Counter Insider Threat Strategy: Engineer The Insider Threat Program, Not The Tools

NITSIG Insider Threat
Symposium & Expo
September 10, 2019

The Insider Threat Tool Process

Customer: Would you tell me, please, which way I ought to go from here?

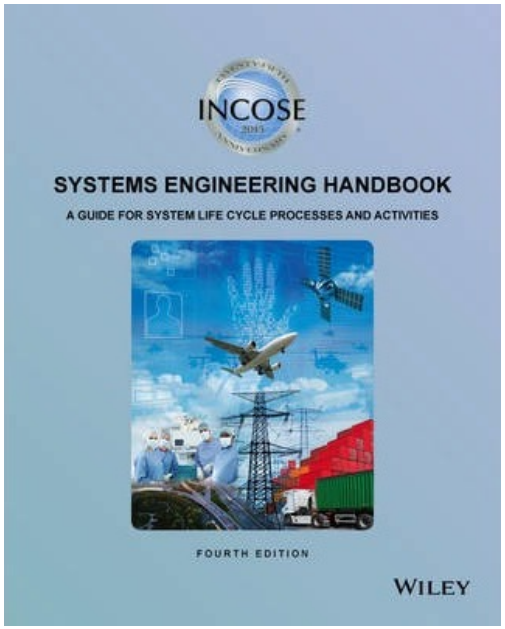
Vendor: That depends a good deal on where you want to get to.

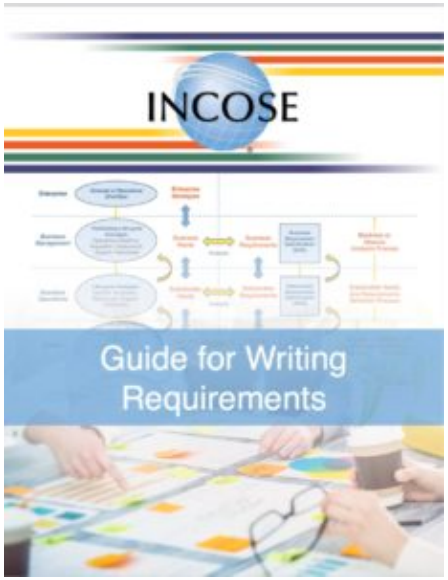
Customer: I don’t really know where.

Vendor: Then we have the perfect tool!

