INFORMATION TECHNOLOGY SERIES NO. 4 - SERVICES: NON-PROFESSIONAL, SUPPORT AND MAINTENANCE, CLOUD

BACKGROUND

IT services include suppliers that assess entity needs, challenges, and ways to improve systems; write software code; process data; document the existing environment; conduct system cleanup; implement new or updated systems; and migrate old systems to new. Oftentimes, support and maintenance services require consultants with very narrow fields of interest, such as cyber security, telecommunications, IT efficiency, disaster recovery, and software specific enhancements.

When procuring IT services, entities should consider a variety of factors, including:

- Focus areas of the consulting engagement, e.g., cyber security, network topography, system integration, system migration, system or program review.
- Identification of the required programming and data processing skills.
- Implementation or migration background assessment.
- The verification of supplier qualifications, e.g., consulting experience, programming experience.

The procurement professional must have a level of expertise in IT Procurement sufficient to ensure that the:

- Services or expertise procured will be appropriate to the need.
- Evaluation committee includes someone with appropriate IT expertise.

When Cloud Services are procured, supplier documentation may be limited to general descriptions of functionality. Cyber security, including data storage locations and disaster recovery features, may be described in user subscription agreements or other similar documents. The entity should consider the suitability of Cloud Solutions and the criticality of the function being automated. XaaS applications in the public cloud may be less amenable to negotiated features. XaaS solutions in private or hybrid deployments, on the other hand, better lend themselves to negotiation.

Definition

Non-Professional Services refer to assistance provided to an entity by a supplier to maximize the efficiency and effectiveness of previously purchased IT hardware and software. Examples of non-professional services include consulting, customized configurations, implementation, programming, and data processing.

Public Procurement Practice

INFORMATION TECHNOLOGY SERIES NO. 4 - SERVICES: NON-PROFESSIONAL, SUPPORT AND MAINTENANCE, CLOUD

(Cont'd)

Definition

Support and Maintenance Services refer to preventive and remedial assistance to optimize hardware and software, including consulting, installation, contract maintenance, repair, and incident support.

Support may also entail the issuance of any new releases of the software to the existing clients. Considerations when procuring support or maintenance services may include the:

- Process the supplier implements for handling technical support requests.
- Supplier's assessment of the existing systems and software.
- Supplier's cyber-security expertise and remediation and restoration plans.
- Supplier's backup plans disaster recovery capabilities.
- IT infrastructure setup and/or support by the supplier.
- Response and resolution times for repair and the hours of support provided by the supplier.
- Capacity of the supplier's support department to handle, respond to, and resolve issues.

Definition

Cloud Services refer to storing and accessing data and programs over the Internet from another provider's servers as opposed to these services being provided by entity's on-premises servers.

XaaS: Anything as a Service, for example:

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Communication as a Service (CaaS)

Element 1: Any design, code, or other modifications made by the supplier that affects operations must be communicated to the entity, i.e., knowledge transfer and training.

As consultants create or modify source code, the entity must be kept updated and receive a record of the existing environment, i.e., the current platform, application, or software, and any changes, i.e., new or modified software or hardware. Knowledge transfer, the documentation of expertise and instructions for performing tasks, is crucial as it positions the entity for future operations when the supplier is no longer there, including the training of future employees.

For cloud services, entities must be aware of update and upgrade modifications made by the supplier. These modifications can also come in the form of enhancements that change the

current environment. Before modifications are implemented, testing of data integrity and processing should be conducted in a test environment to ensure no coding errors, "bugs," or other functionality issues will occur when the modification is applied to the live environment.

Source code, the set of instructions and statements written by a programmer using a computer programming language, which act as instructions for the function of the program, is also an important consideration. Programs may contain one or more source code text files, which can be stored on a computer's hard disk, in a database, or be printed in books of code snippets. At times, entities will require software escrow accounts to ensure that the licensee can access the source code and possibly other materials if the licensor goes out of business; discontinues support of the licensed software; breaches maintenance obligations; undergoes ownership changes, e.g., sale or merger; or some other release condition occurs. Software escrow agreements are used because the licensee is dependent on the licensor for maintenance, updates, and enhancements to the software. The entity must therefore determine if there is a need for the source code to be placed in escrow.

Software escrow agreements may include:

- Licensor delivering a copy of the source code to an escrow agent.
- Escrow agent holding the source code.
- Escrow agent releasing the source code to the licensee only if a release condition occurs.
- Escrow agent returning the source code to the licensor if the term of the escrow agreement ends without the occurrence of a release condition.

Element 2: Entities should be concerned with the location of their stored data, the origin of data entering their system, and any restrictions concerning data access and overall data security.

