APTA STANDARDS DEVELOPMENT PROGRAM
WHITE PAPER
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

PS-TP- WP-001-11
Approved June 2011
APTA Procurement Technology
Standards Workgroup

Technology Terms and Conditions

Abstract: This White Paper discusses the risks and benefits of technology-related terms and conditions which can be included in IT procurement contracts.

Keywords: clause, contract, information technology (IT), procurement, terms and conditions

Summary: As transit agencies incorporate more technology into their operations, standards that guide the procurement of these technologies will improve the purchasing agencies' and suppliers' likelihood of achieving successful procurements. Technology procurements have inherent differences from other procurements that agencies process; therefore, guidance specific to technology will significantly improve the development of terms and conditions and risk management for these procurements.

Scope and purpose: These guidelines can be used by public transit agencies procuring IT systems, ranging from the simple procurement of computer hardware and stand-alone software to the purchase of complex systems involving GPS technology, mobile data terminals, telecommunications, wireless and radio systems, software for scheduling and operations, Internet and automated rider information media. The guidelines are also useful when purchasing IT services, and for making sure the imbedded IT components of rail and bus equipment are properly evaluated.

This White Paper represents a common viewpoint of those parties concerned with its provisions, namely, transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any standards, practices or guidelines contained herein is voluntary. In some cases, federal and/or state regulations govern portions of a transit system's operations. In those cases, the government regulations take precedence over this standard. APTA recognizes that for certain applications, the standards or practices, as implemented by individual transit agencies, may be either more or less restrictive than those given in this document.

APTA Standards Development Program
Lead the Way

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Technology Procurement Standards Workgroup,** which provided the primary effort in the drafting of this *White Paper*.

At the time this standard was completed, the committee included the following members:

Anthony Bombace, Co-Chair
Robin Cody, Co-Chair

Aida Asuncion, Los Angeles Metro
Becky Barrington, Capital Metro
Sreeni Malireddi, Intueor
Colin McKenzie, Trapeze Group
Kunjan Dayal, Metro (Phoenix)
Kevin Dow, APTA
Pete Salazar, SamTrans
Jason Ellis, Medical Transportation Management
Lloyd Sullivan, OCTA
Larry Frum, NCTD
Doug Spaeth, Ontira Comm. Inc.
Tiffany Lorenzen, San Diego MTS
Roger Thorn, Sacramento Regional Transit
David Sullivan, Hampton Roads Transit
Michael Haddad, CATS

Contents

Introduction

Information Technology (IT) is defined in the Transportation Equity Act (TEA) as “the application of information, control and communications technologies to surface transportation.” TEA also states that “Intelligent Transportation Systems (ITS) Projects are any project that includes the implementation and operation of one or more of the ITS User Services defined in the National ITS Architecture. All ITS projects funded from the Highway Trust Fund must conform to the National ITS Architecture.”

In addition, Federal Acquisition Regulations (FAR) define IT as: “Information technology and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information.” Also included in the definition is “acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.”

Accordingly, these guidelines can be used by public transit agencies procuring such systems. IT can range from the simple procurement of computer hardware and stand-alone software to the purchase of complex systems involving GPS technology, mobile data terminals, telecommunications, wireless and radio systems, software for scheduling and operations, Internet and automated rider information media.

The guidelines are also useful when purchasing IT services, and for making sure the imbedded IT components of rail and bus equipment are properly evaluated.

With the rewriting of TEA for 2009 and mandatory standards for compliance with the National ITS Architecture, there will be tougher requirements for IT systems to become more interconnected and to trade data with one another. This means that public transit agencies should be very careful to evaluate the capability of their IT purchases to interact with their existing systems, with planned systems and with the external systems with which there are mandated data exchanges.

As transit agencies incorporate more technology into their operations, standards that guide the procurement of these technologies will improve the purchasing agencies’ and suppliers’ likelihood of achieving successful procurements. Technology procurements have inherent differences from other procurements that agencies process; therefore, guidance specific to technology will significantly improve the development of terms and conditions and risk management for these procurements.

Vendors will benefit from these guidelines by having an understanding of the agency’s risk assessment early on in the procurement process. This will enable the vendors to address these areas in their responses. Discussions and negotiations will be able to begin from a point of mutual understanding of the risks involved and how those risks can be shared.

This document is intended to address technology contracts for acquisitions that involve software and/or services. Hardware acquisitions are generally specification-driven, and low bid is the method of purchase.

The Technology Procurement Standards Committee was formed in July of 2007 and tasked with developing technology-specific procurement standards to guide the procurement process and to improve the development of terms and conditions and risk management.

The committee has benefited greatly from the diverse background of its team members, which include vendors and representatives from transit agencies across the country representing procurement, information technology, project management and general counsel.

This document represents the team’s shared experience and vast collective knowledge of technology procurements and the contracts that support those procurements. The document consists of 39 items focused on terms and conditions and risk management that are critical for successful technology procurements. Specifically, these contracts would generally include technology acquisitions that involve software and/or services, and the language in this document can be applied to any technology acquisition, whether ITS or administrative IT back-office systems.

The initial challenge faced by the committee in developing this document was discerning the differentiators for technology procurements. It was the team's position that if a particular item couldn't be classified as unique to technology procurements, then it didn't belong on the list, so the list is not meant to be exhaustive of all terms and conditions found in a typical contract, but relevant to technology software and services acquisitions.

To help focus the team's discussion, the committee created three broad categories for technology procurements: software, hardware and embedded. The committee separated into two groups, one dedicated to software and the other dedicated to hardware and embedded technologies. It became clear early on that hardware and embedded technologies were generally based on the specifications that were developed for bid. Only the software and/or services that accompanied the hardware or embedded chip technology could be impacted by the terms and conditions.

Throughout several focus group and brainstorming sessions, each team created a list of items that were deemed to be unique to their specific technology procurement category. Once completed, the lists were combined, and the committee joined together again to scrutinize the output. Any item that could not be identified as unique to technology was removed from the list.

The team agreed on a format for the document and reached consensus on five topics that should be addressed for each item: discussion, risks, benefits, common approaches, and a "see also" category to link to related items within the document.

In addition, a checklist is provided at the beginning of the document that agencies can use can to ensure that any key terms and conditions are not missed as they prepare their contracts.

Terms and Conditions Checklist

	Acceptance of Project
	Additional Business Units (Affiliated Agencies)
	Agency/Vendor/Contractor Responsibilities
	Assignment
	Change Order Process
	Compliance Matrix
	Confidentiality
	Current Information Technology Infrastructure
	Customizations
	Definitions of Words and Terms (Glossary)
	Delivery and Acceptance
	Disaster Recovery/Business Continuity
	Dispute Resolution
	Economies of Scale
	End of Life Cycle
	Grant of License and Scope of Use
	Indemnification
	Infringement
	Intellectual Property Rights
	Licenses, Ownership and Transfer
	Limitation of Liability
	Liquated Damages
	Operations
	Order of Precedence
	Ownership and Use of Data
	Path Back (a.k.a. Insourcing)
	Payment and Delivery Schedule
	Project Personnel
	Records and Audit
	Security
	Site Visits
	Software Protection
	Source Code Escrow
	Standards Adherence
	Support and Maintenance
	Taxes
	Term of Agreement
	Training
	Warranty

Acceptance of Product

Discussion

An Acceptance of Product clause applies more to procurement of IT hardware, software or systems rather than to IT services. The key to a successful transition from installation of IT to its active use by the purchaser is a precise definition of the features and performance that are to be delivered in the Compliance Matrix, and a clear acceptance plan for the product, including the measures to be used to determine if it meets contractual requirements.

Both the vendor and agency typically will be involved in acceptance procedures. The purchaser may stipulate in the contract that it will perform acceptance testing according to a mutually agreed plan, or the vendor may conduct testing with the agency monitoring the process and/or reviewing test results.

Acceptance procedures can range from the relatively straightforward, such as turning on delivered hardware and running diagnostics, to actually running complex systems “online” for a trial period.

Where complex products are involved that interact with the agency’s own IT environment, it is important to define “who is responsible for what” ahead of time to avoid finger-pointing. For example, a requirement for 95 percent operation without interruption should exclude power, facility and network disruptions that are the agency’s job to maintain.

Acceptance can occur in several steps, often related to the payment and delivery schedule of the contract. Many IT contracts provide partial payment for a “factory acceptance” of the generic product, another payment when the product is operational on-site, another when customizations are shown to be completed, and the last when the product has completed trials in service. If complex systems are involved, particularly those that take a long time to install, staging acceptance is recommended. This will minimize unexpected results by providing concrete measures of success along the way.

Risks

- Without clear definition of what is an acceptable time frame for installation, scope, schedule and/or cost creep are probable. These are commonly the cause of IT project failure.
- Issues may arise from applications or systems that meet “scope” but not “intent.” This can occur when the method chosen to resolve the issue, or to perform a function, is not functional in the day-to-day operation of the application or unit.

Benefits

- Clear and mutually acceptable acceptance requirements, plans and procedures are a protection for both the agency and the vendor, by defining at the outset what is expected of the project.
- Acceptance definitions provide a detailed separation of perceptual assessments and rely on established measurements for success.

Common approaches

- Tie acceptance requirements to the Compliance Matrix.
- Include acceptance tasks in the work program and schedule.
- Consider staged acceptance if the project is complex.
- Be sure to clarify what the agency is responsible for.

See also **Agency/Vendor/Contractor Responsibilities**; **Compliance Matrix**; **Payment and Delivery Schedule**; and **Dispute Resolution**.

Additional Business Units (Affiliated Agencies)

Discussion

Most agencies are operating with additional business units or affiliated agencies in the day-to-day execution of their overall business. Affiliated agencies may include municipal transit agencies, public transit providers for the disabled, freeway service patrol and others. In many cases, resources and assets, including IT systems, are shared among the units. Therefore, procurements of IT should include the requirements of affiliated agencies.

Contracts, pricing and protection should also be accounted for with respect to additional business units, much as in piggybacking on vehicle procurement.

Risks

If the requirements of additional business units or affiliated agencies are not identified as part of the contract, there may be additional costs for use of systems, hardware and software licenses that could have been part of the original contract and created volume pricing discounts for the agencies.

Benefits

- Additional business units or affiliated agencies are able to utilize the procured system, hardware or software under a single procurement without jeopardizing the validity of the contract or software license agreements.
- Cost is potentially reduced, and interoperability is guaranteed between associative agencies.

Common approaches

Some agencies use the following special provision in their contracts:

> The AGENCY may use the Licensed Software on any and all system components or equipment configurations or whatever make, manufacture and/or model, owned, controlled or contracted for by the AGENCY, or its affiliated agencies provided such affiliated agencies execute the required Software License Agreements. Irrespective of the number of system components or equipment configurations upon which the Licensed Software is used, the AGENCY and its affiliated agencies shall pay no additional license fee, in addition to the total contract price.

See also **Support and Maintenance**; **Grant of License and Scope of Use**; and **Economies of Scale**.

Agency/Vendor/Contractor Responsibilities

Discussion

The fundamental lesson learned from IT projects is that success depends on a team effort between the purchasing agency and the vendor/contractor. As in any team effort with many players, it is crucial to define “who does what when and how” before the action starts.

Agency/vendor/contractor responsibilities can be uniquely challenging to define in technology procurement because of the sheer number of tasks required, the potentially complex interactions between the procurement and the existing agency IT environment, and the impacts that the new technology may have on agency business processes and personnel. Nonetheless, the importance of clearly defining agency/vendor/contractor and third-party responsibilities cannot be overstated.

Responsibilities should be spelled out in the work plan and scheduled for each task and each deliverable, including things such as resource requirements, work space and work rules.

Risks

Assumptions will be made on who is responsible for various deliverables, or pieces of deliverables, causing potential scope changes. Common misconceptions include who is responsible for developing test scripts, creating reports and conducting training. Many vendor/contractors use train the trainer. It is equally risky not to define agency responsibilities to the same level of detail as those of the vendor/contractor. The absence of a clearly documented and defined list of responsibilities may result in the agency not committing the necessary resources to successfully complete the project. A common oversight is to not spell out agency project management, review and acceptance responsibilities, as well as staff availability for training, conducting training, and additional required software such as a specific database, support, connectivity channels, etc.

Benefits

- Eliminates confusion and sets expectations. Also ensures that the proper resources, both human and capital, will be in place at project kickoff.
- Helps minimize “schedule creep” and other implementation problems by determining who is supposed to do what when.
- Requires agency user groups to provide their input adequately and in a timely manner.

Common approaches

- Specify the agency’s/vendor’s/contractor’s responsibilities in the Statement of Work (SOW) and Project Schedule.
- Require the vendor/contractor during the contracting process to provide a combined SOW and work schedule for everyone involved in the project, including the agency and any third parties. This SOW and work schedule, after being reviewed by the agency and revised as needed, will become part of the contract.
- In some cases, agencies include a statement that items and equipment not specified will be the responsibility of the vendor/contractor. This reduces the risk to the agency but may result in increased costs. A well thought out and comprehensive SOW will help minimize the risks to both the agency and vendor, and will reduce the importance of including these types of potentially controversial statements.
- The SOW and work schedule are the “marching orders” for all members of the team. They may be modified by mutual agreement, although if doing so involves a change in cost, effort or schedule, then a change order may be involved.
- Contract should require that the vendor’s/contractor’s and agency’s project managers regularly update the project schedule by recording particular individuals or work groups within each party that is accountable for the scheduled task.

See also **Compliance Matrix**; **Payment and Delivery Schedule**; and **Project Personnel**.

Assignment

Discussion

In the course of contract execution, vendors/contractors or agencies may deem it necessary to assign, transfer, convey or otherwise dispose of all or portions of the work to other parties. This could have a negative impact on the completion of the contracted work and may result in unrecoverable costs to the agency. Contract terms and conditions should define the vendor's/contractor's and the agency's responsibilities when assignments are made during contract execution. Assignments can be work, equipment leases and/or software licenses.

Assignment language needs to apply to the life of the contract and to any ongoing licenses and maintenance contracts. Oftentimes the ongoing licenses and maintenance contracts are overlooked and assignment provisions are extinguished when the original contract terminates.

It is not uncommon for software companies to be acquired by larger organizations. When this occurs, the acquiring firm may request that the agency sign new licensing and/or maintenance agreements, even though assignment clauses exist within the original contract signed by the acquired firm, and possibly within valid support and maintenance agreements. Should this occur, it is important to attempt to enforce the original terms agreed to by the acquired firm according to the terms and conditions outlined in the assignment clause. Failing that, the agency should negotiate the terms of the proposed new licensing and/or maintenance agreements to the best interest of the agency.

Risks

- Work may not be completed as stipulated in the original contract, or the contract may not be completed at all. Agencies may be held responsible for additional costs brought by the transfer of work to others.
- If one vendor/contractor is purchased by another vendor/contractor, which may have different licensing and lease models, due diligence is required by the agency to ensure that negotiated agreements are held intact.

These problems may occur without explicit terms in both the contract and support and maintenance agreements binding assignees and/or successors to the same conditions as the original signatory *and* stipulation that these terms are not extinguished at the completion of the agreements.

Benefits

Assignment of work to others may be the only way to complete the contract, especially if the original contractor is having difficulty financially or technically in completing the work. It will be beneficial if provisions in the contract are made to address assignment of work to a third party. In addition, this provision allows for the agency and the new vendor to maintain their existing agreement without having to renegotiate terms and conditions after the procurement is completed.

Common approaches

The conditions of assignment may be stipulated in the contract's terms and conditions as follows:

> The VENDOR/CONTRACTOR shall not assign, transfer, convey or otherwise dispose of the contract or a Contract Work Order (CWO) or the right, title or interest in it or any part of it without the prior written consent and endorsement of the AGENCY, which consent shall not be unreasonably withheld.
>
> No right under the contract shall be asserted against the AGENCY, in law or in equity, by reason of any assignment of the contract, or any part thereof, unless authorized by the AGENCY as specified in this Article.
>
> Any assignment of proceeds of the contract shall be subject to all proper setoffs and withholdings in favor of the AGENCY and to all deductions specified in the contract or Contract Work Order (CWO). All monies withheld, whether assigned or not, shall be subject to being used by the AGENCY for completion of the work, pursuant to the terms of the contract.

Any assignees, agents or successors to the CONTRACTOR shall be bound by the terms of the agreement.

The CONTRACTOR shall not assign, encumber, transfer, convey, sublet or otherwise dispose of this Contract or of its right, title or interest therein, or in any part thereof without the prior written consent of the AGENCY. Nothing herein shall either restrict the right of the CONTRACTOR to assign monies due or to become due pursuant to *[insert name of state and code section which allows]*, or be construed to hinder, prevent or affect any assignment by the CONTRACTOR for the benefit of Creditors, made pursuant to applicable law.

If the CONTRACTOR violates the provisions of this Article, AGENCY may void the Contract, and AGENCY shall thereupon be relieved from any and all liability and obligation thereunder to CONTRACTOR or to anyone to whom CONTRACTOR shall so assign, encumber, transfer, convey, sublet or dispose, and all monies theretofore earned under the Contract shall be forfeited and lost except so much as may be required to pay employees.

See also **Term of Agreement** and **Ownership and Use of Data**.

Change Order Process

Discussion

With most technology projects, changes are inevitable due to inherent complexities. For example, information technology software and systems projects typically uncover new concepts or changes that could not have been anticipated at the outset of the project. It is critical that a formal, documented process be in place to process the change request. No matter how insignificant the change may seem, it should still follow the documented change process. The Compliance Matrix, Statement of Work and Project Schedule should be consulted to determine whether a proposed change is truly out of scope.

When a change request is initiated for a technology project, consideration needs to be given to "downstream" impacts caused by the change. Oftentimes even the simplest change will require changes to the design documents, testing plans and training materials.

Risks

Without a technology project change order process, project cost and schedule can greatly be impacted and the potential for vendor/contractor abuse can be exorbitant. The absence of a documented change process leads to rampant scope creep, lack of formal acceptance, insufficient testing, potential conflicts and lack of communication.

Benefits

Adoption of a technology project change order process provides for effective management of project costs and schedule. A well-documented change process that is tied into the Compliance Matrix, SOW and Project Schedule will limit the amount of scope creep and will help to ensure that all changes are communicated and required. In addition, when the change is accompanied by a cost, it will allow for a cost/benefit analysis to be done.

Common approaches

The Change Order process should be clearly spelled out in the RFP and should include an approval process and required forms to use. Some agencies stipulate the requirement of a Change Order Process as part of the General Conditions for the contract. Some typical language is as follows:

> Some agencies may order changes within the general scope of the Contract without notice to sureties. These will be authorized by a Change Order. Upon receipt of a Change Order, the VENDOR/CONTRACTOR shall promptly proceed with the change involved, which will be performed under the applicable conditions of the Contract. No order, statement, or conduct of the AGENCY other than a Change Order shall be treated as a change under the Contract or entitle the VENDOR/CONTRACTOR to an adjustment under the contract.
>
> The VENDOR/CONTRACTOR shall promptly submit a Request for Change, described below, to the AGENCY when it receives direction, instruction, interpretation, or determination other than Change Order from any source that it believes to be a change. Except where the AGENCY's authorized representative determines that such work is not a change and orders VENDOR/CONTRACTOR to proceed with the work, VENDOR/CONTRACTOR shall not proceed with the work which is the subject matter of the Request for Change until the AGENCY issues a Change Order.
>
> The VENDOR/CONTRACTOR shall continue to perform work during the change process in a diligent and timely manner, and shall be governed by all applicable provisions of the Contract.

See also **Compliance Matrix**; **Payment and Delivery Schedule**; **Agency/Vendor/Contractor Responsibilities**; **Licenses, Ownership and Transfer**; **Customizations**; and **Taxes**.

Compliance Matrix

Discussion

A table that defines in detail the required capabilities, features and performance of the IT product being purchased is an extremely important prerequisite to a successful IT project. The table layout requires the vendor/contractor to specify whether its solution complies, partially complies, will comply (under development), does not comply or has an alternate to meet the precise functional specifications for each of the requested capabilities, features and performance indices. Once bound into the contract, it becomes the yardstick against which acceptance can be measured and is also a basis for determining if changes along the way are in or out of scope.

If the contract is for information technology services and does not involve hardware/software or other tangible items, a Compliance Matrix is still useful. It can commit the vendor/contractor to assign specific staff for defined periods of time to conduct specific tasks. Performance criteria also can be included.

Risks

A main reason for IT project failure is lack of a clear and comprehensive definition of the deliverable that has been signed off by all the contracting parties. Without a Compliance Matrix, it can be time consuming and difficult to determine if the vendor/contractor has adequately addressed the RFP requirements. There is increased risk of miscommunication and of setting false expectations.

Benefits

- Disciplines the agency to define in detail exactly what is being procured.
- Allows the agency to identify what items are mandatory, preferred or desired.
- Helps the evaluators locate vendor/contractor compliance against the requirements.
- Demonstrates that the vendor/contractor has carefully identified all of the RFP requirements.
- Provides performance standards to hold the vendor/contractor accountable.
- Serves as an internal checklist to ensure full vendor/contractor compliance.
- Minimizes disputes by being clear as to what is in or out of scope.
- Serves as an excellent guide for acceptance test procedures regarding demonstration of features/functionality.
- Can be tied to the project timeline and milestone payment schedule.
- Encourages eventual users within the agency to be clear about their needs at the outset.

Common approaches

Typically, the agency develops a detailed specification for each aspect of the IT being purchased, preferably involving the eventual users. Consultation with other agencies that have gone through similar procurements, vendors and others in the industry produces useful inputs. Agencies may consider putting out a Request for Information (RFI) before the Request For Proposal (RFP) as an aid to developing the Compliance Matrix. The Compliance Matrix will draw out from bidding vendors/contractors the extent to which they comply, partly comply, will comply or cannot comply with the requirements. By so doing it is a useful tool in the selection process. The Compliance Matrix is often regarded as a dynamic document in the contracting process. The agency and vendor may agree to redefine what is mandatory, optional or deferred.

Confidentiality

Discussion

Businesses rely on the products and services that they market for their survival and prosperity. At the same time, agencies are funded by public tax dollars and have to abide by public records and Freedom of Information Act requirements.

Confidentiality requirements will probably apply to information supplied by bidders during the selection process, and will certainly apply to both agency and vendor information during execution of the contract. When the procurement is in service and being supported/maintained, confidentiality may continue to apply.

The simple act of marking information as confidential is not sufficient. Information specific to an organization or contractor's business advantage needs to be clearly identified, and not by a blanket stamp of "Confidential" on the entire document(s), contracts or system specifications.

Risks

If agencies do not maintain confidentiality, the perception is that suppliers may choose to abstain from their business opportunity. Similarly, agencies may be the guardians of information that is protected by privacy legislation, such as ADA client records used by paratransit software. If the vendor has access to this information, then there need be clear requirements that it be held in confidence.

Release of this information can be a large financial burden on the offending agency or contractor; some states require notification to all affected parties, as well as remediation in the form of continued account and misuse monitoring for each individual affected. Confidentiality and nondisclosure terms of both contract and ongoing licensing should not limit the ability of agencies to use the product as intended.

Benefits

- Vendors/contractors will be able to market their products to the procuring agency without fear of disclosure of confidential information to their competition, etc.
- Agencies will be protected from the consequences of divulging sensitive information covered by privacy legislation.

Common approaches

To strike a balance, some agencies will include a conditional confidentiality provision:

- Include a specific statement in RFPs that advises the vendor regarding the state's disclosure requirements. This will protect both the agency and the vendor and allow for the exchange of confidential information.
- Include a confidentiality provision in the contract; for example:

  > The AGENCY shall hold the Software, Source Code Materials, and Documentation in confidence, shall use and disclose them only as expressly authorized by the VENDOR/CONTRACTOR or as required by law and only to its employees, agents or sub-licensees to whom disclosure is necessary or appropriate for the performance and exercise of its rights hereunder, and shall take reasonable steps to ensure that unauthorized persons will have no access to them. Either party may seek an injunction to prohibit actual or threatened disclosure of its confidential information.

- Include terms in both the contract and product licensing that *excludes* data transfers required by federal, state and local law from confidentiality restrictions. For example, confidentiality restrictions should not apply to data exchange mandated by IT architecture requirements.
- Include language in the Ownership and Use of Data clause that prevent the vendor from using confidentiality as an excuse to limit the agency's use of its own data.

Either party may seek an injunction to prohibit actual or threatened disclosure of its confidential information.

See also **Source Code Escrow** and **Ownership and Use of Data**.

Current Information Technology Infrastructure

Discussion

Often IT procurements must fit into and interact with a pre-existing agency environment consisting of hardware and software supplied and/or maintained by the agency and/or other vendors. A common cause of project failure is inadequate attention to the interactions between the procurement and its environment. Accordingly, RFPs, particularly for complex technology projects, should include a full description of the agency's installed and planned infrastructure in order for vendors/contractors to propose and supply compatible solutions. The description should include a detailed layout of the existing technical infrastructure including server hardware specifications, peripherals, backup software, database software, operating systems, virus protection software versions, patch levels, system versions, interface specifications, update procedures, etc. The information should include current load and space availability for additional applications. In addition, the agency's technology infrastructure evolution should be addressed, particularly with regard to how changes may impact the delivery and post-contract maintenance and support of the vendor's/contractor's product.

Also to be included in the "current" list should be all projects or plans for the foreseeable future that may impact the procurement. This can include a companywide move to a new database platform that is not supported by the procured device/service, the upgrade of the environment to Windows 7 from XP, or a decision to remain on Microsoft Office 2007 indefinitely.

Risks

Vendors/contractors may bid incompatible products. The agency may not anticipate issues arising from unanticipated incompatibility of its own systems. Design documents will be built based on the current state of the technology infrastructure. If it is known that changes to the infrastructure will occur prior to implementation and these changes are not communicated or documented, then it's highly likely that integration issues will arise that will impact budget and schedule. A common example would be impacts to required interfaces to other systems that are scheduled to be upgraded or replaced.

Benefits

Providing documentation of the agency's current technology infrastructure ensures that vendor/contractors are able to adhere to the technology standards and propose accurately by decreasing assumptions on available supporting infrastructure. The documentation should clearly highlight the interfaces necessary for the project. An information technology infrastructure document will help flush out all relevant requirements and prevent the need to purchase additional hardware, software or customizations after an award has been made.

As a side benefit, some agencies have not taken the time to describe their own environment. Doing so is a very good start on developing an IT architecture plan.

Common approaches

- Provide information systems standards document.
- Provide network configuration document.
- Provide interface document.

See also **Compliance Matrix**; **Security**; and **End of Life Cycle**.

Customizations

Discussion

Some agencies prefer to have software customized to meet their business rules. Many agencies are moving away from substantially customized or "one-off" applications. An agency should consider whether it is better to alter business rules and use commercial off-the-shelf (COTS) software or to require customizations. Agencies should fully assess all resources and costs associated with maintaining and supporting a customized application over its life cycle.

Agencies sometimes consider contracting customizations as a service contract to a third party. This may be necessary if the vendor is unable or unwilling to perform the work. However, carefully assess whether this affects licensing, ownership, and/or intellectual property of the original system.

Risks

The agency may lose functionality of a customization if it is not practical or cost-effective to maintain. Maintenance of customizations may make the agency dependent on the vendor/contractor over long periods of time, thus driving up the cost of ownership. A vendor may not include installed customizations with upgrades to its generic product. Customizations add to the total cost of ownership over the life cycle of the system due to the maintenance involved when updates take place.

Contracting customizations of installed software to a third party can be risky. It may cause conflict with the original vendor/contractor, may break the software without recourse, and may affect the original software upgrade path.

Since customizing software may also increase cost, the time for completion and the risk to the agency; a cost-benefit analysis should be considered up front to analyze this risk.

Benefits

Customizations may meet agency needs that COTS cannot. The agency will maintain functionality of customizations through upgrades.

Common approaches

- Solicitation requires vendors/contractors to specify in the Compliance Matrix whether a requirement is included or will require a customization.
- Vendors/contractors are asked to include recommended customizations in their proposals as options for the agency to consider; this information will provide the agency with a better understanding of the functionality with or without customization.
- It is unlikely that a vendor/contractor will agree to third parties working on its core software, but certain third-party customizations or interfaces may be granted if requested by the agency.

See also **Compliance Matrix**; **Change Order Process**; **Intellectual Property Rights**; **Training**, **Warranty** ; **Licenses, Ownership and Transfer**; **Economies of Scale**; and **Software Protection**.

Definitions of Words and Terms (Glossary)

Discussion

The definitions section of a commercial contract defines words and terms that are frequently used in the contract. It also provides cross-references to other definitions in the contract of the same word or term; and provides for the incorporation of these definitions in solicitations and contracts by reference. As with other aspects of public transit, IT has its own acronyms and special terms and meanings. Accordingly, including a definition section will minimize the risk of misinterpretation.

Risks

Absence of such definitions can cause different parties to interpret words and terms differently, which will lead to confusion, delay and even disputes. “Interface,” “integration,” “real-time” and “data-centric” are examples of terms that are susceptible to confusion.

Benefits

Defining terms allows the parties to have a meeting of the minds.

Common approaches

The following is some standard text to include in a glossary:

> A word or term defined in this section has the same meaning throughout the Contract, unless:
>
> - The context in which the word or term is used clearly requires a different meaning.
> - Another part, subpart or section provides a different definition for the particular part or portion of the part.
>
> If a word or term that is defined in this section is defined differently in another part, subpart or section of this regulation, the definition in:
>
> - this section includes a cross-reference to the other definitions; and
> - that part, subpart or section applies to the word or term when used in that part, subpart or section.

See also **Order of Precedence**.

Delivery and Acceptance

Discussion

For technology procurements, delivery and acceptance provisions not only help to ensure timely projects, but they are also essential for ensuring that the hardware, software or system performs in accordance with the Compliance Matrix. Many technology procurements will require the development of test scripts, performance of tests, punch lists and/or corrective measures prior to acceptance.

For hardware, delivery terms may be similar to other procurements regarding shipping expenses and transfer of title and should be clearly documented. Software and systems purchases will require project delivery plans, which are generally developed as milestones.

For hardware or COTS software, acceptance is normally evidenced by the execution of an acceptance certificate on an inspection or receiving report form or commercial shipping document/packing list. For customized solutions, acceptance will require documentation of testing results and sign-off by project team members and steering committees.

Risks

Without explicit delivery and acceptance contract clauses tailored to the technology project and commitment by the agency to enforce delivery and acceptance terms, an agency can buy technology goods and services that do not provide the outcome desired and represent a poor investment of time and money.

The following are important items to consider:

- quality assurance procedures and certification.
- responsibility for and place of acceptance.
- certificate of conformance.
- transfer of title and risk of loss.

Benefits

A formal system of acceptance helps to ensure that the agency adequately tests and inspects hardware, software and systems for compliance with the SOW that provides the desired outcome. Developing the delivery and acceptance terms during the procurement planning stage helps the agency better define what performance levels and outcomes are acceptable.

Common approaches

Technology commodity delivery terms may follow other commodity purchases, or may include installation provisions and testing prior to acceptance. Customized software, systems and services often require more generalized delivery and acceptance terms prior to contract award, with a contract modification concerning more explicit delivery terms and acceptance developed pursuant to discovery and test script development during the project.

Particularly with complex projects, agencies should consider accepting the procurement in stages. Staged acceptance can be tied into the payment schedule.

See also **Payment and Delivery Schedule** and **Training**.

Disaster Recovery/Business Continuity

Discussion

Disaster recovery (DR) is the process by which an agency resumes business after a disruptive event. The event might be a natural disaster such as an earthquake or manmade, such as malfunctioning software caused by a computer virus.

Business continuity (BC) planning provides a more comprehensive approach to making the agency can continue to operate. Often, the two terms are combined under the acronym BC/DR. Both determine how the agency will keep functioning after a disruptive event until normal facilities are restored.

It is important that all software and hardware procurements include specific provisions to address both DR and BC. It could be as simple as requiring that all existing DR and BC plans be updated to account for the newly procured equipment, or as complex has having the vendor/contractor propose a complete DR and BC solution for its specific equipment.

It is important then that an agency have specific criteria for each type of procurement as it relates to DR and BC. This should include detailed descriptions of how each of these are currently handled for existing systems, and a set expectation for future systems, including the following:

- What critical systems need to remain functional, and for how long.
- Whether battery backup or a generator will be required.
- Whether backup service is needed for data connectivity.
- What is the acceptable data loss for major outages—minutes, hours, an entire day or week?
- Does the agency require hosted systems for redundancy and uptime or possibly a dark facility?

Risks

Many agencies are prone to ignoring disaster recovery because disasters seem an unlikely event and because creating and maintaining proper DR/BC plans takes a large amount of resources, both in dollars and human capital.

Most agencies believe that they know what they have on their networks, but in reality they don’t really know how many servers they have, how they’re configured, or what applications reside on them. The agency also should ensure that it knows what services are running and what version of software or operating systems it is using. Asset management tools can help in this area, but they often fail to capture important details about software revisions and other critical items.

Agencies often manage their IT, telecommunications and radio systems separately, even though these systems interact. This makes it difficult to plan for a disaster that disrupts more than one of these systems.

Benefits

DR/BC planning ensures that mission-critical business processes and associated hardware and software are able to continue to function should a natural or manmade disaster occur. This often includes having “mirrored” equipment hosted off-site.

Common approaches

Information technology plays a pivotal role, and the BC/DR plan should focus on systems recovery. The Business and Information Technology departments should work together to determine what kind of plan is necessary and which systems and business units are most crucial to the agency. Together, they should decide which people are responsible for declaring a disruptive event and mitigating its effects. Most importantly, the plan should establish a process for locating and communicating with employees after such an event. In a catastrophic event, the plan will also need to take into account that many of those employees will have more pressing concerns than getting back to work.

Two common approaches:

- Having a “dark” backup facility so that all data and systems are replicated as near to real time as possible so only staff need to be redirected.
- Choosing a hosted model where the onus is on the vendor to provide redundant systems in the event of failure; this can also increase uptime and reduce the need for downtime for upgrades as secondary facilities can be utilized while primary resources are being maintained or upgraded.

See also **Compliance Matrix**; **Current Information Technology Infrastructure**; **Security; Software Protection**; and **Licenses, Ownership and Transfer**.

Dispute Resolution

Discussion

Technology projects are often prone to disputes because of the complexities of integrating new technologies and systems into the existing infrastructure and practices of the organization. Despite best efforts to define all performance requirements, the agency and technology vendors/contractors are often not on the same page or fail to anticipate roadblocks to project success. To avoid having these disconnects escalate into disputes that jeopardize the project, a resolution process should be included in the contract and in follow-on support/maintenance agreements. The intent of dispute resolution is to protect both parties, not just the agency. It provides a documented process that a vendor/contractor can follow to seek relief in situations where schedule and budget are being affected due to things outside the vendor's/contractor's immediate control. A common example is when the agency is unable to provide the required dedicated resources to allow the vendor/contractor to meet the proposed schedule or when critical resources are replaced requiring increased time for knowledge transfer.

Disputes can often be avoided if there is an effective Compliance Matrix, clear definition of responsibilities, a SOW and Project Schedule for the entire project team, and a good change order process. Even in the event of a dispute, these tools can make resolution both quicker and easier.

Risks

The absence of a dispute resolution process structured to resolve problems is likely to force disputes into an adversarial process, resulting in increased costs and project time. Dispute resolution processes fall into two major types:

- Adjudicative processes, such as litigation or arbitration, in which a judge, jury or arbitrator determines the outcome.
- Consensual processes, such as collaborative law, mediation, conciliation or negotiation, in which the parties attempt to reach agreement.

Benefits

A mutually acceptable dispute resolution process will be advantageous to both parties, as most disputes can be resolved at the lowest level and only disputes requiring higher level of interaction will rise upward. Both parties will be aware of the relationship and its boundaries.

Common approaches

- Give precedence in the contract and related agreements to the Compliance Matrix, SOW and Project Schedule, and terms defining responsibilities.
- Conduct the project as a team effort; do everything possible to resolve conflicts as quickly as possible and to minimize adversarial relationships.
- To deal with the unpleasant possibility of escalation, include contract provisions and project management techniques to define the following:
    - Applicable law and jurisdiction to dispute resolution (e.g., operation dispute resolution, billing dispute resolution, partnering, claims, dispute resolution board and arbitration).
    - The escalation path within the project teams and organizations for both parties.
    - A schedule for agency and vendor/contractor project teams to meet regularly throughout technology implementations to discuss perceived problems areas/threats to the project.
    - A schedule for regular communication between the agency project manager and contract administrator. (Ensure that the vendor/contractor is provided oral and written communication regarding problems prior to escalation.)
    - A personnel change process within the contract, which should be linked to deliverables, responsibilities and the overall work program and schedule.

See also **Agency/Vendor/Contractor Responsibilities**; **Compliance Matrix**; **Change Order Process**; **Payment and Delivery Schedule**; **Standards Adherence**; **Support and Maintenance**; and **Warranty** .

Economies of Scale

Discussion

Agencies purchasing technology goods and services may benefit from combining the procurement with larger systems, overbuying in anticipation of future needs, or by joining programs offered by other agencies. Including on-vehicle stop annunciators with a bus purchase is an example of a combined purchase. Including excess line capacity in a telephone PBX purchase is an example of overbuying. And participation in state-offered bulk hardware purchase without tender and federal pre-qualification programs are examples of joint programs.

Risks

- Purchase of excess capacity may be wasted because a system becomes obsolete before it is needed.
- Technology available through joint purchase programs may not have features meeting agency needs, may have a longer delivery cycle, or may not fit well with the agency's hardware and software support process.
- Rapid changes in technology may offset economies of scale with unanticipated obsolescence.

Benefits

Economies of scale can have hard cost savings, both on purchase and during life cycle, provided that risks are carefully identified and managed. Vendors/contractors often price technology components higher if they are purchased and installed separately. Softer benefits can include unanticipated or beneficial use of overpurchased components for other purposes. For example, whereas money might not be available for real-time bus arrivals on an agency Web site, if an interface is included in an AVL/MDT system purchase, arrivals information can be fed to the Web site at little cost.

Common approaches

- Check with other agencies and vendors/contractors to identify typical "system packages"; i.e., what do larger systems being purchased now typically include?
- See if technology components can be purchased as an add-on to the agency's current technology infrastructure.
- Review FTA and other agency materials, particularly federal and state ITS plans, to see what is being packaged.
- Review the agency's overall procurement program to see where technology components can or should be included.
- Use the RFI process and talk with vendors/contractors to see what is possible before preparing tenders.
- Compare life cycles of technology component(s) with those of potential larger systems, and with typical industry replacement cycles.
- Smaller agencies may find some economies by piggybacking off of larger agency procurements or other types of group procurements. See the FTA's *Best Practices Procurement Manual* (References).
- If considering purchasing through a joint program, review whether the conditions of the program are compatible with the agency's procurement. Find out from other agencies using the program what their experience has been.

See also **Current Information Technology Infrastructure**; **Customizations**; **Grant of License and Scope of Use**; **Ownership and Use of Data**; **Support and Maintenance**; and **Warranty** .

End of Life Cycle

Discussion

The life cycle of anticipated technology procurements must be estimated to establish the annualized cost of that purchase. Simply put, it is the annualized cost of the procurement that determines the agency's commitment, not the initial purchase price. Life cycle estimation for various information technologies are complex, involving technology change and the human cost of changing out technology systems, be they obsolete or otherwise. It may be harder to retrain scheduling and operations personnel on a replacement system than it is to put up with the eccentricities of an installed older system.

When technology is bundled into larger systems, the life cycles of the various components and their separability should be reviewed. For example, can mobile data terminals included in a fleet purchase be swapped out easily for newer models when they become available, or can the train control software imbedded in rail cars be replaced with newer code?

Contract language should be considered that requires the vendor/contractor to provide advance notice prior to any product retirements.

Risks

Underestimating the rapid pace of technology change can result in overestimating the annual cost of the purchase and sooner-than-expected replacement. Consider the following examples:

- Failure to identify embedded technology components of larger systems with significantly shorter life cycles—and/or failure to specify in the larger system procurement that technology components must be replaceable—will likely mean increasingly expensive and customized maintenance.
- Replacing primary system components, such as computer hardware, networks, vehicles with on-board technology, etc. may force premature issues with embedded technology; for example, forcing replacement of data interfaces and interoperability with other technology infrastructure.
- Unrealistic or missing consideration of the human effort to replace technology components, administratively and involving retraining, impact on riders, etc., can result in poor estimates of these costs as well as the cost of the technology.

Without considering the life cycle of both freestanding and embedded technology components, agencies may inadvertently jeopardize future federal and state funding given the movement toward standardized architecture requirements, such as the federal ITS standards.

Benefits

The principal benefit of considering technology life cycles in relation to their environment is to anticipate overall costs, constraints on upgrading or replacement, human resource implications and potential support and maintenance issues. Although life cycle forecasting is not a science, using it can both uncover issues and determine the magnitude of their impact on the agency budgets and operation.

Common approaches

- Make a range of life cycle and capital/operating cost estimates to determine the magnitude and sensitivity of annualized costs within the range and in the context of agency procurement budgets.
- Check with other agencies and vendors/contractors to identify typical replacement cycles and component replacement or compatibility issues.
- Use the RFI process; talk with vendors/contractors to see what is possible before preparing tenders.
- When procuring large systems with technology components, include in specifications that these are "open architecture" and include an upgrade path. Specifically try to avoid "black box" technologies and legacy code that may be close to or beyond their life cycle already.

See also **Compliance Matrix**; **Current Information Technology Infrastructure**; **Customizations**; **Economies of Scale**; **Grant of License and Scope of Use**; **Support and Maintenance**; and **Warranty** .

Grant of License and Scope of Use

Discussion

Software license agreements (SLAs), are involved in virtually every IT procurement that involves software. Licensing agreements may also apply to data owned by a vendor. The term Grant of License defines what the agency has access to, and Scope of Use defines the usage boundaries on how the agency can use the software. The terms are interdependent and can have profound implications to the licensee if detailed attention is not given during the execution of the SLA.

Risks

- Unanticipated prohibitions that prevent the agency from doing certain things when it has specific business needs in a timely manner.
- Incremental financial costs to eliminate certain restrictive language (e.g., uplift fees). This is particularly important to understand inasmuch as an intermediate (dot) release may be included, and a full or newer version release may cause the agency to have to repurchase the product.
- Vendors often will not alter their standard SLAs, especially for relatively small dollar-value purchases, and may choose not to supply the agency if material changes to the SLA are demanded.
- Watch out for any kind of restrictive language on ownership and distribution of derivative work products (okay to relinquish on the reverse engineering clauses to the licensor).

Risk can mitigated or minimized by conducting necessary due diligence prior to executing the contract and adjusting any terms or definitions as required.

Benefits

With proper due diligence up-front, the agency does not have to constantly revisit the SLA for adjustments, each with a potential to cause unfavorable financial consequences for the licensee.

Common approaches

A general best practice in formulating a licensing strategy is to always consider potential future needs and whenever possible ensure that the SLA definitions are broad enough to meet those future needs. However, be cognizant that broadening of the licensing terms will likely result in higher license fees being charged by the vendor. The following are some guidelines:

- Seek software installation and/or transfer between multiple operating systems (Windows to Linux to Unix) and multiple databases (Oracle, DB2 or any other open source database).
- Do not allow restriction of software to a specific geographical location and/or data center. These attributes may change for an agency.
- Do not restrict software usage to any one class of computers.
- Try to get the broadest language possible on the license count mechanism.
- Make sure the agency has rights to make the necessary copies for backup and archive (especially if it is taking e-delivery).
- Make sure that agency affiliates are covered under the agency license grant, if required and cost-effective.
- When license grant is meant for internal business operations, makes sure the usage guidelines are broad.
- Make sure the agency is licensing directly from the vendor/contractor who owns the intellectual property. For example, resellers typically disclaim all warranties and indemnities, and in such cases, remedies must be sought.
- Make sure that there is no restrictive language for a chosen integrator (who might have a competing software to the licensor) and that all licenses are allowed to be used by the outsourcer. (In other words, accept "use" of licensed software by a third party, not "assignment" to a third party.)
- Make sure that there is a thorough understanding of any restrictions on use of software to any particular type of business within the agency.

- Organize the agency’s SLA negotiations into two categories: business decisions and legal decisions.
- Based on the type of the software/hardware product, do some due diligence by learning from recent industry research and/or peers who have made similar purchases.

See also **Additional Business Units (Affiliated Agencies)**

; **Assignment**; **Indemnification**; **Ownership and Use of Data**; **Support and Maintenance**; and **Warranty** .

Indemnification

Discussion

Technology projects can lend themselves to the need for indemnification because of the complex nature and variables associated with technology implementations. The language of an indemnification clause should be drafted to protect each party to the fullest extent possible, while imposing liability on the negligent party. Each party should strive to be liable only for the acts or omissions of its own employees, officers, contractors or agents. Requiring either party to assume liability for work performed by the other party or its subcontractors and consultants not under its control is called “third-party liability” and not generally accepted practice when drafting these types of provisions.

