# Risk Assessment Reports

This risk assessment report, adapted from NIST’s Special Publication 800-30, provides the essential elements of information that organizations can use to communicate the results of risk assessments. Risk assessment results provide decision makers with an understanding of the information security risk to organizational operations and assets, individuals, other organizations, or the Nation that derive from the operation and use of organizational information systems and the environments in which those systems operate.

The essential elements of information in a risk assessment can be described in three sections of the risk assessment report (or whatever vehicle is chosen by organizations to convey the results of the assessment): (i) an executive summary; (ii) the main body containing detailed risk assessment results; and (iii) supporting appendices.

Reference [NIST 800-30 Guide for Conducting Risk Assessments](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf) as you complete this report, paying special attention to [Section 2.4 Application of Risk Assessments](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf#page=26).

\*Your report should focus on either Tier 1, Tier 2 or Tier 3.

**Tip**: *Search for “Tier 1” or “Tier 2” or “Tier 3” throughout the NIST 800-30 document for references to these Tiers*.

# Executive Summary

*Include the following:*

* List the date of the risk assessment.
* Summarize the purpose of the risk assessment.
* Describe the scope of the risk assessment.
  + - For Tier 1 and Tier 2 risk assessments, identify: organizational governance structures or processes associated with the assessment (e.g., risk executive [function], budget process, acquisition process, systems engineering process, enterprise architecture, information security architecture, organizational missions/business functions, mission/business processes, information systems supporting the mission/business processes).
    - For Tier 3 risk assessments, identify: the information system name and location(s), security categorization, and information system (i.e., authorization) boundary.
* State whether this is an initial or subsequent risk assessment. If a subsequent risk assessment, describe the circumstances that prompted the update and include a reference to the previous Risk Assessment Report.
* Describe the overall level of risk (e.g., Very Low, Low, Moderate, High, or Very High).
* List the number of risks identified for each level of risk (e.g., Very Low, Low, Moderate, High, or Very High).

# Body of the Report: Part 1

*Include the following:*

* Describe the purpose of the risk assessment, including questions to be answered by the assessment. For example:
  + - How the use of a specific information technology would potentially change the risk to organizational missions/business functions if employed in information systems supporting those missions/business functions; or
    - How the risk assessment results are to be used in the context of the RMF (e.g., an initial risk assessment to be used in tailoring security control baselines and/or to guide and inform other decisions and serve as a starting point for subsequent risk assessments; subsequent risk assessment to incorporate results of security control assessments and inform authorization decisions; subsequent risk assessment to support the analysis of alternative courses of action for risk responses; subsequent risk assessment based on risk monitoring to identify new threats or vulnerabilities; subsequent risk assessments to incorporate knowledge gained from incidents or attacks).
* Identify assumptions and constraints.
* Describe risk tolerance inputs to the risk assessment (including the range of consequences to be considered).
* Identify and describe the risk model and analytic approach; provide a reference or include as an appendix, identifying risk factors, value scales, and algorithms for combining values.
* Provide a rationale for any risk-related decisions during the risk assessment process.
* Describe the uncertainties within the risk assessment process and how those uncertainties influence decisions.

# Body of the Report: Part 2

*Include the following:*

* If the risk assessment includes organizational missions/business functions, describe the missions/functions (e.g., mission/business processes supporting the missions/functions, interconnections and dependencies among related missions/business functions, and information technology that supports the missions/business functions).
* If the risk assessment includes organizational information systems, describe the systems (e.g., missions/business functions the system is supporting, information flows to/from the systems, and dependencies on other systems, shared services, or common infrastructures).
* Summarize risk assessment results (e.g., using tables or graphs), in a form that enables decision makers to quickly understand the risk (e.g., number of threat events for different combinations of likelihood and impact, the relative proportion of threat events at different risk levels).
* Identify the time frame for which the risk assessment is valid (i.e., time frame for which the assessment is intended to support decisions).
* List the risks due to adversarial threats (see [Table F-1 in Appendix F](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf#page=77)).
* List the risks due to non-adversarial threats (see [Table F-2 in Appendix F](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf#page=78)).