CONTRACT MANAGEMENT E-CONTRACT AND DIGITAL SIGNATURES

WHAT IS CONTRACT MANAGEMENT?

Contract management is the process that enables both parties to a contract to meet their obligations in order to deliver the objectives required from the contract. It also involves building a good working relationship between customer and provider. It continues throughout the life of a contract and involves managing proactively to anticipate future needs as well as reacting to situations that arise. The central aim of contract management is to obtain the services as agreed in the contract and achieve value for money. This means optimizing the efficiency,effectiveness and economy of the service or relationship described by the contract,balancing costs against risks and actively managing the customer–provider relationship. Contract management may also involve aiming for continuous improvement in performance over the life of the contract.

AN OVERVIEW

Contract management consists of a range of activities that are carried out together to keep the arrangement between customer and provider running smoothly. They can be broadly grouped into three areas.

Service delivery management ensures that the service is being delivered as agreed, to the required level of performance and quality.

Relationship management keeps the relationship between the two parties open and constructive, aiming to resolve or ease tensions and identify problems early.

Contract administration handles the formal governance of the contract and changes to the contract documentation.

All three areas must be managed successfully if the arrangement is to be a success: that is, if the service is to be delivered as agreed, the formal governance properly handled, and the relationship between customer and provider maintained. Although possibly handled by different figures or departments within the customer organization, the various areas of contract management should not be separated from each other, but form an integrated approach to managing service delivery, relationship and contract together.

BENEFITS OF EFFECTIVE CONTRACT MANAGEMENT

Good preparation. An accurate assessment of needs helps create a clear output-based specification. Effective evaluation procedures and selection will ensure that the contract is awarded to the right provider.

The right contract. The contract is the foundation for the relationship. It should include aspects such as allocation of risk, the quality of service required, and value for money mechanisms, as well as procedures for communication and dispute resolution.

Single business focus. Each party needs to understand the objectives and business of the other. The customer must have clear business objectives, coupled with a clear understanding of why the contract will contribute to them; the provider must also be able to achieve their objectives, including making a reasonable margin.

Service delivery management and contract administration. Effective governance will ensure that the customer gets what is agreed, to the level of quality required. The performance under the contract must be monitored to ensure that the customer continues to get value for money.

Relationship management. Mutual trust and understanding, openness,and excellent communications are as important to the success of an arrangement as the fulfillment of the formal contract terms and conditions.

Continuous improvement. Improvements in price, quality or service should be sought and, where possible, built into the contract terms.

People, skills and continuity. There must be people with the right interpersonal and management skills to manage these relationships on a peer-to-peer basis and at multiple levels in the organization. Clear roles and responsibilities should be defined, and continuity of key staff should be ensured as far as possible. A contract manager (or contract management team) should be designated early on in the procurement process.

Knowledge. Those involved in managing the contract must understand the business fully and know the contract documentation inside out ('intelligent customer' capability). This is essential if they are to understand the implications of problems (or opportunities) over the life of the contract.

Flexibility. Management of contracts usually requires some flexibility on both sides and a willingness to adapt the terms of the contract to reflect a rapidly changing world. Problems are bound to arise that could not be foreseen when the contract was awarded.

Change management. Contracts should be capable of change (to terms, requirements and perhaps scope) and the relationship should be strong and flexible enough to facilitate it.

Proactivity. Good contract management is not reactive, but aims to anticipate and respond to business needs of the future

CONTRACT MANAGEMENT RISKS

- Legal and Financial risks.
- Renewal of unfavorable contracts multiply cost to organization.

- Failure to review contracts and its clauses.
- Failure to notice deadlines in time.
- Disputes and Legal expenses.
- No visibility and control over contracts.
- Penalties incurred through noncompliance
- Failure of either party to fulfill the conditions of the contract.
- Inadequately administering the contracts.
- Unauthorized changes to the contract.
- Failure to meet the strategic objectives of the procurement.
- Changing scope and changing technology.
- Fraud.
- Lack of properly maintained records.
- Unethical behavior or conflicts of interests.
- Changes or absences in key personnels.

These risks are eliminated or minimized in the process of Contract management.

PROCEDURE OF CONTRACT MANAGEMENT

Contract management procedures is implemented through a customized software, which automate the process associated with establishing contracts with the parties using such programs. The system manages the termination, conclusion and renewal of contracts. Well-established contract management procedures help to synchronize service delivery and rapport with clients and other parties. They also help in the management of risks related to contract performance.

An important factor for contract management to be successful is to have procedures that are efficient. This helps an organization choose competent service providers and clearly define their requirements. Contract management procedures are intended to guarantee that, the performance of the provider and the quality of the services offered.

Procedures corroborate whether benefits anticipated from the contract are being attained and if value for monies paid is being acquired. Procedures help identify alterations needed to the contract, to cope with varying business demands. Contract management procedures have provisions allowing preparation and introduction of these changes.

Contract management procedures help in solving problems related to the operation of the contract. They help in the anticipation of issues and in dispute resolution. Procedures cover task and responsibilities of the individuals within the corporate and the service provider.