Contractual indemnification involves indemnity based on the agreement of the parties. These terms typically involve a party agreeing to indemnify, defend, and hold another party harmless against a list of possible harms.

Risks

Failure to include an indemnification provision may expose either the agency or the vendor/contractor to damages or costs caused by the negligence of the other party. Each party should be careful to draft a provision that protects it from the negligence of the other party, without unduly burdening that party for liability not caused by its own acts or omissions. Generally speaking, the more stringent the indemnification against the vendor, the higher the cost to the agency.

Benefits

Indemnification provisions protect the agency from the actions of the vendor/contractor and its lower tier subcontractors’ actions, and protect the vendor/ contractor from the actions of the agency. Typically these provisions will protect the damaged party from direct costs; intangible costs (such as loss in customer goodwill) are generally not recoverable. Vendors/contractors should flow down indemnification provisions to their subcontractors.

Common approaches

Most public agencies include very broad forms of indemnification. Occasionally agencies may agree to intermediate or narrow forms of indemnification or at times agree to cross-indemnification, in which each part indemnifies the other for its own negligence.

Other approaches:

- Include a multiplier in lieu of unlimited liability.
- Include a cap on liability for vendors. The total amount of liability can vary significantly depending on the total value of the contract and the risk to the agency.

  NOTE: Most agencies do not define the triggers or events that could result in indemnity proceedings, nor do they provide threshold that would reduce the burden on the vendor/contractor.

See also **Licenses, Ownership and Transfer**; **Liquidated Damages**; and **Ownership and Use of Data**.

Infringement

Discussion

Copyright infringement (or copyright violation) is the unauthorized use of material that is covered by copyright law, in a manner that violates one of the copyright owners' exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works.

Typically, infringement applies to the software code of an IT product and to the data structures related to it. When purchasing software, the agency should do sufficient due diligence to confirm that the vendor owns the intellectual property it is selling, as well as any imbedded applications or code incorporated in those products. The vendor should provide contractual assurances that it is the legal owner of any intellectual property and indemnify the agency for any infringement claims brought against it in relation to the products purchased.

Risks

Without contractual assurances against infringement, the agency faces the following risks:

- It could be sued for intellectual property infringement for products purchased in good faith.
- It could be forced to stop using a product it purchased if it is found to be infringing on another party's rights. In this case, there may or may not be recourse available against the original vendor.

Benefits

Contractual assurances against infringement mitigate the agency's risk and ensure it is buying products from the true intellectual property owners.

Common approaches

The agency and vendor should ensure that an Intellectual Property Rights clause is in their agreement. The agency should seek indemnification for intellectual property infringement from the vendor.

See also **Confidentiality**; **Grant of License and Scope of Use**; **Intellectual Property Rights**; and **Licenses, Ownership and Transfer**.

Intellectual Property Rights

Discussion

Intellectual property rights (IPR) are legal property rights that protect creations of the mind, including copyrights, trademarks, patents, trade secrets and related rights. Such rights may be granted for a variety of intangible properties, such as musical, literary and artistic works; ideas, discoveries and inventions; and words, phrases, symbols and designs. These concepts are commonly used to protect particular software programs designed by vendors. Under intellectual property law, the holder of one of these abstract properties has certain exclusive rights related to the creative work, commercial symbol or invention.

Typically, IPR applies to the software code of an information technology product and to the data structures related to it. In many IT-related software implementations, the product for which the vendor has IPR is improved, enhanced or put to a new use to address agency specific situations. Unless the parties specifically address the ownership of this new product within the written agreement, disputes may arise over who has claim to the “new” IPR.

Risks

Without agreement on IPR, the agency could lose the ownership and potential financial opportunity for new features or uses created and paid for by the agency. Also, other public agencies may be charged for products that could fall under the public domain and benefit multiple transit providers. Finally, the vendor could lose control over its product and/or jeopardize successful implementation of the procurement by being overly protective of IPR.

Benefits

If the IPR of new features and uses is addressed in the written agreement, then both the agency and vendor can benefit. Generally speaking, agencies have no interest in competing with their vendors, but an agency may negotiate royalties for the sale of new features or product uses it designed and paid for. This allows the agency to offset its original design costs and allows the vendor to successfully market the new product enhancements.

Common approaches

The agency and vendor should ensure that an Intellectual Property Rights clause is contained in their agreement. The terms should address who—the agency, the vendor/contractor or both—has rights to the thoughts, enhancements and new uses created by the project.

See also **Compliance Matrix**; **Confidentiality**; **Grant of License and Scope of Use**; and **Licenses, Ownership and Transfer**.

Licenses, Ownership and Transfer

Discussion

This is one of the most important contract clauses for IT software acquisitions. There are two aspects of this clause:

- **Licenses,** which deals with the type and numbers of licenses that are granted by the licensee.
- **Ownership and transfer,** which deal with the assignment of licenses.

Each licensor structures its licensing method based on the best possible financial gain. In addition, vendors/contractors constantly evaluate industry changes for potential gains (e.g., licenses based on single core versus dual core).

On the ownership and transfer side, the licensor tries to define the terms in the narrowest possible way. The agency has to review and understand its specific situation and, based on its specific needs, should seek the right type of licensing and not be limited to the licensor's proposal.

Risks

- Lack of license compliance exposes the agency to penalties.
- Lack of growth assumptions expose the agency to unexpected cost increases.
- Not thinking through the right type of licensing model exposes the agency to incremental costs.
- Software typically can outlive the contract, so without a License, Ownership and Transfer clause, the original contract language may be unenforceable, and use of software is limited.
- The agency may face liability for breach of license.

Benefits

Proper definition of licenses and ownership/transfer clauses enables the agency to apply the software components in a manner that is efficient, meets intended use and provides the agency a satisfactory return on investment over application life cycle.

Common approaches

There are many standard license types:

- **Application software licensing:** named licenses, concurrent licenses, enterprise license
- **Database licensing:** CPU-based license, single core, dual core, quad core, etc.

The agency should consider the following:

- The agency needs to understand the best fit for both current sizing and future growth needs. Seek acceptable growth in license without any additional fees. If the agency cannot size future growth, seek price protection toward future purchases.
- Negotiation should be on the initial license pricing.

  NOTE: Annual maintenance fees are based initial pricing, so the lower the initial base, the less expensive annual escalations.

- For large procurements, such as ERP/EAM implementation, consider phasing the purchases in parallel to implementation instead of purchasing all software at the same time. The agency needs to evaluate costs and benefits, as most of the software is discounted heavily when bundled.
- Watch for restrictive language on ownership and distribution of derivative work products.
- License transfer language should include "use of licenses by a third party while the agency still has the rights to use" instead of a straight assignment, in which case the agency loses its rights to the use of the software.
- The agency should have in place a good license monitoring and control usage that ensures compliance for vendor/contractor audits.

- Ensure that all SLA terms and conditions are honored by licensors in case of an acquisition and/or divesture.

The agency should negotiate terms such as the following:

- Assignability if the political structure of agency changes (such as mergers and acquisitions) or if third-party operates the system (such as hosted applications).
- Yearly support renewal terms.
- Vendor/contractor consequences for breach.
- Irrevocability.
- Additional license and/or maintenance costs.
- Data ownership/use and data communicability.
- Commencement, where vendors/contractors may want to install software and charge a license fee at the outset of a project. Agencies may prefer that the site assessment, system design, implementation document, training plan, test procedure document and successful installation in test environment all be delivered prior to installation and payment of license fees.

See also **Assignment**; **Change Order Process**; **Compliance Matrix**; **Economies of Scale; Grant of License and Scope of Use; Licenses, Ownership and Transfer**; **Operations**; **Support and Maintenance**; and **Warranty** .

Limitation of Liability

Discussion

Limitation of Liability provisions are designed to protect both the agency and the vendor from allocable risk. Typically these provisions allocate measurable risk among the parties based upon negligence, omission or failure to act, and remove intangible risks or costs from the agreement. Limitation of Liability provisions can be especially important to technology vendors who do not want to be exposed to items such as loss of revenue, of customers and of business goodwill as the result of implementing a new technology for an agency. At the same time, Limitation of Liability provisions will not apply when a defect or deficiency in services performed or materials furnished by a vendor results from the willful misconduct of the vendor’s/contractor’s personnel.

Risks

Failure to include a Limitation of Liability provision puts both the agency and the vendor at risk of incurring unreasonable costs or liabilities for negligence or a failure to act. Limitation of liability provisions help to reduce the vendor’s/contractor’s risk and encourage their participation in the agency’s business opportunity. Unlimited liability provisions may cause the agency to lose a competent vendor/contractor.

Benefits

By reducing the liability of the vendor/contractor, the agency encourages vendors/contractors to offer innovative solutions to complex problems. It also reduces the cost of doing business, as the vendors/contractors do not have to protect themselves from undefined damages. At the same time, the agency can protect itself from exposure relative to the actions of its employees and officers.

Common approaches

There is a significant variability in the degree to which liability is limited for IT projects. Some liability clauses attempt to target specific circumstances from which loss or damage may arise (for example employee claims or physical damage of property). Other clauses will cap or limit liability to a specific dollar figure (e.g., one or two times contract value). The agency and vendor should work together to prepare a liability provision that reasonably balances the liability for each party based upon the uniqueness of the specific IT project.

See also **Indemnification**; **Intellectual Property Rights**; **Liquidated Damages**; and **Warranty** .

Liquidated Damages

Discussion

Liquidated damages clauses possess several contractual advantages. First, they establish some predictability involving costs so that the agency and the vendor/contractor can balance the cost of anticipated performance against the cost of a breach. In this way liquidated damages serve as a source of limited insurance for the agency and the vendor/contractor. Another contractual advantage of liquidated damages clauses is that the agency and vendor/contractor each have the opportunity to settle on a sum that is mutually agreeable, rather than leaving that decision up to the courts and adding the costs of time and legal fees.

Technology projects tend to benefit more from using retention and/or establishing a payment schedule based on staged acceptance, rather than liquidated damages. Retention- and/or performance-based payment provide an incentive for the vendor/contractor to complete the project, whereas liquidated damages are a last resort to recoup losses due to a failed project. In most cases, vendors/contractors have already included the potential costs of liquidated damages into their proposals.

Including liquidated damages does serve a political purpose in that it provides a means to demonstrate to the public that there is a course of action to recoup costs when a technology initiative has failed. Unfortunately, with the inherent complexities of technology projects, it becomes extremely difficult to prove vendor/contractor nonperformance to the extent that liquidated damages are actually collectable.

As an offset to a Liquidated Damages clause, performance incentives can be another effective tool to motivate the vendor to meet the agreed-upon scope and schedule.

Risks

Unless mitigated through the use of retention or a payment schedule based on staged acceptance, the lack of a Liquated Damages clause could put the agency at risk should the delivered services/products not be performed on time or per the contract, as the agency will have few avenues of recourse with the vendor.

Benefits

Having an agreed-upon value for the work in advance ensures that the agency and the vendor/contractor are protected in the event that something goes wrong with the task.

Common approaches

- Define a value for the work to be performed in order to establish a fair damage level. Typically liquidated damages allow the agency to collect from the vendor the costs associated with completing the project in-house or with a replacement vendor/contractor.
- Require the vendor to disclose if liquidated damages have been paid on other contracts.

See also **Indemnification**; **Intellectual Property Rights**; **Limitation of Liability**; and **Warranty** .

