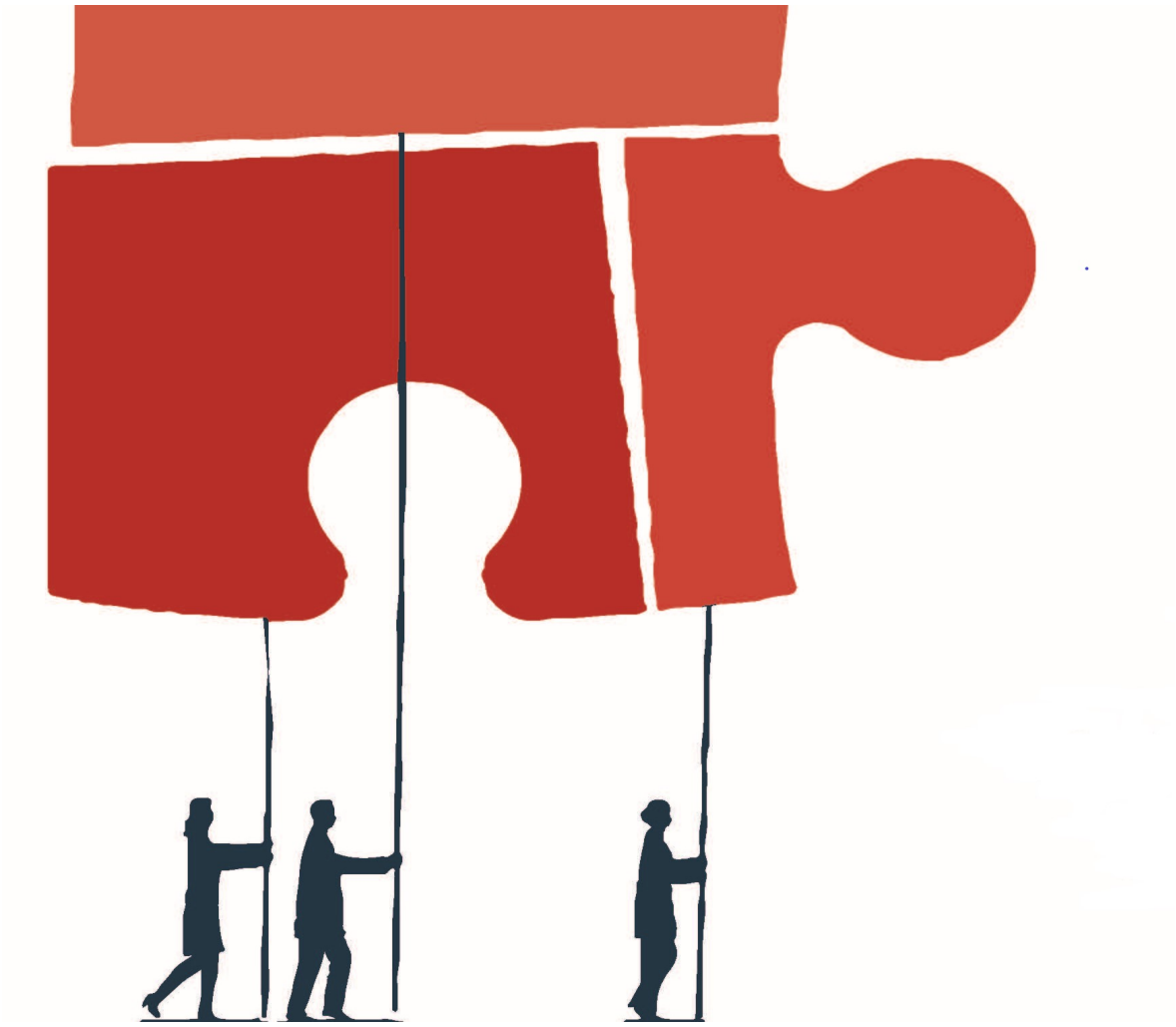
**IACCM**
90 Grove Street
Ridgefield, CT 06877
USA
T: +1 (203) 431 8741
E: info@IACCM.com



# IACCM Contracting Principles

***Text-only***

May 2019

# CONTENTS

# INTRODUCTION

These contracting principles have been developed with and are endorsed by the International Association of Contract and Commercial Management (IACCM) and are referred to as the "IACCM Contracting Principles." They are intended to serve as an industry-adopted set of guidelines to support the drafting of applicable contract clauses and/or the negotiation of applicable terms and conditions between a customer and a supplier. These principles are intended to reduce or eliminate the need for negotiation and shorten cycle time to signature. Participants who accept these IACCM Contracting Principles are free to use them on a case by case basis and as they deem appropriate; however, it is expected that the benefits of their use will be maximized when both parties to a transaction agree to rely on them and draft the relevant clauses accordingly. These principles are not intended to constitute formal legal advice.

# COMPLIANCE WITH LAWS

## A. Definitions

**"Applicable Laws"** means laws, regulations, and edicts that apply to a party's business and its activities, rights, and obligations under a contract.

## B. IACCM Contracting Principles

(i) Contracting parties already have a pre-existing, independent legal obligation to comply with Applicable Laws, regardless of what the contract says. A party should not be required to perform an express obligation in the contract if it would be prohibited under Applicable Laws.

(ii) Each party to a contract should be responsible and liable for its costs of complying with or failure to comply with Applicable Laws that relate to its business and operations, unless expressly agreed otherwise in the contract. Similarly, each party should be responsible and liable for the costs, fines and expenses associated with their respective failure to comply with their Applicable Laws and such other laws as may be agreed to under the contract.