When contract management procedures are introduced into the operation, it results in the smooth operation of routine managerial and secretarial functions. If contract management procedures are implemented, the relations between the organization and contracting parties are enhanced and paves the way for future relationships.

E-CONTRACT AND DIGITAL SIGNATURES

E-contract is a contract modeled, specified, executed and deployed by a software system. E-contracts are conceptually very similar to traditional (paper based) commercial contracts. Vendors present their products, prices and terms to prospective buyers. Buyers consider their options, negotiate prices and terms (where possible), place orders and make payments. Then, the vendors deliver the purchased products. Nevertheless, because of the ways in which it differs from traditional commerce, electronic commerce raises some new and interesting technical and legal challenges.

RECOGNITION: E-CONTRACTS

Offer: The law already recognizes contracts formed using facsimile, telex and other similar technology. An agreement between parties is legally valid if it satisfies the requirements of the law regarding its formation, i.e. that the parties intended to create a contract primarily. This intention is evidenced by their compliance with 3 classical cornerstones i.e. offer, acceptance and consideration. One of the early steps in the formation of a contract lies in arriving at an agreement between the contracting parties by means of an offer and acceptance. Advertisement on website may or may not constitute an offer as offer and invitation to treat are two distinct concepts. Being an offer to unspecified person, it is probably an invitation to treat, unless a contrary intention is clearly expressed. The test is of intention whether by supplying the information, the person intends to be legally bound or not. When consumers respond through an e-mail or by filling in an online form, built into the web page, they make an Offer. The seller can accept this offer either by express confirmation or by conduct.

Acceptance: Unequivocal unconditional communication of acceptance is required to be made in terms of the offer, to create a valid e-contract. The critical issue is when acceptance takes effect, to determine where and when the contract comes into existence. The general receipt rule is that acceptance is effective when received. For contracting no conclusive rule is settled. The applicable rule of communication depends upon reasonable certainty of the message being received. When parties connect directly, without a server, they will be aware of failure or partial receipt of a message. Such party realizing the fault must request re-transmission, as acceptance is only effective when received. When there is a common server, the actual point of receipt of the acceptance is crucial in deciding the jurisdiction in which the e-contract is concluded. If the server is trusted, the postal rule may apply, if however, the server is not trusted or there is uncertainty concerning the e-mail's route, it is best not to apply the postal rule. When arrival at the server is presumed insufficient, the 'receipt at the mail box' rule is preferred.

Consideration and Performance: Contracts result only when one promise is made in exchange for something in return. This something in return is called ‘consideration’. The present rules of consideration apply to e-contracts. There is concern among consumers regarding Transitional Security over the Internet.

Liability And Damages: A party that commits breach of an agreement may face various types of liability under contract law. Due to the nature of the systems and the networks that business employ to conduct e-commerce, parties may find themselves liable for contracts which technically originated with them but, due to programming error, employee mistake or deliberate misconduct were executed, released without the actual intent or authority of the party. Sound policies dictate that parties receiving messages be able to rely on the legal expressions of the authority from the sender’s computer and this legally be able to attribute these messages to the sender. In addition to employing information security mechanisms and other controls, techniques for limiting exposure to liability include: -

1. Trading partner and legal technical arguments
2. Compliance with recognized procedures, guidelines and practices
3. Audit and control programmers and reviews
4. Technical competence and accreditation
5. Proper human resource management
6. Insurance
7. Enhance notice and disclosure mechanisms and
8. Legislation and regulation addressing relevant secure electronic commerce issuing.

EVIDENTIARY VALUE UNDER INDIAN EVIDENCE ACT

The evidentiary value of e-contracts can be well understood in the light of the following sections of Indian Evidence Act. Sections 85A, 85B, 88A, 90A and 85C deals with the presumptions as to electronic records whereas Section 65B relates to the admissibility of electronic record. The above mentioned sections can be explained as follows:

Section 85a:

As regards presumption to electronic agreements, this section is incorporated. It says that every electronic record of the nature of an agreement is concluded as soon as a digital signature is affixed to the record. Section 85A has been added in order to ensure the validity of e-contracts. But there are some restrictions as regards the presumptive value. The presumption is only valid to electronic records, electronic records that are five years old and electronic messages that fall within the ambit of Section 85B, Section 88A and Section 90A of Indian Evidence Act.

Section 85b:

Section 85B provides that the court shall presume the fact that the record in question has not been put to any kind of alteration, in case contrary has not been proved. The secure status of the record may be demanded till a specific time. The digital signature should also be presumed to have been affixed with an intention of signing and approving the electronic record. Further it has been provided that the section should not be misread so as to create any presumption relating to the integrity or authenticity of the electronic record or digital signature in question.

Section 88a:

"The court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission, but the court shall not make any presumption as to the person by whom such message was sent".

This section is self-explanatory as it purports to follow the basic rules of a valid hard-copy agreement. The words "may presume" authorize the court to use its discretionary power as regards presumption. Sections 85A and 85B contained the words "shall presume" which expressly excluded this discretionary power of the court.

Section 90a:

In case of an electronic record being five years old, if proved to be in proper custody, the court may presume that the digital signature was affixed so as to authenticate the validity of that agreement. The digital signature can also be affixed by any person authorized to do so. For the purpose of this section, electronic records are said to be in proper custody if they are in the custody of the person with whom they naturally be. An exception can be effected in case circumstances of a particular case render its origin probable.

Section 85c:

As far as a digital signature certificate is concerned, the court shall presume that the information listed in the certificate is true and correct. Inclusion of the words “shall presume” again relates to the expressed exclusion of the discretionary power of the court.

Section 65b:

Section 65B talks about admissibility of electronic records. It says that any information contained in an electronic record which is printed on a paper or stored/recorded/copied on optical/magnetic media produced by a computer shall be deemed to be a document and is admissible as evidence in any proceeding without further proof of the original, in case the following conditions are satisfied:

The computer output was produced during the period over which the computer was used regularly to store or process information by a person having lawful control over the use of the computer. In case a combination of computers, different computers or different combinations of computers are used over that period, all the computers used are deemed to be one single computer.

The information contained should have been regularly fed into the computer, during that period, in the ordinary course of activities.

The computer was operating properly during that period and if not, it would not have affected the accuracy of data entered.

DIGITAL SIGNATURES

WHAT IS A DIGITAL SIGNATURE?

A digital signature functions for electronic documents like a handwritten signature does for printed documents. The signature is an unforgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached.

A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming the signature was forged.

In other words, digital signatures enable "authentication" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

HOW IS A DIGITAL SIGNATURE USED FOR AUTHENTICATION?

Suppose A wants to send a signed message to B. He creates a message digest by using a hash function on the message. The message digest serves as a "digital fingerprint" of the message; if any part of the message is modified, the hash function returns a different result. A then encrypts the message digest with her private key. This encrypted message digest is the digital signature for the message.

A sends both the message and the digital signature to B. When B receives them, he decrypts the signature using A's public key, thus revealing the message digest. To verify the message, he then hashes the message with the same hash function Alice used and compares the result to the message digest he received from A. If they are exactly equal, B can be confident that the message did indeed come from A and has not changed since she signed it. If the message digests are not equal, the message either originated elsewhere or was altered after it was signed.

Note that using a digital signature does not encrypt the message itself. If A wants to ensure the privacy of the message, He must also encrypt it using B's public key. Then only B can read the message by decrypting it with his private key.

It is not feasible for anyone to either find a message that hashes to a given value or to find two messages that hash to the same value. If either were feasible, an intruder could attach a false message onto A's signature. Specific hash functions have been designed to have the property that finding a match is not feasible, and are therefore considered suitable for use in cryptography.

One or more Digital IDs can accompany a digital signature. If a Digital ID is present, the recipient (or a third party) can check the authenticity of the public key.

HOW LONG DO DIGITAL SIGNATURES REMAIN VALID?

Normally, a key expires after some period of time, such as one year, and a document signed with an expired key should not be accepted. However, there are many cases where it is necessary for signed documents to be regarded as legally valid for much longer than two years; long-term leases and contracts are examples. By registering the contract with a digital time-stamping service at the time it is signed, the signature can be validated even after the key expires.

If all parties to the contract keep a copy of the time-stamp, each can prove that the contract was signed with valid keys. In fact, the time-stamp can prove the validity of a contract even if one signers key gets compromised at some point after the contract was signed. Any digitally signed document can be time-stamped, assuring that the validity of the signature can be verified after the key expires.

A FEW PROVISIONS OF IT ACT 2000 RELATING TO DIGITAL SIGNATURES

Legal recognition of digital signatures (section 5). "Where any law provides that information or any other matter shall be authenticated by affixing the signature, or any document should be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by the means of digital signature affixed in such manner as may be prescribed by the Central Government."

Electronic Record (Section 2(1) (t)). "Means data, record or data generated, image or sound stored, received or sent in an electronic form, or microfilm or computer generated micro-fiche."

Legal recognition of Electronic Record (section 4). "Where any law provides that the information or any other matter shall be in writing or in typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is: (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference."

Secure Electronic Record (Section 14). "Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification."

Secure Digital Signature (Section 15). "If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was: (a) unique to the subscriber affixing it; (b) capable of identifying such subscriber; (c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature."

Certifying Authority (Section (2(1)(g)). "Means a person who has been granted a licence to issue a Digital Signature Certificate under section 24" (issuance of certificates by Controller).

Treatment of Certification Authorities (Chapter VI). "This Act authorizes the Central Government to appoint a Controller of Certifying Authorities. The duties of the Controller are listed under Chapter VI of the Act, and include exercising supervision over the activities of certification authorities and defining the duties of these certification authorities."

COSMOLEGAL SERVICES PRIVATE LIMITED

HYDERABAD- INDIA.
Email: info@cosmolegal.com
Website:www.cosmolegal.com
Call: 04040186536