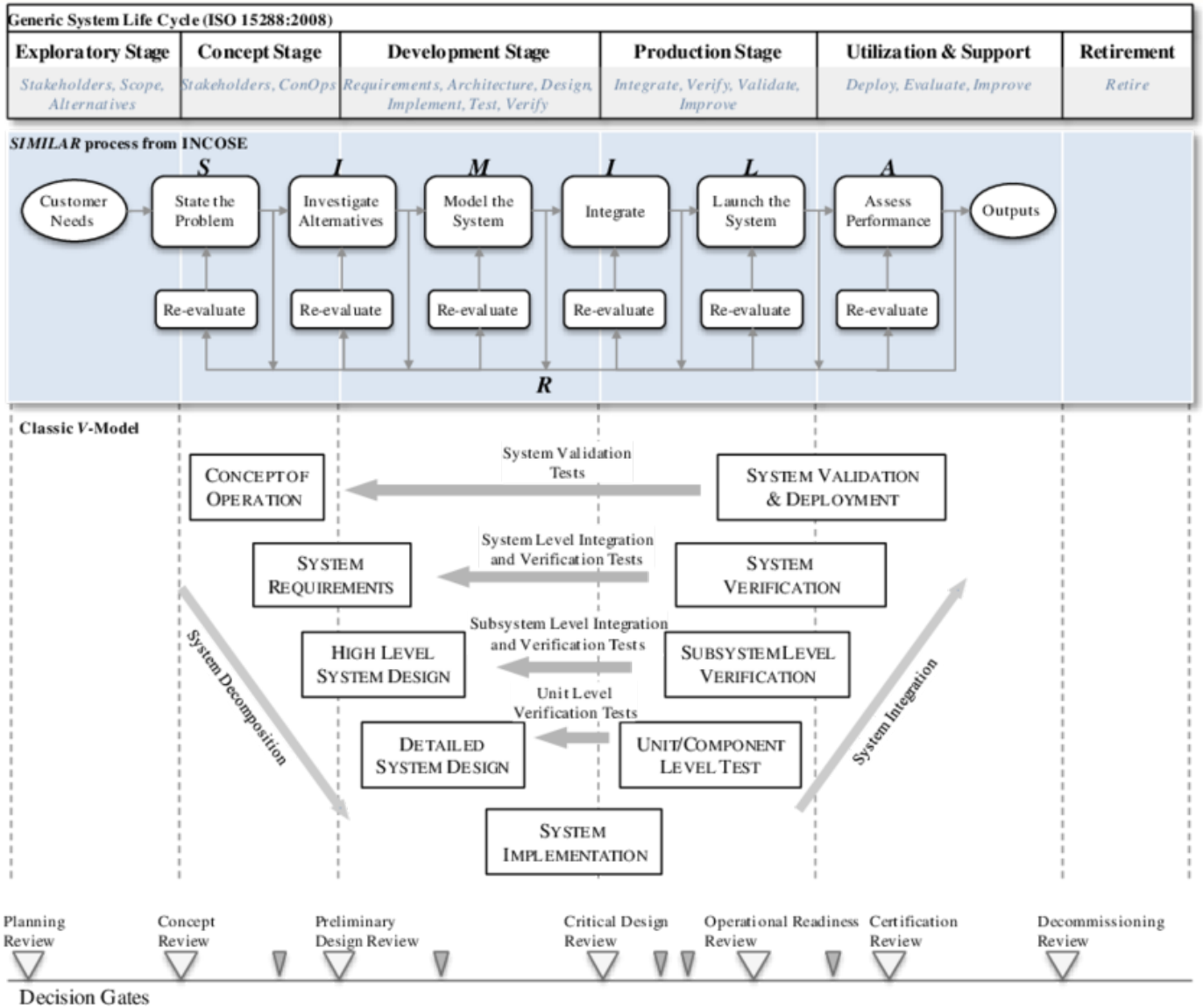
References

INTERNATIONAL STANDARD
ISO/IEC/ IEEE 15288
Systems and software engineering — System life cycle processes
ISO IEC
IEEE


INCOSE
SYSTEMS ENGINEERING HANDBOOK
A GUIDE FOR SYSTEM LIFE CYCLE PROCESSES AND ACTIVITIES
FOURTH EDITION
WILEY


INCOSE
Guide for Writing Requirements

The Systems Engineering Process



Don’t Panic!

