Risk Analysis Framework for Service Contracts

Version 1.1

(Released January 2020)

This guide is designed for both program and project managers, as well as the upper management to whom they report. Procurement staff is encouraged to distribute this guide to appropriate staff at the beginning of acquisition planning. Procurement staff should also share this document with agency legal counsel and use it as a training resource.

This document does not create a binding procedure or create rights or obligations for or against the State.

This guide has been tailored for use in procurements conducted by the Division of Procurement Services.

Basic Framework for Analyzing Risks Associated with Contracting for Services

As with any undertaking, contracts for services contain risks. Some risks are trivial and may be ignored; others are so catastrophic that they may cause a party to demand expensive concessions or back out of a proposed deal. But typically the risks are *manageable* with enough foresight, planning, and careful negotiation. So how do you determine the degree of risk, and whether that risk may be tolerated, managed, or avoided altogether?

Identifying the Risk

The first step is to identify the risk. Almost every contract will have a few common risks. These include the risk of a vendor's delayed, inadequate, or non-performance; an agency's failure to cooperate; or poor contract administration, such as an unintentional waiver of rights or a failure to give some contractually required notice. Unfortunately, not all risks are so obvious. Some contracts have hidden traps that can spring with unintended and unforeseeable consequences.

Take, for example, a contract to host patient health information. When that information is hosted on the contractor's computers, it is easy to identify the risk of lost confidentiality if someone hacks the computer. But what happens if the hacker disrupts the agency's access to that computer? For many operations, this might simply be an expensive nuisance with a cumbersome workaround, but for an unconscious inmate needing a particular medication, the lack of quick access to his records could be devastating. Or what happens if information is hosted and used on a contractor's proprietary application? Is the data useable without the application, and can it be imported into another application? And even if data can be migrated to a new solution, how long will it take?

Another example is a janitorial-service contract. It is easy to identify the risk of personal injury if a janitor fails to leave a warning sign on a slippery bathroom floor, but what happens if the contract involves healthcare, with its own unique risks of exposure to infectious materials?

While there is no easy way to identify all the risks, the best practice involves a three-step process.

1. Thoroughly research the industry for the particular contract. Look at sample industry contract forms for how they deal with risk. Search online for risk-related information. If the contract, for example, involves "Software-as-a-Service," search online for "contract risks for software as a service," "contract risks for cloud computing," and similar queries.

2. Engage those involved in acquiring or managing the service, such as the agency's IT office, *and* those directly involved with using the service, such as medical staff. They know the landscape and are in a good position to know some of the hidden risks. They can tell you, for

example, the type of data that would be hosted on a contractor's server, or whether the janitor's access will extend to confidential data.

3. Understand the contract and the terms you are soliciting. Read it … and read it again. Contracts are not something only lawyers should read.

Examples of potential risks include the following:

- Financial loss
- Property damage
- Loss of confidentiality
- Loss of public confidence
- Loss of data
- Contractor insolvency
- Disruption of contractor services
- Disruption of internal operations
- Exposure to legal liability
- Exposure to federal fines for noncompliance
- Hidden liabilities (agreeing to something unanticipated)
- Costs of re-procurement

Throughout the acquisition, and continuing during contract administration, ask yourself "what could go wrong and how?" It may help to identify, for each risk, (1) the cause of the harm, (2) the type of harm, and (3) the consequences of the harm. Be as specific as possible with regard to each identified risk and associated consequence. Solely for purposes of illustrating a structured approach to identifying risk, consider the following tables, which identify *a few* of the risks associated with third-party hosting of protected health information and janitorial-service contracts, but are not necessarily reflective of what losses might actually occur:

Risks Associated with Third-Party Hosting of Patient Health Information

Cause of Harm	Type of Harm	Consequences
Lack of quick access to electronic records	Personal injury	Pay damages for personal injury
Data breach, data theft	Large scale disclosure of citizens' personally identifiable information / identity theft	Pay damages for privacy intrusion and identity theft monitoring
Data breach, data theft	Loss of reputation or public confidence	PR fees and associated costs
Data breach, data destruction	Large scale loss of agency data	Replacement costs, costs for uploading soft or hard copy backup data and business interruption
Losing access to proprietary application	Unusable data	Conversion costs or licensing fees
Service disruptions	Disrupted internal operations	Loss of employee productivity, payment loss through rescheduled appointments

Risks Associated with Janitorial-Service Contracts

Cause of Harm	Type of Harm	Consequences
Wet floors, unsecured tools and equipment, use of toxic or allergenic cleaning products, unvaccinated cleaning staff, etc.	Personal injury to agency staff	Compensation for personal injury, loss of employee productivity, etc.
Use of caustic or improper cleaning products, carelessness, vandalism, theft, accidental destruction, etc.	Property damage, loss of equipment or valuables	Replacement costs, loss of employee productivity, etc.

Data breach, theft of papers, etc.	Small scale disclosure of citizens' personally identifiable information / identity theft	Pay damages for privacy intrusion and identity theft monitoring
Data breach, theft of papers	Loss of reputation or public confidence	PR fees and associated costs

In addition to the risks involved in the performance of a service, some contracts carry a risk that the contractor will delay or fail to complete a project, as illustrated by the risks associated with completing a software-development project:

Risks Associated with Completing Software Development Projects

Cause of Harm	Type of Harm	Consequences
Delayed completion	Delay damages	Pay incumbent vendor for continued performance and software licensing fees (in addition to license fees for new service)
Project failure; non-completion	Costs of cover, re-procurement costs, sunk costs	Difference in price between failed contractor's price and new vendor's price, costs to re-procure new contract, the value of time and effort wasted on failed project, costly litigation

Analyzing the Risk

After identifying the risk, the next step is to analyze the (a) probability of harm and (b) the severity of harm. In other words, "what are the odds?" and "how bad are the consequences?" First, analyze the probability that the cause of harm will occur during the life of the contract and categorize it as rare, unlikely, likely, or almost certain. Second, analyze the consequences and apply a severity rating that is categorized as negligible, low, moderate, or high. This analysis will result in a "Risk Level" of very low, low, moderate, high, or extreme. The following guideline may help:

- ***Negligible.*** The potential harm to operations, assets, or individuals is *nominal* in isolation—i.e., if the potential harm is not repetitive—with potential insignificant financial loss or insignificant harm to individuals.

- ***Low.*** The potential harm to operations, assets, or individuals is *minimal*, with potential minor financial loss or minor harm to individuals. For example, a temporary service interruption with only a minimal impact on an agency's internal operations.

- ***Moderate.*** The potential harm to operations, assets, or individuals is *serious*, with potential significant financial loss or significant, but not fatal or life-threatening, injuries to individuals. For example, a service interruption where agency can still use a workaround—albeit with significantly reduced effectiveness.

- ***High.*** The potential harm to operations, assets, or individuals is *severe* or *catastrophic*, with potential major financial loss, or fatal or life-threatening injuries to individuals. For example,

a complete service interruption where an agency cannot perform its primary functions over an extended period of time.

Risk Level Table

The following table shows the Risk Level—very low, low, moderate, high, or extreme—where the severity rating intersects with the probability of harm:

		Severity			
		Negligible	Low	Moderate	High
Probability	Almost Certain	Moderate	High	Extreme	Extreme
	Likely	Low	Moderate	High	Extreme
	Unlikely	Very Low	Low	Moderate	High
	Rare	Very Low	Very Low	Low	Moderate

Managing the Risk

Now that you have identified the risks and used the Risk Level Table above to determine the Risk Level for each specific risk, you need to determine how best to manage the risks. The State can manage a risk by assuming, avoiding, mitigating, insuring, or transferring it.

- ***Assume the Risk.*** This means that if something goes wrong, the agency accepts responsibility for the harm.

- ***Eliminate the Risk.*** This includes either avoiding or minimizing realization of the risk. Avoiding the risk could involve a major change, such as deciding not to contract, or a relatively minor change, such as making a manageable adjustment to the agency's operations or contractor's performance obligations. For example, if the risk threatens a total, permanent loss of the agency's data, the risk might be reduced by having a periodic backup copy maintained. The agency could self-perform this service or require the contractor to back up the data to a reputable third party.

- ***Mitigate the Risk.*** Risk is mitigated when the resulting harm is lessened. For example, if the risk involves an improper disclosure of citizen financial data, and the type of harm is "identity theft," a plan for providing "identity theft protection services" may lessen the harm.

- ***Insure the Risk***. Some risks can be covered by acquiring insurance. An agency may either acquire insurance directly from an insurance carrier or require its contractor to acquire the insurance.

- ***Transfer the Risk***. Transferring risk may be particularly appropriate when the contractor is better positioned to manage the risk. Contractual indemnity clauses, in which the contractor agrees to compensate the State for certain losses, can be an effective way to transfer risk. Imposing specific performance obligations on the contractor, such as requiring it to back up the data to a reputable third party, can be equally or more effective.

For some risks, you should combine two or more options. For example, if the Risk Level is high, consider mitigating, insuring, *and* transferring the risk—if not avoiding it altogether. For a low-level risk—or even for a high-level risk where the benefits of the contract greatly outweigh its risk—the State may be comfortable assuming that risk.

When determining how to manage the risk, you should compare the Risk Level of the agency's current practices to the Risk Level associated with the contractor's services. This may impact how the risk is managed. For example, the Risk Level associated with data loss may be high with a Software-as-a-Service contract, but it may involve less risk than what the agency is doing now, which may impact whether the agency seeks to assume or transfer the risk.

Keep in mind that the more risk you shift to the contractor, the more the contractors will charge, and the less likely they will bid.

Using the Contract to Manage the Risk

Careful drafting of contract terms is a powerful tool for managing risk. Common contract clauses, such as those addressed below, can be used to transfer, mitigate, or insure risk; however, **appropriate performance obligations are often the best approach to managing risk effectively**.

Performance obligations. These clauses require the contractor to perform a particular task which is intended to mitigate a specific risk. For example, requiring the contractor to maintain a backup of State data with a reputable third party reduces the risk of data loss. For a janitorial-service contract, requiring a certain level of screenings and background checks for janitors reduces the risk of theft.

Insurance clauses. These clauses require the contractor to acquire insurance against certain risks. To use these clauses effectively, you must understand the risks they cover and whether they address the risks at issue. You must also understand the risks they do *not* cover; insuring a risk is of little value if the policy has an "exclusion" that excludes the very risk you hope to cover. For example, if the policy has an "illegal or criminal act exclusion," the policy may not cover the risk of theft by a contractor's employee. Remember, you must also require the level of coverage appropriate to your Risk Level.

The following clauses illustrate this point. However, do not rely on this summary description of coverages. Rather, read the clause and the associated guidance in the Compendium and consult your

resource on insurance. **Further, do not assume that the default coverage-limits printed in the model clauses (e.g. $1,000,000, $5,000,000, etc.) will be appropriate for your agency's needs.**

- *Contractor's Liability Insurance – General (FEB 2015).* This clause requires three types of insurance: Commercial General Liability ("CGL"), Automobile Liability, and Worker's Compensation/Employer's Liability. In broad terms, CGL covers claims for personal injury or property damage arising out of the contractor's performance; Automobile Liability covers claims for personal injury or property damage arising out of the use of automobiles as part of the contractor's performance; and Worker's Compensation/Employer's Liability covers personal injury suffered by contractor's employees arising out of the contractor's performance. [07-7B056-2]

