

D. Risk Analysis Guide

Developing a risk analysis requires the proposal writer to identify risks, define controls to mitigate the identified risks, and establish risk factors. This guide provides examples and definitions of various risks that can affect projects as well as examples of controls to mitigate them. In addition, this guide provides instructions on how to establish the likelihood and impact scores for each risk, including instructions on how to complete the corresponding risk template. Throughout this guide, the risk template, and the applications, the terms “risk control”, “risk mitigation”, and “risk management” are used interchangeably.

The narrative in this section assumes the proposal development team is requesting full acquisition funding. The table below provides the level of information required for both planning-level and acquisition-level applications. (Please note: Information technology proposals should ensure risk is addressed in accordance with requirements from the Office of Information and Technology/CIO).

Be sure to include (or attach) the risk analysis documents to your submitted capital investment 300 Acquisition application. A completed risk template will provide the following data.

Deliverable	Planning Applications	Acquisition Applications
Risk Score	Preliminary assessment of risk level for each risk category	Comprehensive assessment of impact and likelihood of occurrence for each risk category (include risk template worksheets and summary sheet)
Risk Analysis	Preliminary description of likely risks for each risk category	Completed risk template – comprehensive assessment of risks
Risk Control Plan	Not required	Completed risk template – comprehensive assessment of risk mitigation activities and internal resources

Background

Risk is an inherent part of any capital investment. Project risk, left unattended can be costly but substantially reduced if understood and controlled. Identifying all of the risk components that are inherent in projects during the proposal development stage can have a significant impact on the project's overall success. There are ten significant risk components identified in this guide: Organization and Change Management; Business; Data/Information; Privacy; Technology; Strategic; Security; Project Resources (Financial, FTE); Project Schedule; and Legal/Contractual. By identifying all known risks, developing a plan to mitigate and control them, the project will have a greater chance for success.

Risk Evaluation Process

The risk evaluation process is composed of three steps: identifying and scoring risks; rationalization; and control. The first step in the process is the identification and scoring of the project risks; the risk template serves as the guide. Each identified risk needs to be scored based upon an assessment of likelihood and impact. The end result of this step is a risk score for both the proposal and each of the individual risks.

Once the risks have been identified and scored, the second step is rationalization. This step is evaluated as the Quality of Risk Analysis criterion of the Capital Investment Decision Criteria model for the 300 Acquisition applications. This step provides an opportunity for the proposal team to define their justifications and conclusions regarding each individual risk.

The final step is establishing a control plan to mitigate associated risks. This step is evaluated as the Quality of the Risk Control Plan criterion of the Capital Investment Decision Criteria model. This step requires the proposal team to determine risk controls based upon their available resources and identify responsible parties.

These steps, combined deliver a complete project risk assessment, providing an overview of anticipated project risks. This guide presents the tools needed to accomplish this task, including a risk template and examples of risk controls.

It is important to note that not all risks apply to all investments, and the analyst must determine which risks apply on a case-by-case basis.

Identify and Score Risks

The ten areas of risk to analyze when determining the overall risk score of a project are:

1. Organization and Change Management
2. Business
3. Data/Information
4. Privacy
5. Technology
6. Strategic
7. Security
8. Project Resources (Financial/FTE)
9. Schedule
10. Legal and Contractual

The overall assessment of the risk of project failure is presented by the total risk score.

1. Organization and Change Management Risk

Organizational risk is determined by key stakeholders within the organization and their view of the proposed alternative. Organizational risk can be determined by, but is not limited to:

- Redistribution of power – the single greatest element that will increase organizational risk.

The greater the number of stakeholders from whom you can achieve buy-in for an investment (from the top management to the users), the lower the organizational risk.

2. Business Risk

Business risk is the degree to which a proposed project alternative solves business problems or takes advantage of business opportunities. Will the proposal do what it is expected to do? The business case for any project can be enhanced if it can be linked to the overall strategic plan or the information management plan at the Administration or field level. Include information about how the proposed alternative will affect organizational structures and procedures. Alternatives with broader impacts on existing organizational structures or procedures are more risky than those with lesser or more narrow impacts. Be clear about how the alternative will fit into the day-to-day operations.

The business risk also addresses the risk posed by the inability of the proposal to accurately predict the lifecycle of projects. Problems can result from the failure to attain expected benefits from the project, inaccurate project cost estimates,

inaccurate project duration estimates, failure to achieve adequate system performance levels, failure to adequately integrate a new system with existing hardware and software or failure to integrate organizational procedures or processes.

In addition to those business risks listed above assess the feasibility of the project, the reliability of systems, the risk of creating a monopoly for future procurements, and the capability of the Department to manage the project.