Operations

Discussion

This clause primarily relates to outsourced contracts/agreements. The questions that need to be addressed in the instrument include responsibility for the following:

- Determining operations/production schedule requirements.
- Initiating/starting each application.
- Monitoring that each application successfully completes operation.
- Resolving the cause of abnormal application terminations.
- Making updates and changes to operational run books.
- Restarting applications that have not successfully completed operations.
- Monitoring that required application interfaces are operational.
- Monitoring that required application data are available when needed.
- Communicating with the application business owner regarding problems.
- Reviewing output of applications to ensure that correct processing occurred.
- Predicting changes to the business operation, including increases or decreases in workload.
- Designing hardware/software changes to accommodate changes in workload.
- Scheduling changes in the data center.
- Ensuring that data center change control practices are followed.
- Authorizing user access to application and datasets.
- Implementing authorized access to applications and dataset.
- Ensuring the physical security (access, fire, UPS, etc.) of the data center.

In addition, this section should address who is responsible (both operationally and financially) for the utilities required to operate the data center; who will be responsible for the electronic distribution of software to the agency or other end users' desktop systems; what the required hours of data center operations are; who is the appropriate party to contact when interfaces/data are not available when required by the application; and who defines data center change control practices, including how hardware and software changes will be implemented.

Risks

When outsourcing technology services, most agencies focus on finding the right company for the job. While this is important, there are bigger issues to address. With concerns like increasing computer crimes and the growing need for agency control over business practices and protection of information, the real focus should first be on whether or not outsourcing technology services is even a viable option given the associated security risks.

Whether the agency is hiring a third party for desktop support, security testing or network monitoring, the more eyes and hands the agency has on its electronic assets, the greater the risk of something unfortunate happening. The potential for loss increases given the seemingly endless amount of data stored on so many different computers.

Benefits

Benefits of outsourcing typically lie in the fact that either the agency does not have the right resources or for some reason does not want to obtain the resources for reasons of funding, program life or changing business environment.

Common approaches

Effective work performance under management or operating contracts usually involves high levels of expertise and continuity of operations and personnel. Because of program requirements and the unique nature of the work performed under management or operating contracts, the agency is often limited in its ability to effect competition or to replace a vendor/contractor. In order to derive full benefits of outsourcing and effective operational results, the agency should take extraordinary steps before award to assure itself that the prospective vendor's/contractor's technical and managerial capacity are sufficient, that organizational conflicts of interest are adequately covered, and that the contract will grant the agency broad and continuing rights to involve itself, if necessary, in technical and managerial decision making concerning performance.

The agency should review each management and operating contract, following agency procedures, at appropriate intervals. The review should determine whether meaningful improvement in performance or cost might reasonably be achieved. Any extension or renewal of an operating and management contract should be authorized at a level within the agency no lower than the level at which the original contract was authorized.

Replacement of an incumbent contractor is usually based largely upon expectation of meaningful improvement in performance or cost. Therefore, when reviewing vendor/contractor performance, the agency should consider the following:

- The incumbent vendor's/contractor's overall performance, specifically including technical, administrative and cost performance.
- The potential impact of a change in vendors/contractors on program needs, including safety, national defense and mobilization considerations.
- Whether it is likely that qualified vendors/contractors will compete for the contract.

A sample approach is illustrated by the following sample provisions:

> In addition to the rights and obligations stated elsewhere in this Contract, AGENCY shall have the following rights with respect to oversight and monitoring of the VENDOR'S/CONTRACTOR'S performance:
>
> - Monitor the records, facilities, and equipment developed or used, and monitor personnel used, by the VENDOR/CONTRACTOR in performance of its obligations under this Contract, as well as adherence to policies and procedures. The VENDOR/CONTRACTOR shall provide the AGENCY with a summary of monthly reports documenting any audits of employee performance, including efficiency test, performed by the VENDOR/CONTRACTOR.
> - Specify supplies and equipment to be used by the VENDOR/CONTRACTOR in providing the work, and provide the VENDOR/CONTRACTOR with any required Material Safety Data Sheets. If the VENDOR'S/CONTRACTOR'S specifications or policies for such items differ from those of the AGENCY, the AGENCY'S policy and specifications shall govern.
> - Inspect any equipment at any time, and remove from service any equipment which, in the AGENCY'S sole discretion, is in an unacceptable condition.
> - At the AGENCY'S sole discretion, direct the VENDOR/CONTRACTOR to cease work. The VENDOR/CONTRACTOR shall resume work only upon receipt of approval from the AGENCY.
> - Direct the VENDOR/CONTRACTOR to permanently remove from AGENCY property any employee for conduct, if such conduct is not in compliance with AGENCY'S Code of Conduct.

Other issues that are recommended to be included are partnering; standard work schedule; interference with operations; assignment and subcontracting; substitution of subcontractors; vendor's/contractor's authority; approvals; contract work hours; and contract administration.

See also **Path Back (Insourcing)**.

Order of Precedence

Discussion

Contracts for IT typically combine materials from a variety of sources, including agency-generated requirements; standard contract language; flow-through of federal, state and sometimes regional regulations; the vendor’s proposal; and negotiated items such as the Compliance Matrix, SOW, Project Schedule, Agency/Vendor/Contractor Responsibilities, form of license, etc.

To avoid conflict and confusion among these, it is essential to establish the order of precedence by which they will control the agreement (highest to lowest). The Order of Precedence clause defines which document is controlling if terms conflict. The agency contract, SOW and Compliance Matrix should take precedence over the vendor’s/contractor’s proposal. It is important to make sure that all documents are included in the order and that multiple conflicting orders of precedence do not exist.

Risks

Conflicts and inconsistencies among contractual documents may result in contentious issues unless an order of precedence is clearly defined. It will be difficult to hold the vendor/contractor accountable to deliverables and agency requirements without having contractual priorities defined in the Order of Precedence clause. Conversely, vendors may not be able to hold the agency to its obligations without this clause.

Whereas the Compliance Matrix, SOW and Project Schedule and definition of responsibilities should be controlling, often the vendor/contractor proposal contains terms that conflict with these. Without agreement to the contrary, the standard interpretation of documents is that the most recent documents are controlling; therefore, the vendor’s/contractor’s proposal would take precedence.

If the SOW and Compliance Matrix are not defined in the Order of Precedence as controlling, then it is difficult to hold the vendor/contractor accountable to the deliverables and agency requirements.

Benefits

Simply put, the fewer the contradictions within the contract, the lower the likelihood that disputes will arise into the project. Giving precedence to the Compliance Matrix, SOW, Project Schedule, definition of responsibilities and other terms that are specific to who does what when and what gets delivered only makes sense.

Common approaches

- Most agencies include the Order of Precedence as part of the standard terms and conditions for purchase orders and contracts.
- The Compliance Matrix, SOW and Project Schedule take precedence over all other documents.
- Whereas the agency generates the Compliance Matrix, typically the vendor drafts the initial version of the SOW and Project Schedule within general guidelines supplied by the agency. A discovery session taking place after selection can finalize these for inclusion in the contract. The session may occur during contract negotiations, or after signing (although the latter may require an amendment to the contract.

See also **Compliance Matrix**; **Dispute Resolution**; and **Payment and Delivery Schedule**.

Ownership and Use of Data

Discussion

All contracts that require data to be produced, furnished, acquired or used in meeting contract performance requirements should contain terms that delineate the respective rights and obligations of the agency and the vendor/contractor regarding the use, reproduction and disclosure of that data. Data rights clauses do not specify the type, quantity or quality of data to be delivered, but only the respective rights of the agency and the vendor/contractor regarding the use, disclosure or reproduction of the data. Consideration should be given to data accessibility, both reading from and writing to the database. Consideration also should be given to system architecture, as systems based on propriety and nonproprietary architecture may have different restrictions in terms of data usage and accessibility.

It may be beneficial for Ownership and Use of Data clause(s) to define the agency as having rights to the following data except for copyrighted works:

- Data first produced in the performance of a contract (except to the extent that the data constitute minor modifications to data that are limited-rights data or restricted computer software).
- Form, fit and function data delivered under contract.
- Data (except as may be included with restricted computer software) that constitute manuals or instructional and training material for installation, operation or routine maintenance and repair of items, components or processes delivered or furnished for use under a contract.
- All other data delivered under the contract, other than limited rights data or restricted computer software.
- Generally, rights in data provision enable the vendor/contractor to protect qualifying limited rights data and restricted computer software by withholding the data from the agency and instead delivering form, fit and function data.

Risks

- The Ownership and Use of data clause may limit the data or data intercommunication in the manner intended.
- In response to the clause, the vendor/contractor could provide a product or service without the accompanying data to maintain or upgrade the system.
- If ownership and use of data is not sufficiently defined, it may limit the agency’s choice in vendors for subsequent procurements.

Benefits

With this clause, the agency retains ownership of its data and is able to use that information in order to most effectively and efficiently run its operations.

Common approaches

- Specify in the contract any interfaces for data exchange with external systems that are required by the agency.
- Include a data rights clause to ensure that the agency can effectively utilize the equipment or service.

For contracts that do not require the development, use or delivery of items, components or processes that are intended to be acquired by or for the agency, the agency may adopt an alternate definition of limited-rights data. This alternate definition should not require that the data pertain to items, components or processes developed at private expense, but rather that the data were developed at private expense and embody a trade secret or are commercial or financial and confidential or privileged.

Any disclosure by the agency should be subject to prohibition against further use and disclosure by the recipient. The following are examples of specific purposes that may be adopted by an agency:

- Use (except for manufacture) by support service contractors.

- Use (except for manufacture) by other vendors/contractors participating in the agency's program of which the specific contract is a part.
- Emergency repair or overhaul work.

See also **Compliance Matrix**; **Confidentiality**; **Current Information Technology Infrastructure**; and **Intellectual Property Rights**.

Path Back (Insourcing)

Discussion

The purpose of a Path Back (Insourcing) clause is to give the agency the ability and the means to transition outsourced service(s) back to its control or to another provider. This process includes, but is not limited to, software, processes, services, hardware, communications, and data and records.

Risks

If the contract/agreement does not specify transition services/support to be provided by the vendor/contractor—such as durations of transition service/support, costs and applicable service levels, if any—then the agency is placed at risk to undue costs and loss of data.

In addition, the contract/agreement should specify data, property and records to be returned, whether it's the agency's or the vendor's/contractor's, as well as the timing of the return.

Benefits

A path back allows the agency to mitigate risk and control cost.

Common approaches

Some scenarios to be explicit about in the contract include the following:

- The agency owns software, documentation and other material specifically developed by the vendor/contractor for the agency. The agency also owns any modification(s) made to its materials.
- The software licensed by the vendor/contractor for the exclusive use of the agency should be licensed with assignment rights to the agency.
- Software licenses (and any other intellectual property rights) extended from the agency to vendor/contractor should remain agency's property, without charge.
- Hardware transferred or sold to the vendor/contractor should have an established price at which the agency can repurchase it, if desired.
- Hardware purchased by the vendor/contractor for the exclusive use of the agency should have an established method for determining the price at which the agency can purchase it.

See also **Operations**.

Payment and Delivery Schedule

Discussion

The work performed under the contract should be clearly defined and broken down into discrete tasks in a Statement of Work (SOW). The SOW should also include what deliverables are produced by each task or group of tasks, along with vendor, agency and any third-party responsibilities for each. A Project Schedule will determine when these tasks are planned to start and end, as well as their interdependencies.

While some technology projects are paid through monthly invoicing, or at arbitrary points in the schedule, more successful technology projects use milestone payments tied with clear acceptance procedures for each deliverable. In this case, payments are made once a milestone is delivered by vendor/contractor, or when accepted by the agency. Milestone payments tied to deliverables are also a good way to monitor performance during the project and to incent the vendor to complete the work according to the SOW and Project Schedule.