- *Contractor's Liability Insurance – Information Security Privacy (FEB 2015).* In broad terms, this clause requires insurance that covers claims arising out of data breaches, malicious viruses, invasion of privacy, theft or corruption of data, negligence, and similar acts or omissions in the performance of IT service contracts. For more details, read the model clause and the associate guidance. [07-7B058-1]

Indemnification. Indemnity clauses are useful where the contractor's actions could expose the State to third-party liability. Contractors do not like these clauses. These clauses are only as valuable as the contractor's pockets are deep; thus, they should be used to supplement, not replace, insurance coverage. Consider the following clauses:

- *Indemnification – Third-Party Claims – General (NOV 2011).* This clause generally provides that, in the event a person brings a claim against the agency arising out of the contractor's service, act, or omission, the contractor will defend the agency and pay any judgment against the agency. For example, if a citizen slips on a wet floor caused by the negligence of a contractor's janitor, and the citizen then sues the agency, this clause requires the contractor to defend the claim and pay any settlement or judgment. [07-7B100-2]

- *Indemnification – Third-Party Claims – Disclosure of Information (FEB 2015).* This clause is tailored to disclosures of information, such as health information or social security numbers, caused by any act or omission of the contractor while performing the contract. This would apply, for example, if a contractor failed to implement required controls for protecting information on its computer server, leading to unauthorized disclosure of protected health information. [07-7B103-1]

- *Information Use and Disclosure (FEB 2015).* Subsection (h) of this clause provides that, in the event of improper disclosure of citizen information, the contractor shall provide legally required notice, pay for identity theft monitoring services, pay any related fines, undertake customary measures for such disclosures, and pay the agency's reasonable costs and public relations services involved in responding to the disclosure. [07-7B108-1]

Do not rely on the foregoing summary of the clauses referenced. Rather, read the clause, read the associated guidance, and consult your appropriate agency resource.

Other clauses. Clauses requiring indemnification and insurance are not the only clauses that manage risk. Likewise, the **suggestions in this Framework are not the only options to manage the risk.** Other contractual ways to manage the risk include, but are not limited to—

- *Liquidated damages*. A liquidated-damages clause may be appropriate when time is of the essence and there is a risk that the contractor will delay performance. For example, for every day the contractor misses a milestone in a software-development project, it must pay the State $1,000. To be enforceable, **liquidated damages cannot be a "penalty,"** but rather a reasonable cover of the estimated costs of the delay to the State, as determined at the time of contracting. Service credits in a service-level agreement are a form of liquidated damages that are sometimes used in IT service contracts: if the contractor fails to maintain a specified service level, the agency would be entitled to a service credit.

- *Contractual incentives*. If liquidated damages are the "stick," contractual incentives are the "carrot." They can also be used in conjunction with liquidated damages. For example, for every day a contractor misses a milestone, it must pay $1,000 in liquidated damages, but for every day it is ahead of schedule, it receives $1,000.

- *Performance bonds*. Performance bonds include completion bonds and indemnity bonds. Performance bonds do not ensure a contractor's performance, but they do provide a reliable source of funds if a contractor cannot perform due to its lack of funds. For additional discussion on the proper use of performance bonds, see https://procurement.sc.gov/legal/proc-docs and https://www.nascio.org/Portals/0/Publications/Documents/NASCIO_PerformanceBonds_August2012.pdf

- *Limitations of liability clause*. "Limitation of liability" clauses are risk allocation devices that impose limits on the liability of a contractor (and the agency). Because they limit a contractor's liability, they should rarely be used, and only in limited circumstances, such as contracts for software licensing and complex IT services such as cloud-based services or software development. Limiting liability may encourage otherwise reluctant vendors—particularly larger and more sophisticated IT firms—to bid on a solicitation. Use caution and consult upper management and legal counsel before including one in a solicitation. For more information, see the Division's "Basic Guidelines for Using Limitation of Liability Clauses in Complex Information Technology Contracts."

Despite their value, such clauses are not a silver bullet and, in the right circumstances, may create their own complications. For example, contractual incentives can be a powerful motivator, but when both parties claim the other has caused delayed performance, they may also incentivize litigation.

Practical Considerations for the Acquisition Process

The risks involved in a project can discourage contractors from bidding or cause them to submit bids that are non-responsive, too expensive, or too focused on risk—all to the detriment of effective contract performance. To avoid these results, several steps should be considered.

1. Identify, analyze, rate, and plan for management of the agency's risks, along the lines outlined herein.

2. Avoid the temptation to saddle the contractor with all the risk.

3. Consider asking potential contractors to identify the risks associated with the undertaking. This may occur during market research, in the solicitation phase, or both. A clause for asking vendors to disclose known risks is attached as **Attachment A**. This effort signals to vendors your awareness of their concerns and your understanding of the need for an appropriate allocation of risk. In the process, vendors may provide the agency with valuable insight to potential risks to the agency.

4. If you conduct negotiations, consider addressing appropriate risk allocation and its impact on price and performance.

Putting It All Together

To assist you in your efforts to identify, analyze, rate, and plan for management of the agency's risks, you may find it helpful to use the Risk Analysis Table found at **Attachment B**. Finally, when planning and negotiating, consider the following suggestions:

1. Involve upper management, counsel, or both when preparing a solicitation that—
    a. Involves at least a moderate Risk Level
    b. Involves contractor access to, or the hosting of, critical or confidential data
    c. Solicits services provided by large IT firms

2. Always—
    a. Research the risks and engage the end users prior to solicitation to obtain input regarding risk identification, analysis, and management approaches
    b. Consider risk analysis a never-ending process during the entire contract life cycle
    c. Read and re-read the solicitation, then the contract, with the idea of risk in mind
    d. Assume the worst could go wrong, and plan for it
    e. Insist that every contractor have proof of insurance (if required)
    f. Confirm that the contractor's insurance policy conforms to the contract's requirements
    g. Consider using a limitation of liability in complex IT service contracts

3. Never—
    a. Blindly rely on model or standardized contract clauses
    b. Default to the contractor's standard insurance policy
    c. Agree to limit liability to total contract price, absent careful consideration and compelling circumstances; doing so may effectively eliminate the recovery of any damages to the agency—leaving only a refund for something you may not have received
    d. Include a limitation of liability clause without approval from upper management

ATTACHMENT A

INFORMATION FOR OFFERORS TO SUBMIT – RISK ANALYSIS (JAN 2020): When both parties fully understand the risks associated with a proposed contract, they can better manage and more appropriately allocate those risks. Accordingly, and for purposes of evaluation, you should submit the following: (i) an identification of key risks involved in the contract's performance and non-performance; (ii) an identification of the key risks to successful performance; (iii) an analysis and evaluation of the risks identified; and (iv) recommendations for managing the risks. Please address risks to everyone involved, such as the agency, contractor, expected users, and business partners. In responding, you are welcome to use the Risk Analysis Table found at www.procurement.sc.gov/legal/resources. [04-4013-1]

ATTACHMENT B

Risk Analysis Table

You may find it helpful to use the spreadsheet found at www.procurement.sc.gov/legal/resources. Some cells have drop down menus and the Risk Level is automatically calculated based on the input provided. The following is an example of how to use this spreadsheet for *one* of the risks associated with third-party hosting of patient health information.

Cause of Harm	Probability	Type of Harm	Consequence	Severity Rating	Risk Level	Management Approach	Management Mechanism	Estimated Cost of Management Mechanism
Data breach, theft	Rare	Loss of agency data, loss of client confidentiality, loss of reputation	Replacement costs for back up data	High	Moderate	Mitigate, insure, and transfer	Mitigate by requiring a backup and requiring contractor to pay for identify theft protection; insure by requiring contractor's insurance to cover sufficient risk; transfer by requiring contractor to indemnify claims by citizens against the agency	$_____ (Optional)