Conference

INCOSE

Medical Device Security Assurance and Vulnerability Disclosure

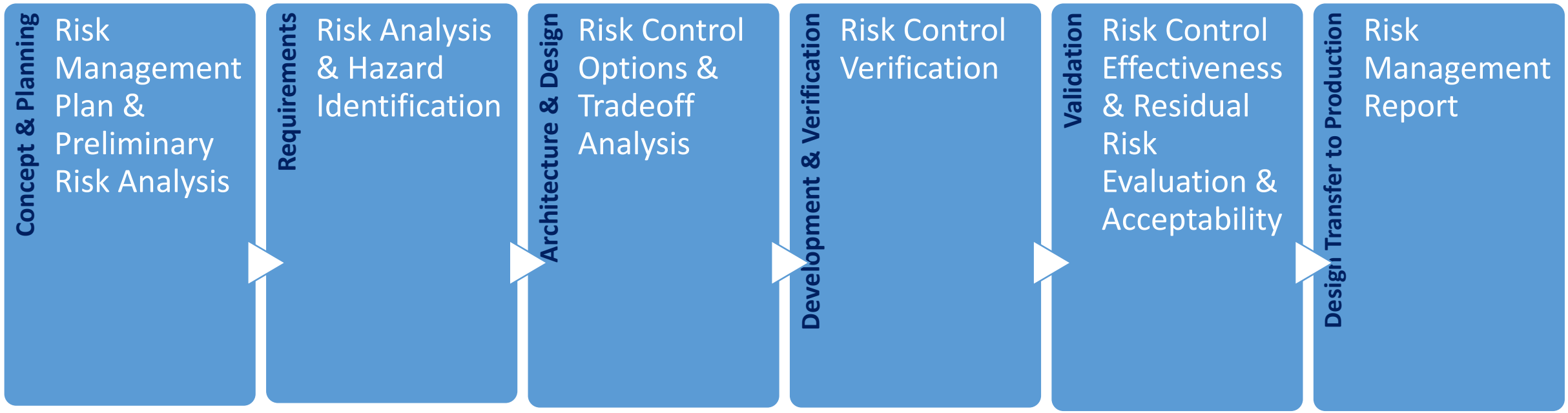
Copyright © 2018 by Matt Russo, Permission granted to INCOSE to publish and use.

Risk Management Process Overview

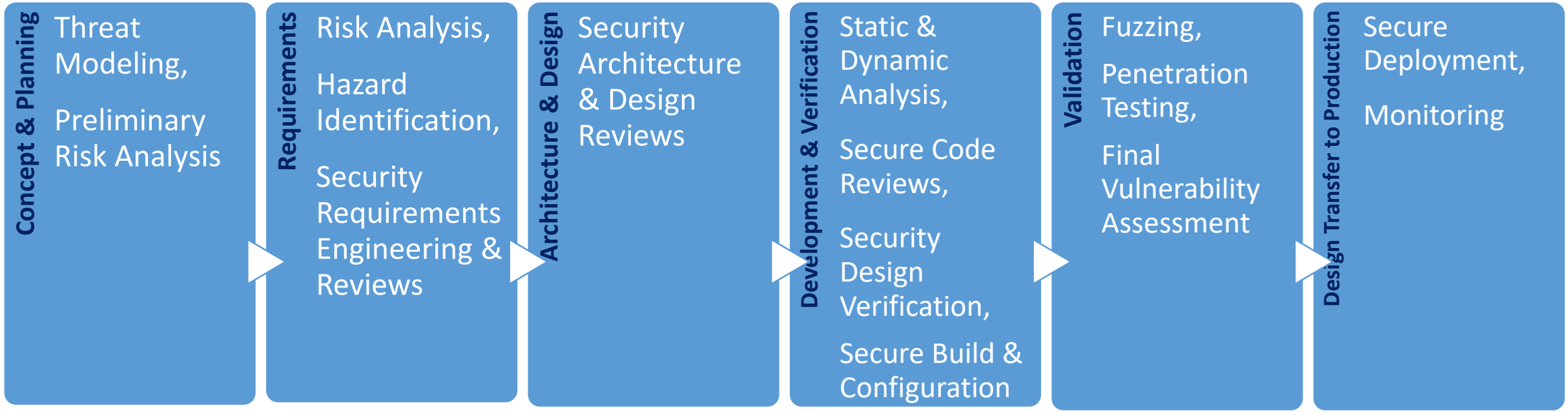


- Medical Device Manufacturers are focused on building security into new products
- This starts with a comprehensive Risk Management Process during the development of new products

