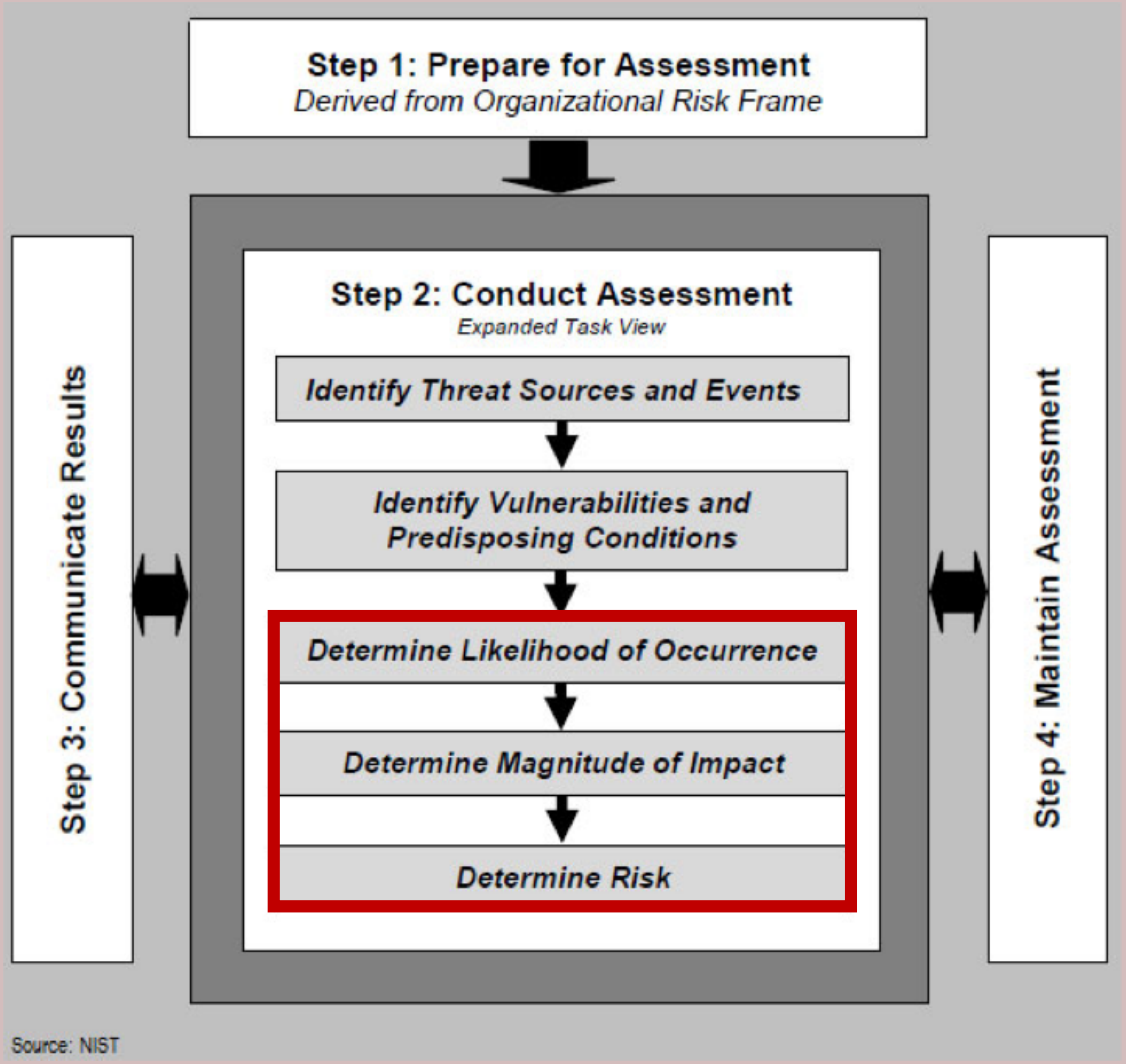
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Likelihood, Impact, and Risk

THREAT MANAGEMENT

NIST SP 800-30

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



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

Likelihood and Impact

- Measurement of the risk that the combined threat and vulnerability pose is based on the likelihood and impact
- Likelihood is the chance that the risk will be realized
- Impact is the severity of damage that occurs if the risk is realized

Likelihood Factors

- What is the likelihood that the threat will initiate the risk?
  - Example: How likely is it that the hacker attack us?
- What is the likelihood that if the risk occurs it will have a bad impact for us?
  - Example: If the organization has proper security controls, the threat may be mitigated with no adverse affects to the organization.
- Likelihood is qualitative
  - Low, Medium, High

Impact

- Always assume the threat takes place and the risk is realized when measuring
- Identify the severity of the impact
- Consider each of the pieces of CIA triad: confidentiality, integrity, and availability
- Impact is qualitative
  - Low, Medium, High

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE