APPENDIX F—RISK ASSESSMENT

PURPOSE

Risk is part of any capital investment. Identifying and controlling risks during the Select Phase can have a significant impact on the investment's overall success. However, risk is not the only consideration for investment evaluations. Investments with high technical risk may be selected if the investment is deemed a strategic or operational necessity. Other investments may be selected simply because they have low risk and require few resources. Conducting a risk assessment and controlling risk is a continuing process throughout the investment lifecycle.

F.2 PROCESS

The risk evaluation process is composed of three steps:

1. Identify risks
2. Analyze risks
3. Control risks.

Each of these steps is detailed in the following sections.

1. Identify Risks

Risk identification consists of determining and documenting risks that will likely have an impact on the investment. The identification and associated analysis is a continuing process that should be done periodically throughout the investment lifecycle. Both internal and external risks should be identified. Internal risks are those that can be directly controlled within the project. There are several mechanisms available to assist in identifying risk areas that include historical information, work breakdown structure (WBS), project plans, risk checklist, and interviews. The following checklist is provided to assist in the risk identification. Risk assessments for all investments must include:

1. Schedule (i.e., the degree to which the expected completion dates for all major investment activities meet organizational deadlines and constraints for effecting change);
2. Initial costs (i.e., the feasibility of being able to provide the initial funding outlay);
3. Life-cycle costs (i.e., the confidence the stakeholders have in the accuracy of the life-cycle costs and ROI);
4. Technical obsolescence (i.e., the likelihood that the technology supporting the investment will be made obsolete by follow-on technology);
5. Feasibility (i.e., the overall likelihood of the investment succeeding);
6. Reliability of systems (i.e., the degree to which users depend upon the systems);
7. Dependencies and interoperability between this investment and others;
8. Surety (asset protection) considerations (i.e., the level to which the investment assets are protected from loss);
9. Risk of creating a monopoly for future procurements (i.e., the probability that government action will give a contactor an unanticipated economic advantage over competitors in the future);
10. Capability of agency to manage the investment (i.e., the extent to which a the agency has successfully managed similar investments in the past);
11. Overall risk of investment failure (i.e., the chance that the investment will fail completely);
12. Organizational and change management (i.e., risks associated with key stakeholders and their view of the investment);

13. Business (i.e., the degree to which a proposed investment solves business problems or takes advantage of business opportunities);
14. Data/info (i.e., the type, importance, and sensitivity of the data being collected);
15. Technology (i.e., the type, maturity, user-level acceptance, and pervasiveness of the underlying technology expected to be used);
16. Strategic (i.e., the long-term importance of the investment to the sponsoring organization);
17. Security (i.e., the potential impact of an underlying system being compromised);
18. Privacy (i.e., the extent to which data will be used that can individually identify people); and
19. Project resources (i.e., the level and type of resources expected to be employed on the underlying project).

2. Analyze Risks

Each risk is analyzed based on an assessment of likelihood and impact. Numerous activities are used to analyze risks and obtain a complete risk assessment to aid in developing risk management and control strategies. The following provides a summary of activities to assist in risk analysis:

- Group similar and related risks into categories. This will assist in identifying related risks as well as identifying potential dependencies between risks.
- Determine risk drivers or variables that affect the probability and impact of identified risks.
- Determine the root cause or source of risk.
- Use risk analysis techniques and tools such as simulation or decision trees to assess trade-offs, interdependencies, and timing of identified risks.
- Estimate risk factor or risk exposure. Multiply probability of occurrence or likelihood with the consequence or impact (in financial terms) if the risk occurred.
- Determine risk severity. Risk severity is determined by assessing the risk factor with the relative risk timeframe for action. This provides a means to assist in prioritizing risks to better focus control strategies.
- Rank and prioritize risks.

