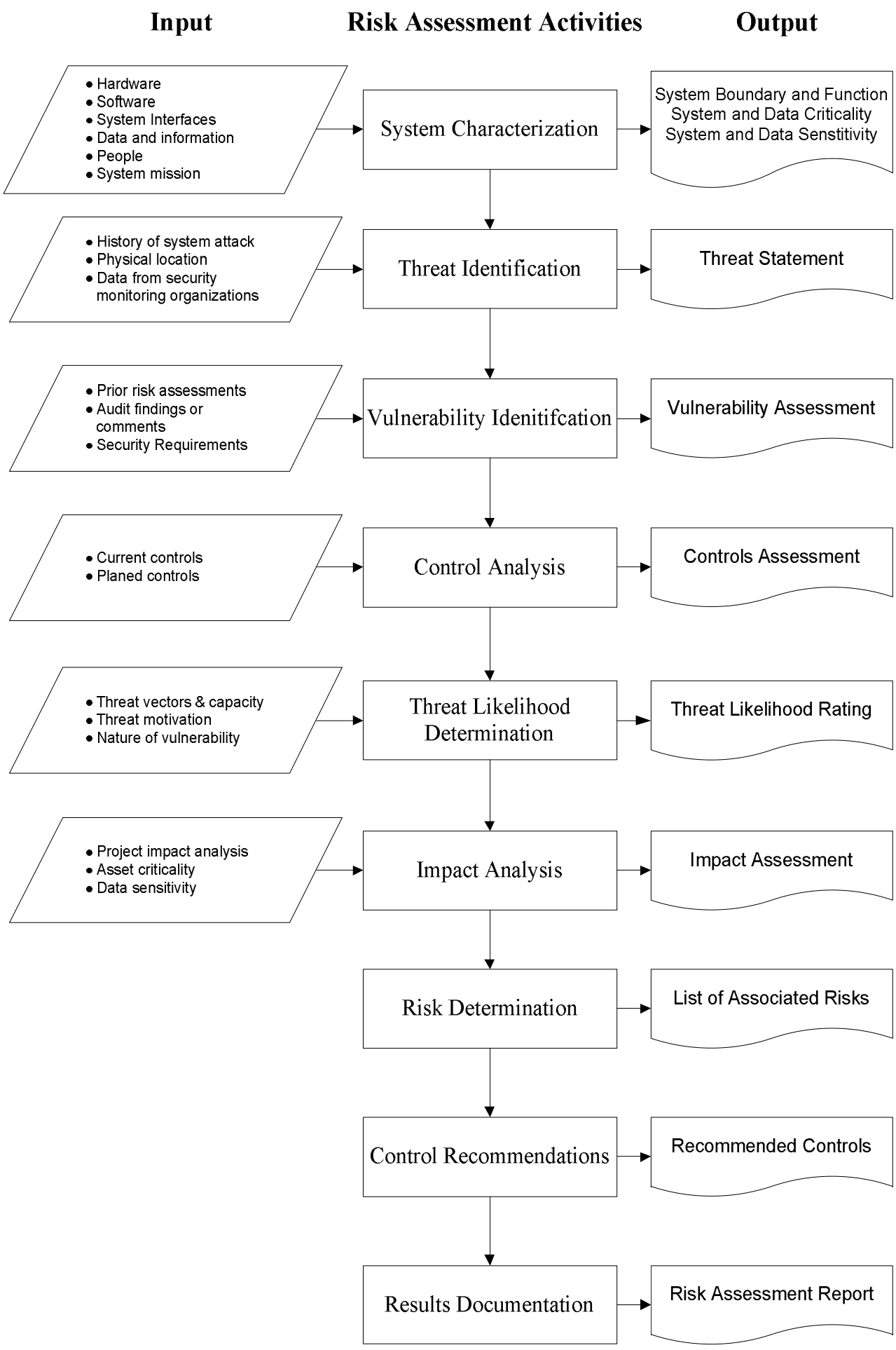
Input
Risk Assessment Activities
Output
• Hardware
• Software
• System Interfaces
• Data and information
• People
• System mission
System Characterization
System Boundary and Function
System and Data Criticality
System and Data Senstitivity
• History of system attack
• Physical location
• Data from security monitoring organizations
Threat Identification
Threat Statement
• Prior risk assessments
• Audit findings or comments
• Security Requirements
Vulnerability Idenitifcation
Vulnerability Assessment
• Current controls
• Planed controls
Control Analysis
Controls Assessment
• Threat vectors & capacity
• Threat motivation
• Nature of vulnerability
Threat Likelihood Determination
Threat Likelihood Rating
• Project impact analysis
• Asset criticality
• Data sensitivity
Impact Analysis
Impact Assessment
Risk Determination
List of Associated Risks
Control Recommendations
Recommended Controls
Results Documentation
Risk Assessment Report

SAMPLE RISK ASSESSMENT REPORT OUTLINE

Executive Summary

I. Introduction

- Purpose
- Scope of this risk assessment

Describe the system components, elements, users, field site locations (if any), and any other details about the system to be considered in the assessment.

II. Risk Assessment Approach

Briefly describe the approach used to conduct the risk assessment, such as—

- The participants (e.g., risk assessment team members)
- The technique used to gather information (e.g., the use of tools, questionnaires)
- The development and description of risk scale (e.g., a 3 x 3, 4 x 4 , or 5 x 5 risk-level matrix).

III. System Characterization

Characterize the system, including hardware (server, router, switch), software (e.g., application, operating system, protocol), system interfaces (e.g., communication link), data, and users. Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.

IV. Threat Statement

Compile and list the potential threat-sources and associated threat actions applicable to the system assessed.

V. Risk Assessment Results

List the observations (vulnerability/threat pairs). Each observation must include—

- Observation number and brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked)
- A discussion of the threat-source and vulnerability pair
- Identification of existing mitigating security controls
- Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)
- Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)
- Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)
- Recommended controls or alternative options for reducing the risk.

VI. Summary

Total the number of observations. Summarize the observations, the associated risk levels, the recommendations, and any comments in a table format to facilitate the implementation of recommended controls during the risk mitigation process.