3. Data/Information Risk (applies to Information Technology Investments)

Data/Information risk quantifies the level that is inherent in the source/location of the data/information and/or from where it originates. Information and data required to successfully operate a new or improved information technology asset is often easily comprehended, located, analyzed, and cleanly imported to the new systems with minimal problems or issues. However, some complicated systems that must rely on data/information sources (external and internal) are difficult to retrieve. This variance is what is measured with more risk. It is necessary to assess the differences in risk between the alternatives and the existing operations. It is primarily associated with IT investments. Like data/information risk, it is measured by its level of presence. Does the investment comply with the Department's Architecture Enterprise IT platforms or must it be modified to be successful? That level of success or failure is what is quantified and measured.

4. Privacy Risk

Privacy risk is normally associated with protecting the personal rights of individuals and organizations from unwanted or unwarranted data or information release. Individuals and organizations have an inherent expectation that their personal and private information captured in databases or records will be kept private.

Examples of data contained in databases or processed for specific purposes are:

- Medical records
- Photos
- Personal background information
- Graphics or medical pictures
- Financial records
- Benefits records

Examples of uses of data from individuals or organizations are:

- Medical research
- Personnel actions

- Financial reporting
- Benefits delivery
- Verification of burial eligibility

Information that must remain private may be transferred and collected online through the Internet, Intranet, or wireless transmission or by personal interviews.

Other examples of risk in privacy are the capture of "cookies" and other automatically directed activities related to computer use to track personal preferences and habits.

The level of risk for privacy is measured in the ability for the proposed investment to ensure that privacy will remain intact throughout the life of the investment and information is not shared.

5. Technology Risk

Technology risk measures the state of the investments capacity to remain relevant in the future. It is the measurable level of risk that improvements in affected technology will overcome the investment. Technical risk can be determined by four primary factors:

1. Project Size

- Number of members on the project team
- Project duration
- Number of organizational departments involved in project
- Size of programming or construction effort (e.g. hours)

2. Project Structure

- New system, construction or renovation of existing system(s)/buildings
- Organizational, procedural, structural, or personnel changes resulting from the system
- User perceptions and willingness to participate in effort
- Management commitment to project
- Amount of user information in project development effort

3. Project team's experience with technology or business area

- Familiarity with proposed business or application area
- Familiarity with target-hardware, software development environment, tools, and operating system or familiarity with construction process
- Familiarity with building similar systems or buildings of similar size

4. User group's experience with development projects

- Familiarity with information systems development process or construction development process
- Familiarity with proposed application or business area
- Familiarity with similar systems or projects

6. Strategic Risk

Strategic risk is the measurement of the alternative against the strategic plan of the agency. Is there a risk that the investment relies on potentially evolving or changing strategic missions? If so, then there is more risk for the investment. If the investment is based on the Department's core strategic missions, such as caring for veterans, then the risk should be slight that there will be a change. Investments that are impacted by changing strategic missions may be more risky, and conversely, investments that are needed for core Department missions will have less risk.

In addition to other strategic risk defined for this project discuss the risk of dependencies and interoperability issues between this project and others.

7. Security Risk

Security risk assesses the amount of confidence that the investment will not be compromised by external threats.

The security risk would be considered high if the alternative failed to incorporate a security plan that discusses technical controls for the system, methods for identifying, appropriately limiting, and controlling interconnections with other systems, procedures for the on-going monitoring of the effectiveness of security controls, and provisions for the continuity of support in the event of system disruption or failure.

Security risks related to facilities should also be considered in relation to efforts to protect homeland security.

8. Project Resources Risk (Financial/FTE)

Financial risks are any risks that could ultimately cause VA to pay out unexpected monies. These risks are usually thought of in dollar amounts when considering the impact variable. Financial risk can result from, but are not limited to:

- Cost overruns (for the initial acquisition and life cycle costs)
- Legal disputes
- Lost information/data
- Hardware or software failure and replacement
- Reliance upon a single vendor without cost controls

9. Schedule Risk

Schedule risk is the degree to which the expected time frame and completion dates for all major activities within a project meet organizational deadlines and constraints for effecting change. Concerns might include, but are not limited to:

- Governmental regulation deadlines
- Resource availability within time frame

Consider scheduling trade-offs, outsourcing, or altering the technical development environment.