In addition to prioritized risks, a primary output of the risk analysis is an overall “risk factor” that can be applied to each risk. To calculate the risk factor, determine the impact a particular risk (in financial terms) will have on the investment if it is realized, and the likelihood (probability in percentage terms) of this risk occurring. Then multiply these two numbers together. Calculate the risk factor for each identified investment risk and sum the risk factors to determine an overall risk rating for the investment. The overall risk rating should reflect the risk-adjusted ROI for the investment (see Appendix E: Cost-Benefit Analysis for a discussion on ROI and risk adjustment.)

To aid comparisons across investments, it is useful to also calculate a risk score. This is computed by dividing the investment’s overall risk rating by the number of identified risks. This encourages Project Managers to include all identified risks and provides a more accurate picture of the overall investment risk. For example, several low -impact, low -likelihood risks may be less risky than a single high-impact, high-likelihood risk.

The Risk Assessment Plan, submitted as part of the Select and Control Phases should, at a minimum, have the columns shown in Table F-1.

Table F-1 Example of Risk Assessment Table

Risk Categories	Description	Probability of Risk Occurrence (1)	Risk Impact (2)	Risk Factor (3)	Risk Prioritization (4)	Cost of Risk (5)	Adjusted Risk Cost (6)
1 – Schedule	Delays in acquisition process.	Low (35%)	Low	Low	3	$$$ ($2500)	$$$ ($875)
2 - Initial Costs	Funding shortfalls	Low	Low	Low	3	$$$	$$$
3 - Life-Cycle Costs	Costs may exceed original estimates	Low	Low	Low	3	$$$	$$$
4 - Technical Obsolescence	Aging system(s) will be unable to provide utilities at reasonable cost compared to newer technology.	Low	Low	Low	3	$$$	$$$
5 - Feasibility	System(s) will be unable to provide necessary utility due to technical limitations	Low	Moderate	Low	2	$$$	$$$
6 - Reliability of Systems	System downtime reduces available computational cycles	Low	Low	Low	3	$$$	$$$
7- Dependencies and Interoperability Between This and Other Investments	System or its products will be unable to interact with other extant systems.	Low	Low	Low	3	$$$	$$$
8 - Surety (Asset Protection) Considerations	Loss of system productivity due to accident, abuse, or malicious intent	Low	Low	Low	3	$$$	$$$
9 - Risk of Creating a Monopoly For Future Procurements	Continued selection of one vendor stifles competition	Low	Low	Low	3	$$$	$$$
10 - Capability of Agency to Manage the Investment	Inadequate resources to monitor system, contract performance.	Low	Low	Low	3	$$$	$$$
11 - Overall Risk of Investment Failure	System fails to provide required capabilities.	Low	Moderate	Low	3	$$$	$$$

Risk Categories	Description	Probability of Risk Occurrence (1)	Risk Impact (2)	Risk Factor (3)	Risk Prioritization (4)	Cost of Risk (5)	Adjusted Risk Cost (6)
12 - Organizational and Change Management	Potential rejection by operating unit personnel; possible discontinuance due to personnel loss.	Low	Low	Low	3	$$$	$$$
13 - Business	Possible vendor default or contract non-performance.	Low	Low	Low	3	$$$	$$$
14 - Data/Info	Data loss	Low	Moderate	Low	3	$$$	$$$
15 - Technology	Acquisition of inappropriate hardware/software solution.	Low	Low	Low	3	$$$	$$$
16 - Strategic	Changing business requirements	Low	Low	Low	3	$$$	$$$
17 – Security	Lack of system confidentiality, integrity, or availability.	Moderate (65%)	Low	Low	3	$$$ ($2500)	$$$ ($1625)
18 - Privacy	Unauthorized person(s) could access systems and personal information.	Low	Moderate	Low	2	$$$	$$$
19 - Project Resources	Reduction in funding	Low	Low	Low	3	$$$	$$$

(1) For Probability the following scale may be used:
- High Impact from 66% to 100%
- Moderate Impact from 36% to 65%
- Low Impact from Less than 35%

(2) For Risk Impact the following scale may be used:
- High Impact from 66% to 100%
- Moderate Impact from 36% to 65%
- Low Impact from Less than 35%

(3) Risk Factor = Risk Probability x Risk Impact

(4) Risk Prioritization: The overall rating Risk Priority is defined as follows:
1 = High Impact from 66% to 99%
2 = Moderate Impact from 35% to 65%
3 = Low Impact from less than 35%
Risk Prioritization is ranked based on how risk impacts to the project.

