Risk Assessment

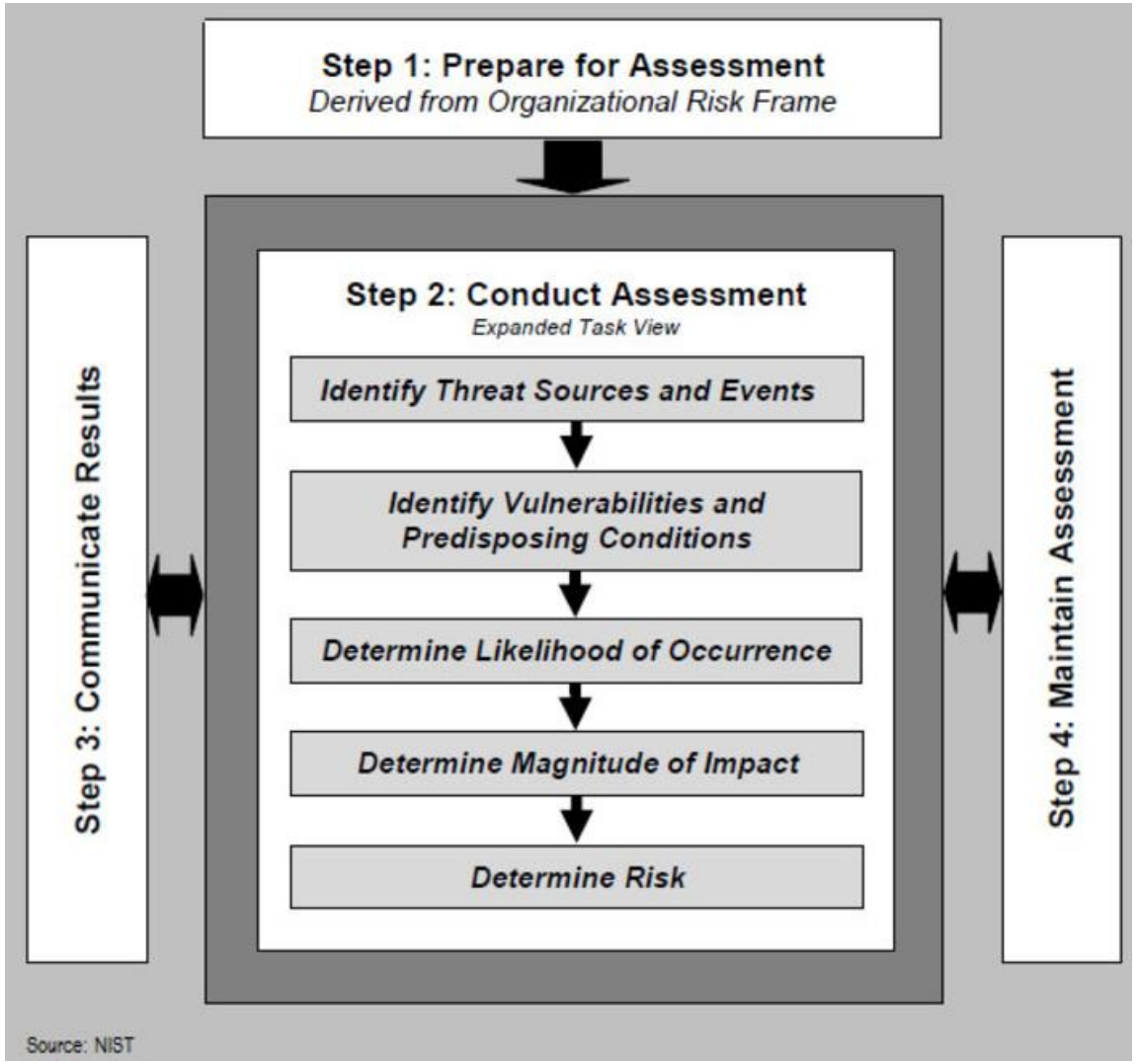
Objectives

- Understand what a risk assessment is
- Discuss approaches to risk assessment
- Understand that not all risk assessments fit into your organization

Security Management

- Risk assessment starts at the beginning of a service or system
- There are steps that need to be followed in order to ensure that the system can not only run properly, but without risk or take that risk into account
- Most organizations start risk assessment after a system or service has been running for a while. Why?

Risk Assessment Process – From NIST



Step 1: Prepare

- Identify the purpose of the assessment
- Identify the scope of the assessment
- Identify the assumptions and constraints associated with the assessment
- Identify the sources of information to be used as inputs to the assessment
- Identify the risk model and analytic approaches

Step 2 - Conduct

- Identify threat sources that are relevant to organizations
- Identify threat events that could be produced by those sources
- Identify vulnerabilities within organizations that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation
- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful
- Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events)
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.

Step 3 - Communicate

- Communicate the risk assessment results
- Share information developed in the execution of the risk assessment, to support other risk management activities.

Step 4 - Maintain

- Monitor risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors
- Update the components of risk assessments reflecting the monitoring activities carried out by organizations.

Develop your own

- Risk assessment is tough
- Developing your own assessments within your own organization should be done
- Most all of the format still should hold true
  - Define Scope
  - Conduct the analysis including likelihood and impact and risk analysis
  - Report and recommend
  - Maintain