Security Risk Management in the System Development Lifecycle



Security Engineering in the System Development Lifecycle



Comprehensive Pre-Market Testing is Key

Pre-Market Testing Requirements

- Appropriate resources
  - Risk is the driver, not schedule or budget

- Appropriate skill
  - Mix of internal and external expertise

- Independent Oversight

Outline of an Internal Testing Function

Product Testing services for use during the development of new products – needs to be in a separate function from R&D

Product Testing

- Independent testing
- Can be iterative
- Could help increase the quality of testing
- Assist in controlling the cost to R&D groups
- Compliment testing strategy to leverage expert 3rd party organizations
- Build out of tools to be leveraged
- Could develop chargeback model

Vendor Organization and Negotiation

- Assist in management of testing 3rd parties
- Vet service firms including core competencies
- Maintain "evaluation" database
- Assist with negotiation of rates

What About Legacy Products?

- Risk Management doesn't stop once a product is approved / released
- Ongoing process to monitor security signals for existing products
- May need to publicly disclose vulnerabilities and patch / update
- Vulnerabilities may impact future development and risk decisions

What can a company do to be proactive about legacy risk?

Post Market Testing or Red Teaming

Red Teaming is a process designed to detect network and system vulnerabilities and test security by taking an attacker-like approach to systems. (*SANS, 2003*)

- Testing process to identify potential issues prior to external discovery

  Blackbox: represents a hacker; no information provided prior to assessment

  Whitebox: efficient assessment with full access to internal resources and design information provided

  Graybox: some information provided, but not full system knowledge

This function can also assist in the independent assessment of security researcher inquiries

https://www.sans.org/reading-room/whitepapers/auditing/red-teaming-art-ethical-hacking-1272

Vulnerability Disclosure

The practice of reporting security flaws in computer software or hardware

- Vulnerability disclosure can be a controversial topic
- Regulatory bodies (i.e. FDA) and other US Agencies (ICS / US CERT) are supporting more transparency on this topic
- Can be a challenging time for organizations, developers, and stakeholders responsible for development or management of a product or service
- Important to not to personalize notice of a possible vulnerability
- Critical to remain professional in all communications

Objectives for a Disclosure Program

OBJECTIVES

External

- Create a consistent, comprehensive and global coordinated response capability that allows third parties to easily report vulnerabilities

Internal

- Create a process to receive, understand the impact and create team involvement through triage, verify, and respond to the finder/researcher / users / regulators

Disclosure Program Tips

- Need for a consolidated “intake” process for security inquiries
- Universal agreement that coordinated response is important at all levels
- Identify internal team members across all functions
  - Likely to include legal, Security SMEs, PR, Leadership, etc.
- Have a plan on when something is closed
- Need for widespread visibility into the status of inquiries internally
- Security is NOT an advantage against competitors – shouldn’t be used for marketing

Someone’s feelings are going to get hurt – don’t let that derail the process!

Anatomy of a General Disclosure Process

Do we need to do something? → How big of a deal is this? → What are we going to do? → Do it. → What did we do? Let's make sure it doesn't happen again.

Post-release is critical to ensure that lessons learned are used to improve future activities

360 Degree View

Public disclosure of vulnerabilities can be uncomfortable for companies. It challenges internal processes, past business decisions, and strains resources. It's REACTIVE. To be more PROACTIVE, organizations can develop more secure products by leveraging Security Assurance Concepts.

INCOSE
Healthcare Working Group
4th Annual Systems Engineering in Healthcare Conference

Thank you for attending!

Share your experiences at #HWGSEC