(5) Cost of Risk: Most risks have a cost associated to them. The cost of risk relates to the financial setbacks that would be encountered as a result of the risk. The figures for calculation in the table below

are the mean amounts of the range for each cost level. For example, the figure used for cost level "B" is $15,000, the mean of the $5,000 and $25,000 bounds of the range for that level.

Category	Range	Figure for Calculation
A	Less than $5,000	$2,500
B	$5,000 to <$25,000	$15,000
C	$25,000 to <$100,000	$62,500
D	$100,000 to <$2.5 Million	$1.3 Million
E	$2.5 to <$5 Million	$3.75 Million

(6) Risk adjusted cost is measured by multiplying each risk cost (in dollars) by the percentage probability of the risk's occurrence.

---

3. Control Risks

To successfully control risk, the Project Manager must establish and execute a risk management plan in which the development of a risk response strategy of Mitigation, Acceptance, Avoidance or Transference and a risk response plan are needed to manage and mitigate the risks identified.

- Risk Acceptance: establishes the contingency plan to be implemented if the risk occurs and the allocation of time and cost reserves to the project or leaves the action to be determined as needed.
- Risk Avoidance: eliminates the threat by eliminating the cause.
- Risk Transference: shares responsibility for the risk through contract terms, subcontracts high-risk tasks or outsources the work.
- Risk Mitigation: develops and executes a mitigation plan to eliminate or minimize probability of occurrence and impact.

The Risk Management Plan includes determining risk controls based upon available resources and identifying responsible parties. The plan should include the identification of the appropriate risk control strategy, objectives, alternatives, mitigation approach, responsible parties, resources required, activities, actions taken to date, and results achieved. The risk management plan is an evolving strategy to assist the Project Manager and ensure a higher probability of success for the investment. The plan should be updated continually as risks change throughout the lifecycle. Risks, actions taken, and results should be tracked and included as part of periodic reviews.

Risks can rarely be completely eliminated, however they can be controlled. If the following controls or risk mitigation strategies are in place, the likelihood of risk decreases and the investment is more attractive:

Financial Controls

- Perform Cost-Benefit and economic analyses
- Implement a rigorous investment management program
- Utilize earned value, share in savings, use contracting approaches, etc. to help control costs
- Purchase liability insurance
- Establish clear benefits to be realized
- Use competitive bidding for each investment design increment.

- Technical Controls
- Reengineer the process first

- Use development lifecycle methodology/ structure
- Use project planning/management software
- Use appropriately trained personnel
- Divide the investment into increments
- Isolate custom design portions of the investment
- Assign a Project Manager (preferably with Project Management Institute or similar organization certification) to be accountable for the investment
- Conduct an IV&V
- Conduct pilot test(s).

Operational Controls

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

Schedule Controls

- Use contractual incentives for quality or timeliness
- Use contractual penalties for missed deadlines
- Use contractual incentives for meeting or beating deadlines
- Use project management software
- Use an experienced/certified Project Manager and/or provide the necessary training to the Project Manager
- Set realistic expectations and manage those expectations
- Use outsourcing to augment scarce internal resources.

Legal and Contractual Controls

- Create a software license management program
- Review all applicable laws
- Apprise contracting personnel of potential legal concerns and contract disputes
- Maintain communication with contractors to minimize contract disputes
- Provide multiple termination opportunities within a contract.

Organizational Controls

- Obtain “buy-in” from top management early in planning stages
- Work closely with end-users to establish system requirements
- Maintain good communication with all stakeholders.