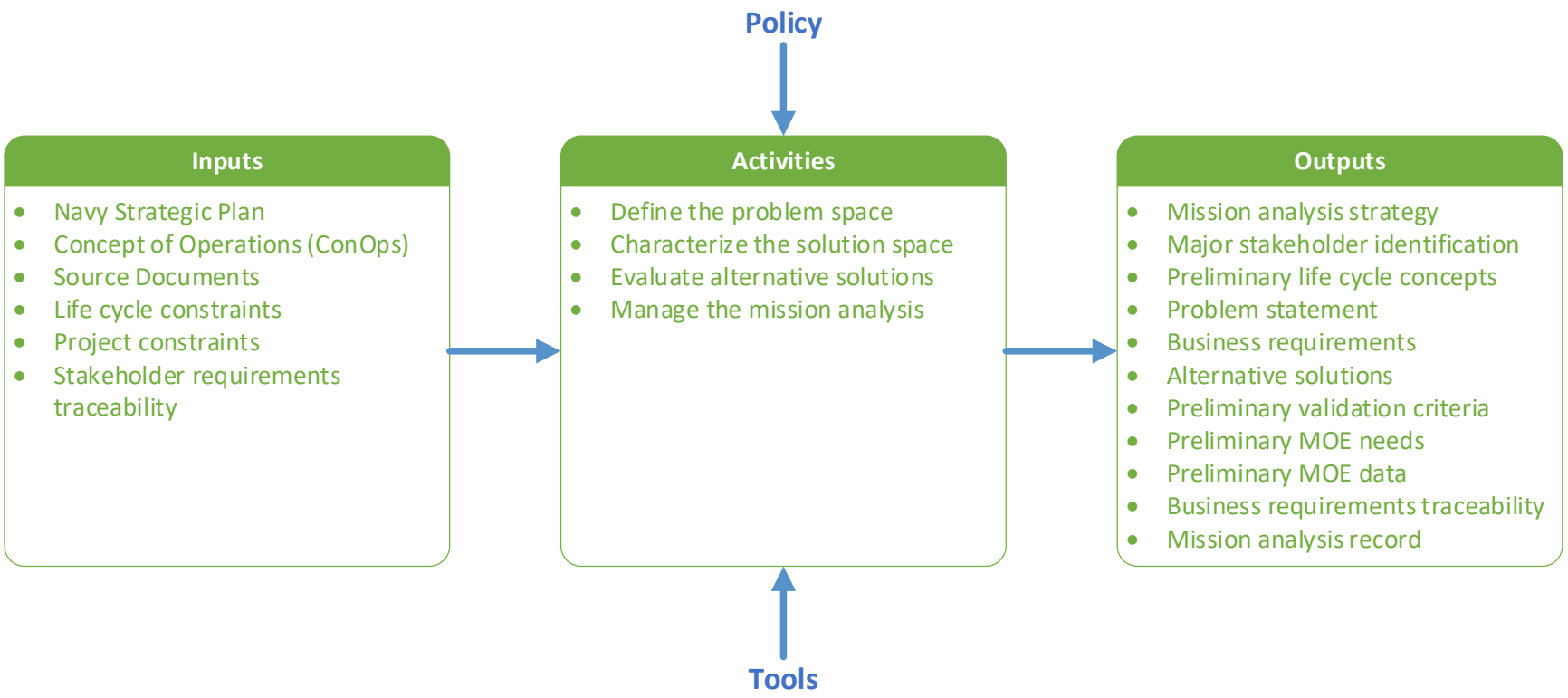
- Most of your tool needs can be determined by the first three processes!

1. Mission Analysis
2. Stakeholder Needs and Requirements Definition
3. System Requirements Definition

1: Mission Analysis

- Define the Mission Problem
  - I know the problem!
    - Do you really?
- Characterize the Solution Space
  - Requirements!
    - Use cases
- Determine **Potential** Solutions
  - Meets the Mission
  - Fulfills the Requirements

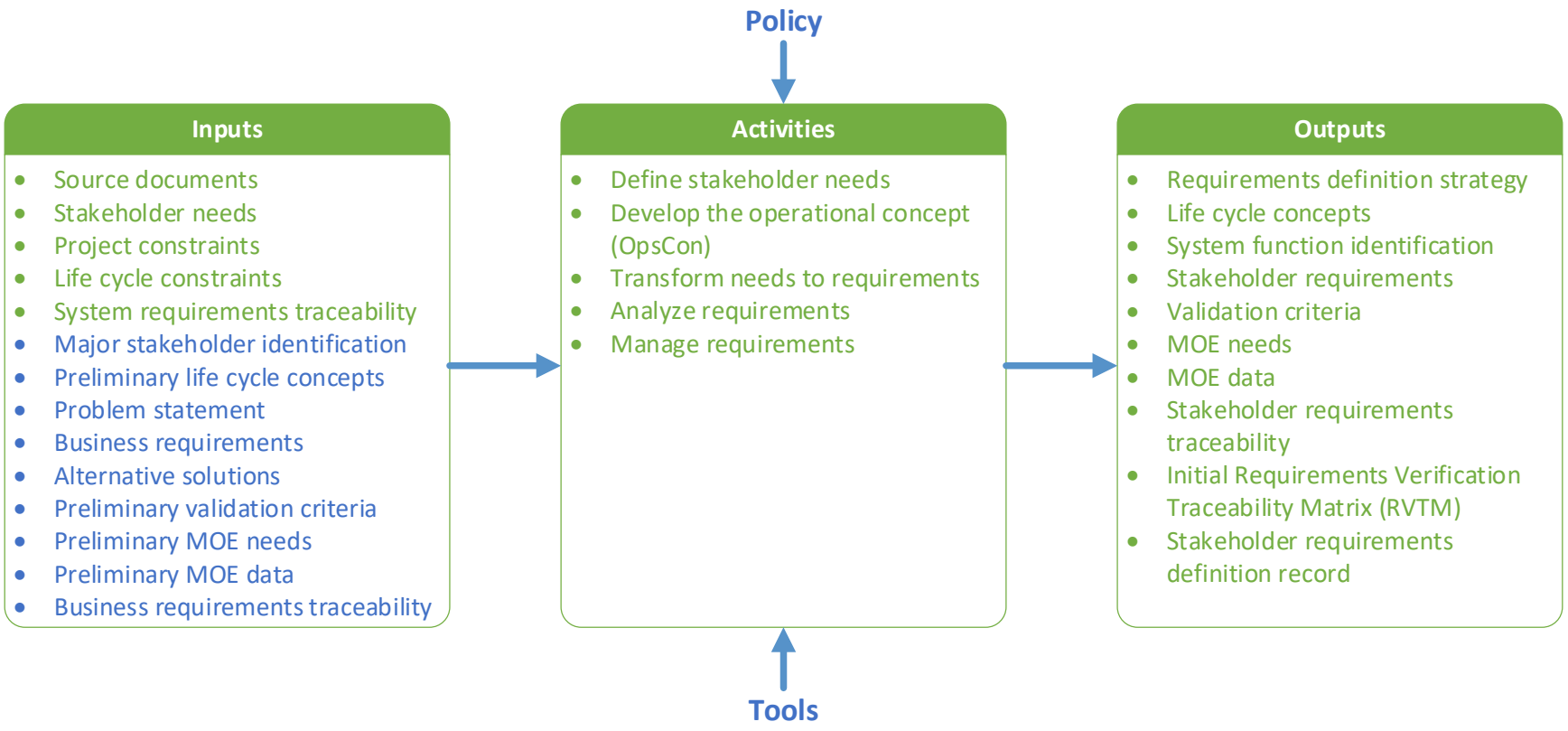
Mission Analysis Input - Process - Output



2: Stakeholder Needs and Requirements

- Goal: an *implementation-free* understanding of stakeholder needs
  - The what, not the how
- Stakeholders include stakeholders of constituent systems, capability users, customers, and responding agencies