Milestones can still be useful in technology service contracts that do not involve tangible hardware/software, both as a means to break up the service into manageable pieces and to provide the agency with waypoints at which to assess performance. Service contracts that are funded out of operations should have payment schedules that are compatible with agency budget cycles so that money does not run out before the contract has expired, or remain unspent in large amounts.

The agency should be aware that project milestones established at the beginning may need to be modified during the project if numerous deliverables are tied to a milestone and the vendor/contractor has supplied some deliverables but is being unreasonably delayed in delivery of others due to the acts of the agency.

Risks

- Without a contracted Payment and Delivery Schedule, the project may be subject to scope creep.
- Lack of a payment schedule with a clear tie to *accepted* deliverables often leads to front-loaded projects in which the vendor/contractor has been paid the majority of its fee while the agency has accepted a minority of its deliverables. A vendor/contractor could be paid 80 percent of the project when only 20 percent has been completed.

Benefits

- The agency receives its expected value.
- The vendor/contractor held accountable.
- Project payments are tied directly to project progress.
- The vendor/contractor is motivated to complete work on time in a satisfactory manner.
- Minimizes payment dips.
- Discourages the agency from making last-minute change requests for work that has already been accepted and paid for.

Common approaches

Structure all aspects of the contract around the outcome desired as opposed to the process by which the work is to be performed. Performance-based contracting methods are intended to ensure that required performance quality levels are achieved and that total payment is related to the degree that outcomes achieved meet contract standards. Some thoughts:

- Describe the requirements as outcomes rather than inputs (project approach).
- Use measurable performance standards (in terms of quality, timeliness, quantity, etc.).
- Institute quality-assurance surveillance.
- Define and use fiscal reductions when results are not achieved and possibly financial incentives if performance exceeds expectations.

Some additional tools for consideration:

- milestone payments

- progress payments
- compensation schedule
- liquidated damages to recapture tangible losses
- change order process to facilitate the changing of milestones
- fiscal incentives or disincentives
- performance-based contracting

See also **Acceptance of Product**; **Agency/Vendor/Contractor Responsibilities**; **Change Order Process**; **Compliance Matrix**; **Liquidated Damages**; and **Payment and Delivery Schedule**.

Project Personnel

Discussion

The key to IT project success is a motivated, capable and stable team made up of agency and vendor personnel working together at the right levels throughout the project.

Vendors/contractors and agencies are sometimes unable or reluctant to provide the actual personnel that will be assigned to the project and instead will simply include "generic" resumes that are representative of the types of skill sets available. It may be advantageous to identify the actual agency and vendor project personnel as early as possible in the process. Some projects may also be best served by ensuring continuity of both the agency and vendor personnel throughout the project.

Risks

The success of technology procurements is influenced by the resources available to complete the required tasks, both from the vendor/contractor and the agency. The wrong people at the wrong time, without the requisite skills, may cost the agency and the vendor time, money and unacceptable results.

Staff instability on either the agency or vendor/contractor side could cost time and effort, which puts the project at risk.

Benefits

Building a strong project foundation starts with aligning the proper resources and skill sets with the proposed work effort. Engaging and keeping vendor/contractor personnel and the agency's personnel involved at the appropriate levels will build on the success and long-term return on investment of the new technology.

In some cases it is necessary to align agency subject-matter experts (SMEs) with their associated counterpart assigned by the vendor/contractor. All agency-critical resources may even be co-located to the project "war room." This is especially beneficial in reducing day-to-day distractions and sends a strong message to the agency and the vendor/contractor as to the importance and priority of the project.

Working in a collaborative environment greatly reduces the risks of missing the desired end result. It also makes system acceptance more of a formality than the nail-biting experience it tends to become when the agency resources are not fully engaged throughout the design and build process.

Common approaches

- The agency may request to meet, either in person or via conference call, with key members of the vendor's proposed project team during the selection process.
- The agency may want to negotiate the project schedule and/or adjusting certain critical tasks to allow for the best resources to become available.
- The agency should also evaluate the size of the procurement and analyze the number of personnel needed by both the agency and vendor to make the project successful. The agency also should involve eventual users of the product at the most effective stages of the project.

See also **Agency/Vendor/Contractor Responsibilities** and **Compliance Matrix**.

Records and Audit

Discussion

This clause primarily relates to outsourced contracts/agreements. The Records and Audit section provides a provision whereby the vendor's/contractor's records are subject to audit and reproduction by the agency or its authorized representative as necessary to permit evaluation and verification of any invoices, payments or claims submitted by the vendor/contractor. Vendor/contractor records include accounting records, billing, written policies and procedures, subcontract files (if applicable), original estimates, estimating work sheets, correspondence, change order files, and any other records or documents deemed necessary by the agency. In addition, records such as programming and systems documentation, operating manuals, maintenance and support records, and call center logs should also be subject to audit.

Risks

Without contract provisions for Records and Audit, the potential for erroneous billing, misinterpretation of contract requirements, improper identification of contract changes, and fraudulent utilization of funds may occur. The risk of miscommunication and false expectations may increase at a level that could impact proper contract execution.

Benefits

- Disciplines the agency to define in detail exactly what is being procured.
- Helps evaluators locate vendor/contractor compliance.
- Demonstrates that the vendor/contractor has carefully identified RFP requirements.
- Provides performance standards to hold the vendor/contractors accountable.
- Serves as an internal checklist to ensure full vendor/contractor compliance.
- Minimizes disputes by being clear about what is in and out of scope.
- Meets federal, state and regional requirements for post-project evaluation.

Common approaches

The Records and Audit section should mirror language required by the regulating and funding bodies. For example:

> These are provisions whereby the VENDOR/CONTRACTOR, its subcontractors and suppliers, shall maintain, within the United States, accurate and complete financial and employment records of its activities, sufficient to properly reflect all costs claimed to have been incurred or anticipated to be incurred in performing the contract, or related to negotiating, pricing or performing a contract change. Such records shall be subject at any reasonable time to audits by the contracting AGENCY and/or any firm of auditors appointed by the AGENCY or other authorized AGENCIES acting as agents of the AGENCY ("authorized auditors") to verify compliance with all contract requirements. Reasonable advance written notice shall be provided with a copy sent to the VENDOR'S/CONTRACTOR'S authorized representative for any audits performed at the VENDOR'S/CONTRACTOR'S and/or subcontractor's home office.

See also **Dispute Resolution** and **Payment and Delivery Schedule**.

Security

Discussion

This clause establishes a framework for incorporating security into all phases of the software/hardware acquisition process and establishes information technology security requirements for vendors/contractors who wish to respond to RFPs.

Risks

Failure to meet federal, state and industry standard requirements for data security—HIPAA, PCI DSS, GLB Act, FACTA, etc.—can leave the agency at risk for all financial responsibility relating to inadvertent or unauthorized disclosure.

Benefits

Ensures that COTS software and custom-developed software products used to perform mission-related tasks have the security features necessary to protect the agency's sensitive data in accordance with federal and state laws and regulations, as well as agency policies. Ensures that all facets of security are considered, which includes but is not limited to physical access, electronic access, long-term storage and disposal.

Common approaches

- Identify security specifications relevant to the agency's environment and the project: HIPAA, GLB Act, FACTA, CA SB-1386, Patriot Act, etc.
- Provide the vendors/contractors federal and state requirements that the agency deems applicable to the project.
- Provide vendor/contractor with the agency's security standards documentation: 128 bit encryption, Secure Socket Layer, Secure FTP, HTTPS, SNMP vulnerability, etc.
- Provide language in the contract that specifies confidentiality agreements that must be signed by vendor/contractor and all employees who will have access to the agency's data (provide actual agreements when available).
- Include requirements for the preferred or acceptable list of third-party vendors/contractors approved by the agency to provide security background checks for all individuals who will have access to the data/systems when required.
- Stipulate specific third-party software standards for data deletion from test and development systems: CyberScrub Compliance Suite, FDRERASE/OPEN, etc.
- Stipulate specific requirements for the archival and storage of all data; include media, formats and encryption standards; SQL 2005 database encryption, etc.
- Stipulate remote support options that are acceptable to the agency; VPN, Mesh, GoToMyPC, Terminal Services, etc.
- Have the vendor/contractor detail its required level of access to ancillary systems and hardware required for support and installation, including both physical access to components as well as network and security login access and any third party (long distance, or payroll systems) that the vendor/contractor may need to be added to for configuration and implementation.
- Utilize common language to encompass all bids rather than case-by-case based language for security requirements to standardized selection process.
- Define clearly the fiscal, civil and criminal liability of the vendors/contractors as it relates to the unauthorized release of data caused by the vendor's/contractor's software and/or systems and staff: repayment of lost funds, repair of damaged credit, ongoing monitoring account licenses for all affected clients, etc.

- If possible, differentiate between required elements and those that allow the vendor/contractor to be flexible with its bidding; find the cost/benefit balance between security and providing a successful solution.

  NOTE: A breach or lost data can have many indirect costs, e.g. damage of reputation and lost future business, which are not truly quantifiable when doing a cost-benefit analysis.

See also **Compliance Matrix**; **Current Information Technology Infrastructure**; **Disaster Recovery/Business Continuity**; and **End of Life Cycle**.

Site Visits

Discussion

Vendor/contractor visits to the agency site and agency visits to top vendor/contractor sites can be informative and valuable. The purpose of agency site visits is to view similar implementations and have time to discuss with others their experiences. The purpose of vendor visits to the agency is to provide an opportunity to see firsthand the environment into which the procurement will fit and to anticipate any problems or opportunities at the outset.

Make sure sufficient budget is allocated to accommodate site visits if desired.

Risks

Without a visit to the agency site, the vendor/contractor may not have a clear understanding of the agency IT infrastructure and environment for integration. Without a visit to the vendor site, the agency may not be aware of the top vendors/contractors successes, issues and failures with other clients.

Benefits

A vendor/contractor site visit will elicit questions that will lead to a more accurate proposal. The agency can solicit a deeper understanding of the software offering by seeing it in action at a similar agency. Face-to-face and direct phone/video-conference interaction with users of the software will elicit a more accurate evaluation of the software fit for the agency and vendor/contractor performance.

Common approaches

Include a travel budget for site visits. This is usually missed by the agency. Site visits can be called out in the RFP process or as early as the business case analysis. In addition to site visits, other research/investigations could include telephone and/or conference calls with both peers and vendors/contractors to gain as much information and knowledge as possible.

Agencies sometimes conduct a pre-bid information event at their site, incorporating a group session for all potential vendors with opportunities for individual follow-up.

Vendor site visits may be included in interviews, during contract negotiation, or as the first “kick-off” task in the SOW. However, the later the visit, the more likely it is to require a change order.

See also **Agency/Vendor/Contractor Responsibilities** and **Project Personnel**.

Software Protection

Discussion

Ensure that the most recent version of the software is always available to the agency. This should include frequent backups and redundancy for the online system, as well as escrow of latest source code by a neutral third party during and after installation and requirements that the vendor/contractor meet version update/security/backup/restore procedures related to the escrowed code.

Risks

- A current and complete compile plan with the necessary tools and configuration files may not be available.
- The escrowed system may not be compatible with current data structures, interfaces with external systems and/or changes that have occurred in networks, facilities and hardware.
- If catastrophic failure occurs, only stale or version incompatible software may be available.

