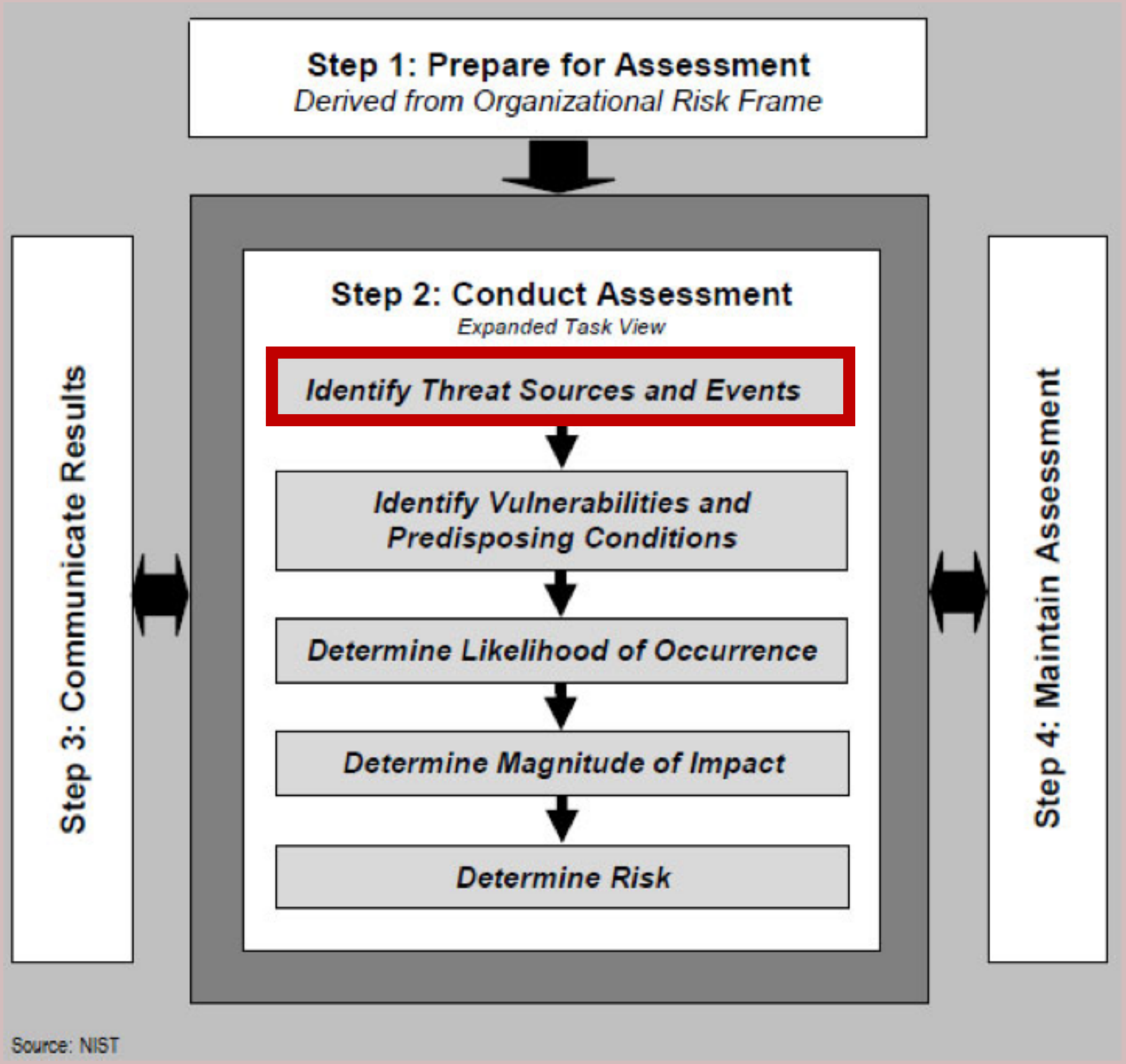
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identify Threats

THREAT MANAGEMENT

NIST SP 800-30



Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Source: NIST

Identify Threats

- Adversarial Threats
- Accidental Threats
- Structural Threats
- Environmental Threats

Adversarial Threats

- Consider their capability, intent, and likelihood

- Examples:
  - Trusted insiders
  - Competitors
  - Suppliers
  - Customers
  - Business partners
  - Nation states

Accidental Threats

- Occurs when someone makes a mistake that hurts the security of the system
- Example:
  - System administrator accidently takes servers offline causing loss of availability
  - Amazon Web Services (Feb 2017)
    - Technician utilized a SOP to take a small number of servers offline, but input the command incorrectly
    - Caused a large number of servers to go offline
    - It took down the entire US-EAST-1 region!
    - https://aws.amazon.com/message/41926/

Structural Threats

- Occurs when equipment, software, or environmental controls fail

- Example:
  - IT server fails due to hard drive failure
  - Servers fail due to overheating (HVAC fail)
  - Software failure (OS bug or crash)

Environmental Threats

- Occurs when natural or man-made disasters occur

- Example:
  - Fires
  - Flooding
  - Severe storms
  - Loss of power from the city power grid
  - Fiber or telecommunication lines cut

Always Remember…

- Threats come from both external and internal sources, but most risk assessors think of internal sources first…
- We aren’t just worried about hackers, but also the trusted insider…
- As you design security controls, don’t forget to think about disgruntled employees, inept administrators, or the insider threat!

Best Practices

- It can be helpful to get copies of a similar organization’s risk assessment to use as a baseline for your own organization

- Conduct quality assessment checks throughout the process to ensure you stay on track