Requirements Input - Process - Output



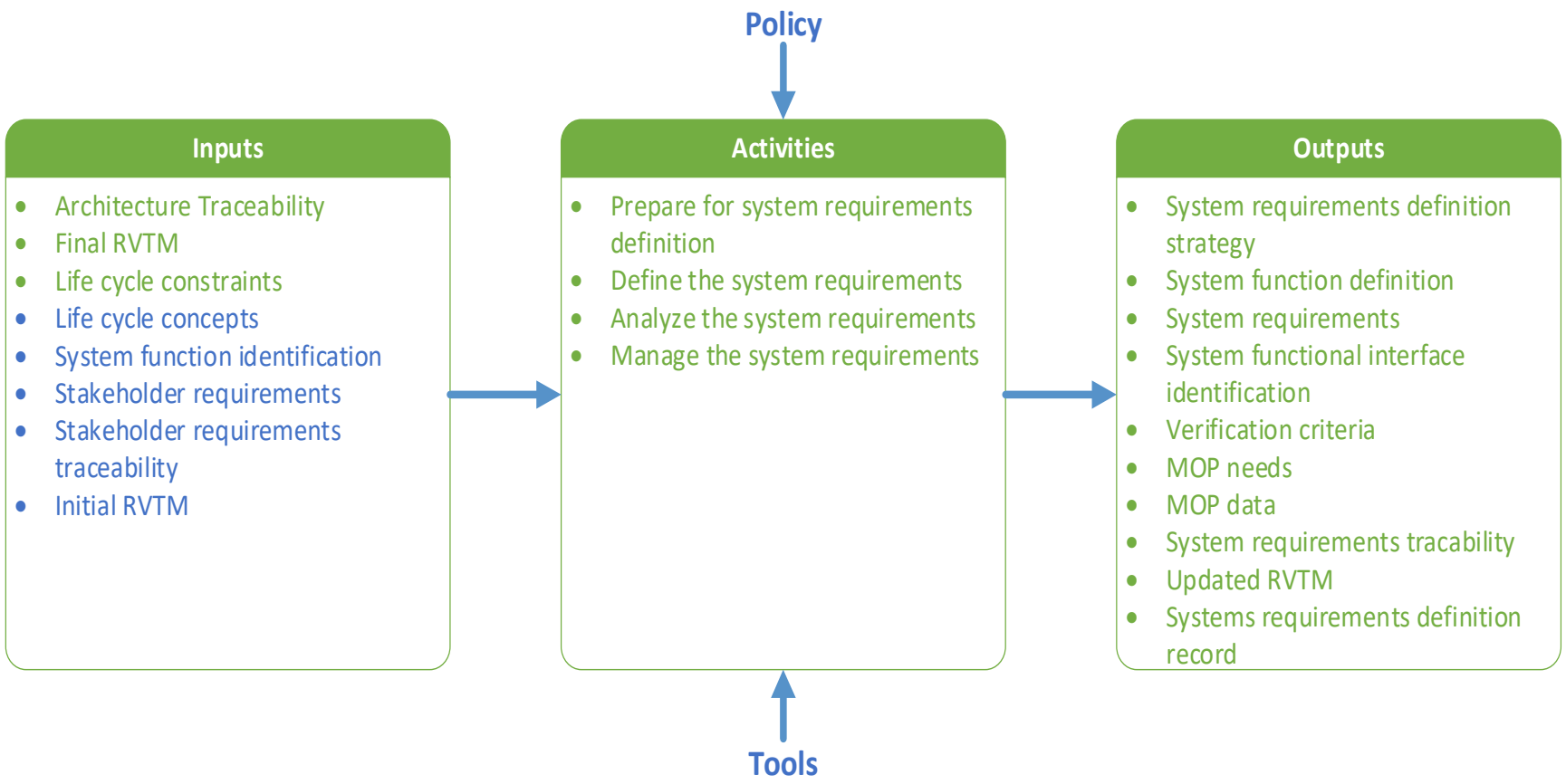
3: System Requirements Definition

- Goal: an *implementation-free* understanding of stakeholder needs
  - The what, not the how
- Seeks to specify the system's characteristics, attributes, functions, and performance to ensure the system meets the stakeholder's needs
  - Stakeholders include stakeholders of constituent systems, capability users, customers, and responding agencies

Systems Requirements Definition

- Identification of interfaces and interactions with other systems
- Identification of critical quality characteristics such as security, reliability, and supportability
- Identification of organizational limitations and constraints
- This is also the process where requirements are analyzed to identify conflicts

System Input - Process - Output



Results

- Ensures that requirements are necessary, singular, verifiable, complete, feasible, achievable, conforming, consistent, bounded, and implementation independent

- Ensures that the supplier’s perspective aligns with the user’s perspective