Benefits

The agency may be protected by a Software Protection clause in the contract should the vendor/contractor fail to maintain or lose ownership of the software.

Common approaches

The agency should provide a contract provision that requires the vendor/contractor to maintain current versions of software in escrow. This should be proactively managed against future upgrades to ensure compatibility if escrowed software must be used. It may also be possible to include a “first-right-to-hire” clause that, in the event that the company goes out of business, would allow the agency to hire the required programming expertise from the company to continue to support the escrowed software.

See also **Compliance Matrix** and **Disaster Recovery/Business Continuity and Source Code Escrow**.

Source Code Escrow

Discussion

Source code escrow applies to software license agreements and means the deposit of the source code of the software into an account held by a third-party escrow agent. Escrow is typically requested by the agency to ensure survivability of the software. The software source code is released to the agency if the licensor files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.

Having access to escrowed source code does not guarantee that the agency will be able to successfully install it. Oftentimes the escrowed source code is not maintained and may not include the latest software version. Escrowed source code generally does not include any customizations that apply to the agency’s specific installation. Even if it’s possible to reinstall the escrowed software, it will be costly and may require a significant investment in time and money by the agency.

The escrowed source code may also require additional developer tools and software to be usable such as software specific compilers and various plug-ins.

Risks

- Without this contract provision, if a catastrophic failure occurs, only stale or version-incompatible software may be available.
- The agency should conduct analysis of the costs to escrow the source code relative to total project costs to determine whether escrowing the source code is in the agency’s best interest.

Benefits

With a Source Code Escrow clause, the agency is protected should the vendor/contractor fail to maintain or lose ownership of the software or if a smaller customized vendor goes out of business.

Common approaches

The agency should provide a contract provision that requires the vendor/contractor to maintain current versions of software in escrow. This should be proactively managed against future upgrades to ensure compatibility if escrowed software must be used. It may also be possible to include a first-right-to-hire clause that, in the event that the company goes out of business, would allow the agency to hire the required programming expertise from the company to continue to support the escrowed software.

See also **Licenses, Ownership and Transfer**.

Standards Adherence

Discussion

Technology procurements have unique standards adherence considerations. Technology standards include the following:

- Federal standards for information technology including TCIP, National IT Architecture, HIPAA and PCI DSS.
- State and regional standards, including state information technology plans.
- Industry and other technology standards.
- Funding and procurement standards and requirements.

Due to the volume of standards, it is important that the agency identify and focus on those standards that it deems critical (i.e. those that could impact funding).

Risks

Nonadherence could:

- jeopardize federal/state funding;
- trigger complicated post-procurement audits and evaluations;
- cause unforeseen problems with inter/intra agency systems interaction; and
- force costly future technology procurements to mitigate noncompliant products and systems.

Benefits

- Clearly specifies requirements for the vendor.
- Ensures compliance with necessary federal or state mandates.
- Helps future funding and procurements by establishing agency reputation.

Common approaches

- Ask other agencies that have procured similar systems, funding agencies for the project, and the regional transportation authority for a list of relevant standards. Particularly check against the agency’s IT architecture plan.
- Ask vendors of the product for their advice on what standards apply
- If the procurement is particularly large and/or complicated, consider obtaining expert advice. Certain IT, such as telecommunications, will have well-established standardization.
- From a definition of what data the procured system will use or produce, work backward to what standards apply. For example, automated financial transaction standards will apply if the system delivers automated (Web or interactive voice response) transit pass purchasing.

See also **Compliance Matrix**; **Current Information Technology Infrastructure**; **Ownership and Use of Data**; and **Standards Adherence**.

Support and Maintenance

Discussion

A Support and Maintenance clause provides the agreement for issue resolution and performance improvement following implementation. Particularly with complex applications involving interdependency with other agency systems, make clear who is responsible for supporting what. Ensure that for a fixed period of time any hardware specifications by the vendor/contractor will support any enhancements included within the agency's maintenance, or that may arise as a result of subsequent deliverables that have not been completed.

The agency needs clear definitions, including service level agreements, response times for various levels of issues, escalation procedures, and after-hours and holiday support schedules.

Risks

Without a sound maintenance agreement, the agency will lack the means to resolve performance issues. Lack of a sound maintenance agreement can create fertile ground for finger-pointing between the agency and the vendor/contractor and co-dependent third-party systems.

Maintenance agreements should take into consideration key provisions and requirements as outlined in the original contract, as the license agreement typically outlives the contract and the original contract language may be unenforceable.

Benefits

- The vendor/contractor has clear responsibility for trouble calls, fixes and upgrades to the software under defined terms.
- The agency should be able to access support and resolutions without additional fiscal investment or unnecessary downtime.

Common approaches

- Maintenance support period starts following warranty.
- Maintenance support starts after system acceptance and warranty period.

See also **Compliance Matrix** and **Current Information Technology Infrastructure** (might be unable to upgrade due to hardware requirements).

Taxes

Discussion

Although taxes appear to be standard language for commodity purchases, in the case of an information technology software procurement, taxes may not be required in some states if the software is downloaded via the Internet and no physical media is taken by the agency. This is known as e-delivery.

Risks

The obvious risk is that the agency will pay more than legally necessary for the software.

Benefits

The inverse of the risk is that the agency can save a considerable amount of money by not having to pay taxes on its purchase.

Common approaches

Vendors/contractors generally do not bring this forward, usually because they are not aware of this option. However, the agency should ensure that tax-free e-delivery, if an option within the agency’s state, is included as part of the agency’s agreement.

The agency may want to ask that taxes be included as part of the RFP so that it clearly understands the tax costs. The agency may consider having the vendor/contractor pass through any tax savings if the agency is tax-exempt.

See also **Payment and Delivery Schedule**.

Term of Agreement

Discussion

The term of contracts to purchase and install IT products is generally tied to how long it will take for installation and acceptance, although certain clauses such as indemnification survive the basic contract.

Contracts for services or operation may have terms tied specifically to what is being provided, or commonly to the operating budget cycle.

Generally, a software license is granted in perpetuity. However, all conditions of support, maintenance and updates are usually tied to annual timeframes (one year). So if the annual maintenance is not paid, then technically, from a licensor's perspective, the SLA is void without technical support and there would generally be some sort of a reinstatement period (although most software vendors/contractors will not stop the agency from using the software).

Risks

The term of an agreement of any type can have implications:

- If the term of a contract to purchase IT is too short, then extensions may push the project beyond the budgeted funding.
- Service contracts with terms that are not timed to operating budget cycles can either run out of money to pay for obligations, or leave unassigned surpluses.
- Terms for support and maintenance agreements may not be supported by funding, resulting in potential loss of warranty and support.
- Delay in the original period of performance may result in accruing incremental costs or in reinstatement costs.
- Failure to include survival clauses may result in the loss of indemnification, protection against assignment and other problems.

Benefits

A Term of Agreement clause provides assumptions to plans for resource and other capital resources.

Common approaches

- In general, make sure the term of contract provisions corresponds to funding and budget cycles. Ensure that survivability has been carefully considered.
- On the service contracts, the agreement term should be carefully developed with realistic, not aggressive, planning. Push for licensing agreements that are not affected by support/maintenance.
- The agency should do an independent assessment and use the longer of the terms for all resource and capital planning.

See also **Acceptance of Product**; **Liquidated Damages**; and **Warranty** .

Training

Discussion

Technology deployments may be unsuccessful if the agency does not receive effective training on the technology. Extremely detailed training requirements and deliverables should be included in the RFP or negotiated prior to the award of contract.

It is important that the agency and vendor are in agreement as to what will be delivered as part of the training. Things such as customized manuals, frequency of training, timing of training (from before go-live through post implementation), class size, and post-roll out/ongoing training need to be considered.

Risks

Insufficient time and or funds for training can cause project delays, or a go-live with insufficiently trained agency staff.

The agency must clearly understand its collective bargaining agreements (CBAs) relative to training. In some cases, only union jobs can provide the training. In this case, the vendor/contractor would conduct train-the-trainer type training and can only conduct classroom training if the impacted union employee is also in the training class.

Training conducted too early in the project can be forgotten come “go-live,” whereas training too little or too late can jeopardize use of the system. Training plans should also take into account potential agency staff turnover.

Benefits

Clearly defined training deliverables will ensure that adequate training is accounted for in the project schedule and budget. It will also allow for the vendor/contractor to propose correctly and for proper expectations to be set.

Common approaches

- Use train-the-trainer.
- Provide customized training manuals. Incorporate training aids within the system, and/or make it available on the vendor’s Web site.
- Use remote meeting and conferencing tools to conduct training from the vendor’s offices.
- Provide training at different stages of the project: when the generic system is installed, when the system is operational off-line with sample or real data, as the system is going online, and with over–the-shoulder support for a period thereafter.
- Include follow-up training to account for staff turnover and reinforcement.
- Web-based training using instructor-led training (ILT) and or videos where demonstrations are required.

Make sure that the agency and vendor/contractor understanding is the same regarding what constitutes training hours. Some vendors may consider time devoted to developing the training and writing instructions for agency customizations as training hours, while others may count only actual classroom or remote training.

See also **Acceptance of Product** and **Compliance Matrix**.

Warranty

Discussion

A warranty addresses the fitness or performance of the software and defines remedies in the event that the software fails to meet the stated warranty.

Risks

Without a sound warranty, the agency may lack the means to resolve performance issues. Without a sound warranty/maintenance agreement, it can create fertile ground for finger-pointing between the agency and the vendor/contractor and co-dependent third-party systems.

Benefits

- The vendor/contractor has clear responsibility for trouble calls/fixes /and for upgrades to the software under defined terms.
- The agency should be able to access support and resolutions without additional fiscal investment or unnecessary down time.

Common approaches

- Provide for a 90-day warranty following system acceptance.
- Provide for a support period that starts following the warranty.
- Support does not start until after system acceptance and warranty period.

See also **Compliance Matrix** and **Current Information Technology Infrastructure** (might be unable to upgrade due to hardware requirements).

References

American Public Transportation Association *Recommended Practices*, “Creating a Business Case for Transit Information Technology Projects and Procurements with Information Technology Components” and “Negotiating Information Technology Contracts,” both 2010.

American Public Transportation Association White Papers, “Technology Acronyms” and “Glossary of Technology Terms,” both 2010.

Federal Transit Administration, *Best Practices Procurement Manual*, November 2001. http://www.fta.dot.gov/documents/BPPM_fulltext.pdf

Abbreviation and acronyms

ADA	Americans with Disabilities Act
APTA	American Public Transportation Association
AVL	automatic vehicle location
BC	business continuity
CBA	collective bargaining agreement
COTS	commercial off-the-shelf
CWO	contract work order
DR	disaster recovery
HTTPS	Hypertext Transfer Protocol Secure
ILT	instructor-led training
IPR	intellectual property rights
IT	information technology
ITS	intelligent transportation systems
EAM	enterprise asset management
ERM	enterprise resource planning
FACTA	Fair and Accurate Credit Transaction Act
FAR	Federal Acquisition Regulations
FTA	Federal Transit Administration
FTP	File Transfer Protocol
GLB	Gramm-Leach-Bliley
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act
MDT	mobile data terminal
PCI DSS	Payment Card Industry Data Security Standard
RFI	Request for Information
RFP	Request for Proposal
SLA	software license agreement
SME	subject-matter expert
SQL	Structured Query Language
SOW	Statement of Work
TCIP	Technologies for Critical Incident Preparedness
TEA	Transportation Equity Act
VPN	virtual private network