Data security is crucial in all IT procurements as suppliers will likely have access to confidential information. How this information is handled will impact the entity's security. Both the entity and the supplier must establish policies, procedures, and physical structures to prevent, for instance, someone from walking into a data storage area and removing a drive from a device or from simply transferring data to a flash drive and walking away. Considerations include:

- Compliance with the entity's data security requirements.
- Protection from "Ransomware" attacks.
- Payment Card Industry (PCI) compliance, i.e., credit card information.
- Determining equipment disposal requirements and standards to protect against data loss.
- Determining how security breaches or incidents will be handled and reported.
- Determining responsibility for securing supplier systems stored at the entity's site.
- Determining the appropriate insurance limits of liability and coverage.
- Determining the steps necessary to ensure supplier compliance with policies, laws, and regulations concerning data security, e.g., security practices questionnaire.
- Determining the suitability of the supplier's virtual and physical storage security.
- Establishing data triage procedures in the event problems are encountered.
- Establishing the right to audit and how often your entity should perform independent supplier security reviews, assessments, or audits.
- Geographical restrictions on data downloads and IT work must be understood and agreed to in advance. For instance, can the entity's data leave the state or province? Can the data leave the nation or the continent? This is important if the supplier has employees around the world and your rules limit or restrict data downloads to persons living within a specific boundary.

Public Procurement Practice

INFORMATION TECHNOLOGY SERIES NO. 4 - SERVICES: NON-PROFESSIONAL, SUPPORT AND MAINTENANCE, CLOUD

(Cont'd)

Element 3: Cyber security should be considered at every point where data is being accessed or transferred.

Not only must the entity's cyber security be robust, the supplier's cyber security must also ensure the protection of the entity's systems. Considerations include:

- Anti-virus protection methods.
- Determining how incidents will be handled and reported.
- Determining how to limit data-sharing.
- Determining how to manage risks from the supplier's subcontractors.
- Determining if the supplier limited their liability through their standard terms and conditions.
- Determining the appropriate insurance and coverage level.
- Determining encryption requirements.
- Determining protection from ransomware attacks and responses thereto.
- Ensuring compliance with applicable policies, laws, and regulations.
- Ensuring the right to audit the supplier's security arrangements.
- Establishing non-disclosure agreements for the supplier and their subcontractors.
- Establishing non-sharing standards for entity data.
- Establishing password requirements including two-factor authentication for the supplier to access data.
- Establishing systems segregation so that entity data is not stored with data from other entities.
- Establishing the schedule for independent supplier security reviews and assessments.
- Establishing the activity schedule, i.e., when the supplier is supposed to be active in the system.
- File sharing limitations and requirements.
- Firewall requirements.
- Geographical location of supplier staff and any limitations or restrictions imposed by the entity.
- The entity's security standards statements that the supplier must meet.

Element 4: When considering responsibility, the supplier's qualifications, capacity, and capability of internal resources should be considered in view of data and information security as well as the desired outcomes.

Responsibility determinations are an important part of guarding the entity's interests by ensuring awards are made to suppliers that can meet the entity's desired outcomes. When determining a supplier's responsibility, the entity should consider the supplier staff's technical skills and certifications. Considerations may include:

- Company partnership levels, e.g., Oracle, Microsoft.
- Legal or financial issues.
- Internal security practices.
- Comprehensive information security policies and disaster recovery plans.
- Performance of regular data backups and internal security audits.
- Background checks on and appropriate security clearances for the employees and consultant personnel who will have access to client data and data storage facilities.
- Knowledge of entity's security requirements.

(Cont'd)

Element 5: Disaster recovery and system redundancy should be considered.

Entities must plan for potential emergencies during the lifecycle of the hardware, software, and data. Disaster recovery plans need to be in place prior to any emergencies and should include system redundancy, preferably in multiple locations. Considerations include:

- Physical security needs at data storage centers whether at the entity or at a supplier's location, including failover or redundant locations, i.e., multiple backup servers to which the data is instantly transferred.
- The strategic placement of the redundancy locations.
- Anti-virus protection methods.
- Firewall requirements.
- Systems segregation.
- Supplier plans for disaster recovery and business continuity.
- Encryption requirements.
- Source code and if an escrow account is needed or already exists.
- Regular data backups, i.e., how often, to what extent, and to where.
- Assignment clauses in the agreement.
- Site visits and security checks of the redundant locations.

Summary

The entity should use special expertise and templates developed for IT Technology including consulting, support and maintenance, and cloud services. Data security is critical, and the procurement professional must take all reasonable steps to protect the entity's data from misuse, unauthorized disclosure, and other issues such as viruses, worms, and ransomware. The procurement professional should leverage the expertise of IT professionals to take the highly technical information inherent in IT procurements and communicate it clearly and effectively in solicitations, negotiations, and contracts. The type of services covered in this practice are often required to keep the previously purchased IT commodities functioning at optimal levels.