10. Legal & Contractual Risks

Legal and Contractual risks refer to the project ramifications that result from the construction of a building, purchase of a machine or service, or development of an information system. Risks may include, but are not limited to:

- Copyright infringements
- Non-disclosure
- Labor laws
- Anti-trust (limiting information sharing)
- Foreign trade regulations (limiting encryption techniques)
- Malpractice
- Inadequate building standards
- Financial reporting standards
- Software ownership in joint ventures
- License agreements
- Non-disclosure with partner
- Involvement of outside organizations

Developing Risk Control Plans

One cannot discuss risk without also discussing controls. Controls are those procedures or activities put into place that mitigate (or minimize) risks. Rarely can risk be eliminated; however, it can be controlled. If these controls are in place in a project plan, then the likelihood of risk decreases and the alternative becomes more attractive. It is important to note that not all risks apply to all investments and the analyst must determine which risks apply on a case-by-case basis. Listed below are some generic risk mitigation strategies for each of the ten risk categories that the analyst may use to decrease the likelihood of risk occurrence.

1. Organization and Change Management Controls

Organizational Controls

- Obtain buy-in from top management very early on in planning stages
- Work closely with end-users to establish requirements for new system
- Improve communication

Change Management Controls

- Use a strategic information management framework
- Establish clear requirements and objectives
- Use a change management program to minimize organizational disruption
- Adequately train and provide follow on support
- Establish performance metrics and reporting system to monitor those metrics

2. Business Controls

- Ensure all components of the life cycle analysis are in place and have been thoroughly reviewed for accuracy
- Determine if expected benefits have changed since the proposal was developed
- Ensure the investment will comply with existing or known future changes to the systems requirements/architecture/specifications
- Carefully recheck project estimates to ensure they are up-to-date at time of proposal submission
- Provide a comprehensible and functional description of how the proposal is intertwined into the operation of the organization

3. Data/Info Controls (Information Technology Proposals)

- When data is required from external/internal sources, complete a verification process that ensures access to data is available and the compatibility between data/information sources and the proposal is reliable
- Ensure that all data/information required for the system to operate effectively and efficiently is consistent and accurate
- When data/information must be obtained from external sources, ensure that top management from all organizations that provide and/or use data/information, approve in writing, the data/info transfer
- Complete a study that addresses all costs associated with data/information transfer and ensure agreement by all parties

4. Privacy Controls

- Ensure personal and private information capture in databases or records are private when transferred and collected on-line through the Internet, Intranet, or wireless transmission or by personal interviews
- Ensure that privacy will remain intact throughout the life of the investment, and data are not shared

5. Technology Controls

- Use development lifecycle methodology/structure
- Use project planning/management software
- Use appropriately trained personnel
- Break the project into increments
- Isolate custom design portions of the project
- Assign project manager to be accountable for the project

6. Strategic Controls

- Conduct a review that addresses the strategic plan and ensures that just prior to submitting the proposal every effort was made to match all requirements of the proposal with VA's strategic plan
- Address any differences between the strategic plan and the proposal
- Ensure the proposal is fully linked to and complies with the Department's and Administration's strategic plan and objectives;

7. Security Controls

- Identify any security weaknesses and known threats by conducting a security analysis
- Determine the source and depth of the risk or threat, and methods to mitigate the risk
- Security controls may also consist of physical barriers and equipment that protects personnel, services, space and equipment from threats. Proposals must identify all necessary steps to mitigate or eliminate threats to facilities
- Information Technology systems may require a security control back-up plan in the event a system is disabled due to a web-based intrusion or system compromise

8. Project Resources (Financial/FTE) Controls

- Perform cost-benefit and economic analyses
- Implement a rigorous investment management program
- Utilize Earned Value methodology during project lifecycle to control costs
- Purchase liability insurance or bond by contractor
- Establish clear benefits to be realized
- Use competitive bidding for each increment of project design
- Implement an investment review board

9. Schedule Controls

- Use contractual penalties for missed deadlines
- Use project management software
- Set realistic expectations and manage those expectations
- Use outsourcing to augment scarce internal resources

10. Legal and Contractual Controls

- Create a software license management program
- Review all applicable laws
- Keep contracting personnel apprised of potential legal concerns and possible contract disputes
- Maintain good communication with contracting personnel to ensure minimal opportunity for contract dispute
- Provide multiple opportunities within a contract for termination

Scoring Impact and Likelihood

Once risks and controls have been identified, it is important to determine the level of impact and likelihood of those risks on a given project. Examining the impact and likelihood will result in a risk factor, which can be applied to each risk that was originally identified.

First, determine the impact that a particular risk would have on the project if it were realized. This rating will occur on a scale of 1 through 3, with 1 implying minimal impact and 3 implying the most catastrophic impact. Second, determine the likelihood of risk occurrence. While the impact of a particular risk may be high, the likelihood of it taking place may be minimal. Use a probability of impact where 1 indicates minimal likelihood of occurrence and 3 indicates a certainty of occurrence. Finally, multiply the two together to arrive at a risk factor for each risk identified:

(Impact x Likelihood) = Risk Factor

For example, the construction of a clinic is very important for meeting the needs of a growing segment of veterans in the market area. It is estimated that the clinic will require 19 months to complete. Construction will begin in June 2002. To determine the Schedule Risk, the impact and likelihood must be determined for that individual risk. If VA fails to complete the hospital by June 1, 2004, the impact will be significant. You might assign it a medium level risk, or a 2 on a scale of 1 to 3. However, the risk of the project going beyond the deadline is small since you have a 19-month project with 24 months to complete. Therefore, you might assign a likelihood rating to Schedule Risk of low level risk, or a 1 on a scale of 1 to 3. Calculating your Risk Factor yields a 2 (e.g., Impact of 1 multiplied by Likelihood of 2 equals 2).

Using this same scale across all identified risks to an alternative, and subsequently summing all risk factors will provide the analyst with a final Risk Rating for a particular project alternative. Taking the risk rating and dividing by the number of identified risks yields a Risk Score. The risk score will be used to determine the level of impact risk has on the proposed project. Given that the scale will vary from project to project, risk scores will be placed in a Low, Medium, or High effect category, where:

Low is for Risk Scores between 1 and 3

Medium is for Risk Scores between 4 and 6

High is for Risk Scores between 7 and 9

For example:

Identified Risks	Likelihood	Impact	Risk Factor
Cost overruns	2	2	4
Unfamiliar with similar systems	1	2	2
Limited resources	1	1	1

Risk Rating (sum of risk factors) = 7

Risk score (risk rating divided by the number of risks) or $7/3 = 2.33$

The use of the risk score has two benefits. The first is that it encourages users to include all identified risks. Using only the risk rating would discourage this practice since the higher the score, the higher the penalty. The second benefit is a more accurate overall picture of the project risk. Several low impact, low likelihood risks are far less dangerous than a single high impact, high likelihood risk. This will be captured in the risk score.

Even if the proposal yields a high risk score, it does not mean that the proposal will be rejected. Rather, in many cases high-risk proposals yield the highest returns. This type of consideration is in line with VA's current effort in moving towards portfolio management where proposals with varying levels of risk could be selected given that they should produce higher returns. (**Note:** After

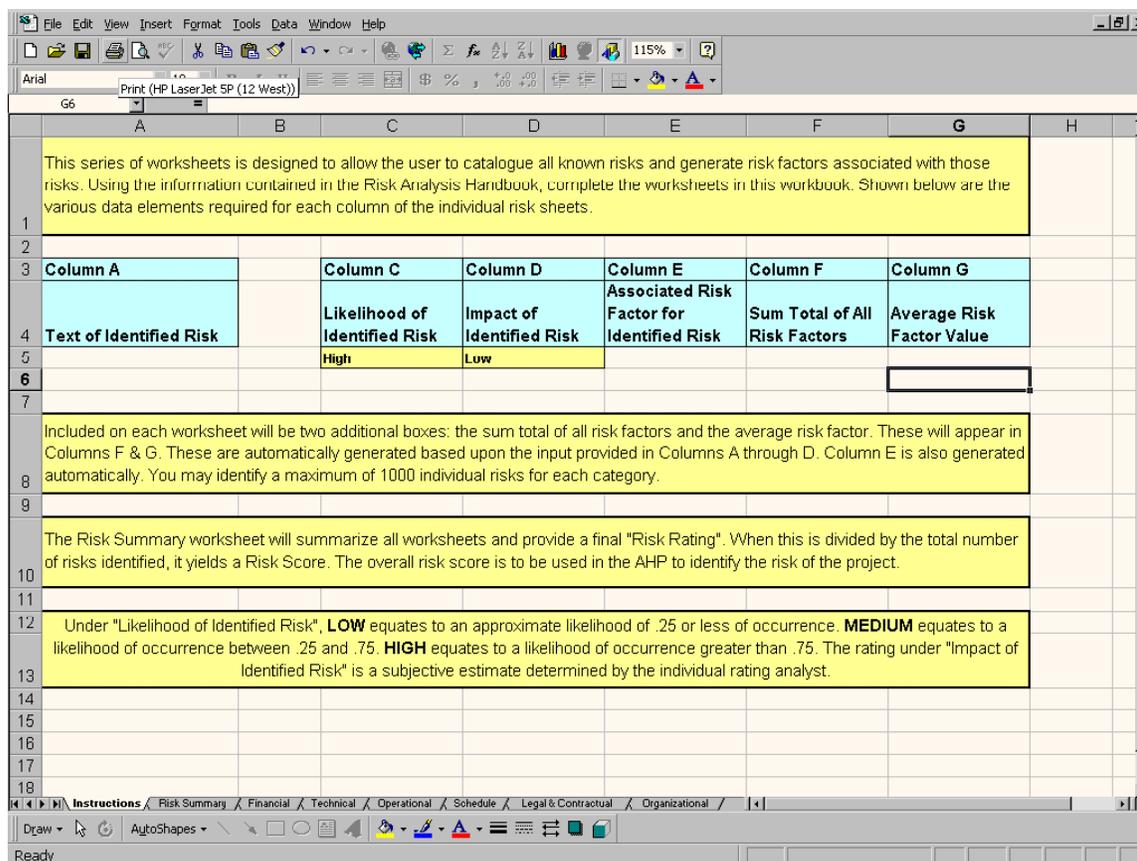
completing the template and deriving the results, be sure to print a copy of the risk summary sheet and all risk category worksheets, and attach them to the application. Input the results in the appropriate section of the application.)

Complete the Template

The accompanying Microsoft Excel® workbook (Risk Analysis Template.xls) provides a tool in which to catalogue and score risk. The workbook contains twelve separate worksheets: an instruction sheet; a risk summary sheet; and ten individual risk category sheets. Below is a description of what you will find in each worksheet.

Instruction Sheet

This worksheet provides a brief overview of the Risk Analysis workbook. Columns are identified and terms are explained. No inputs are required on this worksheet.



To operate the buttons to clear sheets change the security (under tools, macros, in excel) from high to medium, then save the sheet, close it, then reopen. Otherwise the button will not operate. You will know it works when you open the file and it prompts you to enable macros.

Risk Summary Sheet

This worksheet is a self-generating summary of the proposal's risk ratings and risk scores for each risk category as well as the overall scores for the alternative. No data should be entered directly in this worksheet. The total risk score is the number that is of concern to the evaluator. The total risk score is the data element used when comparing the risk level of the chosen alternative to all other proposal alternatives.

Risk Category Worksheets

These worksheets are where information is entered for analysis. There is one worksheet for each of the ten risk categories. Each of the risk category worksheets has the same column headings. The information to be provided is as follows:

- Column A** Identify the individual risks associated with the particular category. **Input a textual description** of the risk in this column. For example, under Technical Risks, one identified risk could be "difficulties integrating systems that are not supported by current architecture".
- Column C** **Input the likelihood of occurrence** for the identified risk. Use the drop down menu to choose: **High** (probability of .75 to 1.00); **Medium** (probability of .25 to .75); or **Low** (probability of 0 to .25).
- Column D** **Input the impact** of the risk on the project if it is realized. Use the drop down menu to choose: **High** (significant impact); **Medium** (moderate impact); or **Low** (very little impact).
- Column E** This column is **automatically generated**. The number appearing here is the **individual risk factor** for the risk, and is a factor of columns C and D.
- Column F** This box is **automatically generated**. It is the **risk rating** and is found by summing the individual risk factors for the entire risk category.
- Column G** This box is **automatically generated**. It is the **risk score** for the category and is found by dividing the risk rating (Column F) by the total number of risks identified within the category.

Before printing, remember to set your print area otherwise you will print several hundred pages.

Evaluating the Risk Analysis

Proposals will be evaluated on the two sub-criteria under Risk listed in the FY 2005 Capital Investment Decision Hierarchy:

Quality of Risk Analysis: This sub-criterion will be evaluated on whether the proposal team identified all potential risks associated with a given alternative and gave reasonable impact and likelihood scores to them. If all risks have been identified and the ratings are reasonable, then the proposal has the best chance of receiving the highest score for this area. However, if the reviewer can identify risks that the proposal team did not, or feels that impact and likelihood score are not reasonable, then the evaluation will decrease.

Quality of the Risk Control Plan: This sub-criterion will be evaluated on the quality of the risk control plan. A good plan identifies actions that project managers will take to minimize identified risks (risk controls), resources the Department has internally to mitigate the risk, and the individual responsible for initiating those actions and resources. In addition, a good risk control plan notes the data that a specific risk was identified and is updated with the current status of that risk. It further identifies the project variance (e.g., 10% cost or schedule overruns) that will initiate corrective action. These variances may be cost overruns, schedule overruns, etc. Developing control plans can counter the negative impact that risks may have on the project. Consequently, proposal teams *should present feasible control plans, which can improve the overall Risk criterion score.*