(iii) Adding a covenant to comply with Applicable Laws relevant to either party will make it a breach of contract in the event a party fails to comply with them and can trigger certain rights and remedies as set forth in the contract if that failure damages the other party or causes the other party to violate Applicable Laws that apply to it. Depending on the materiality of the breach, remedies can include reimbursement or payment of fines, compensation for damages, and even termination of the contract.

(iv) The parties may also include references to specific laws that are relevant to a particular industry or to laws that are particularly significant or relevant to the transaction.

(v) To the extent Applicable Laws may change during the term of the contract and may have a material impact on a party's costs or performance, the contract should provide a mechanism that enables the impact of these changes to be reflected by adjustment of the contract.

(vi) A party should not be required to perform an express obligation in the contract if it would be prohibited under Applicable Laws.

## C. Applying the Principles to Contract Terms

### 1. What Applicable Laws Apply to Each Party?

(i) Each party should be obligated to comply with all Applicable Laws relating to its performance under the contract but should not be responsible for complying with Applicable Laws that apply solely to the other party unless that obligation is expressly set out in the contract.

(ii) If specific laws or regulations are more important to a contracting party because of the industry it is in or because of the specific applicability to the contracting activities, the

contract should specify compliance with those specific laws and regulations and the consequences of failing to abide by those specific laws or regulations.

## 2. Failure to Comply

(i) The consequences of a party's failure to comply with Applicable Laws should be spelled out in the contract. The party that did not comply with Applicable Laws should bear the cost of any fines or penalties (which should be deemed to be direct damages) and take reasonable steps to rectify the failure.

(ii) The party responsible for the violation of Applicable Laws should be liable only to the extent damages are attributable to the failure to comply.

## 3. Indirect and consequential damages

(i) The disclaimer of indirect and consequential damages should control on the issue of the applicability of the types of damages for which a party is responsible as a result of a violation of Applicable Laws. Therefore, the parties should specify for what damages a party that violates Applicable Laws is responsible (e.g., fines and penalties and reasonable defense costs incurred and directly attributable to the other party's violation of Applicable Laws). Reputational impacts on a party due to the violation of Applicable Laws by the other party should be deemed to be a consequential damage.

## 4. Anti-boycott laws

(i) Companies are required to comply with applicable anti-boycott laws.

(ii) For international contracts, a company should specifically address compliance with anti-boycott laws in other areas of the contract or specifically exclude in the Compliance with Laws section compliance with any laws that would conflict with US anti-boycott laws.

# CUSTOMER AUDIT OF SUPPLIERS

## A. Definitions

The following definitions apply to this IACCM Contracting Principle:

"**Financial Audit**" means investigation and examination of the supplier's financial records and other documents for the purpose of verifying amounts charged (including any price changes as stipulated in the contract) and/or credited (e.g., SLA credits).

"**Service Quality Audit**" means investigation and examination of the supplier's records for the purpose of verifying that service levels are being met.

"**Compliance Audit**" means investigation and examination of the supplier's records and/or premises for the purpose of verifying supplier's compliance with data security requirements, specific legal requirements, employee screening requirements, and/or other supplier contractual obligations (other than SLAs, which are covered by the Service Quality Audit).

## B. IACCM Contracting Principles

These general concepts form the basis for the more detailed IACCM Contracting Principles that follow:

(i) Formal audits are generally expensive (particularly if conducted by third parties such as accounting firms) and disruptive to day-to-day operations. Therefore, parties should consider more efficient ways of ensuring that the supplier is conforming to its contractual obligations (e.g., provide customer access to portals that provide service quality statistics, provide comparisons of charges in invoices and orders, and/or schedule periodic operational reviews by the parties).

(ii) Audits may be more relevant in cost-plus arrangements or in large, global deals where mission-critical operations have been outsourced. The type and extent of audit rights granted should be memorialized in the contract based upon business-to-business discussions. The scope of the customer's audit rights should be aligned with the suppliers' obligations to mitigate costs, confidentiality issues, and disruption and other burdens to the supplier.

(iii) The customer's audit rights should not require the supplier to violate its own legal or contractual obligations to third parties.

## C. Applying the Principles to Contract Terms

### 1. General Audit Principles

(i) When audit rights, whether for Financial Audits, Compliance Audits or Service Quality Audits, are agreed to by the parties, they should be subject to:

1. reasonable parameters on what can be audited;

2. requirements to provide reasonable advance notice; and

3. restrictions on frequency.

(ii) Reasonable audit parameters could include the exclusion of third party information, confidential information (unless proper protections are in place) and the supplier's highly sensitive information (e.g., detailed security measures).

(iii) Audit rights should apply during the term and any other periods during which the supplier is contractually required to maintain the records subject to audit, but audits should not be permitted to go back further in time than the period for which a remedy is permitted under the contract or under law.

(iv) Costs of an audit should be borne by the customer, unless the parties agree that the supplier should bear some pre-agreed portion of the reasonable audit costs if, for example, a Financial Audit discloses material over-billing on the part of the supplier or in the event of other material non-compliance.

(v) Where a customer needs audit rights to comply with its own corporate audit requirements, the supplier's support obligations should be specified in the agreement and should be limited to its provision of services or products that are relevant to that regulatory regime.

(vi) If faults found during audit constitute a breach of the supplier's contract obligations, they should be treated the same as any other contract breach (e.g., the supplier should be given an opportunity to cure, and the customer should be entitled to the same remedies otherwise available under the agreement).

(vii) The customer and the supplier should agree on audit methodology and on a process to jointly review audit results, give the supplier an opportunity to correct for discovered deficiencies, and to confirm when corrections are made.

(viii) If the customer requests to use third party auditors, the parties should ensure that appropriate confidentiality obligations and use restrictions are established with that third- party auditor and that the third-party auditor is not a competitor of the supplier who could gain competitive advantage through the audit. Where feasible, the entity performing the audit should be required to destroy all data gathered during the audit.

## 2. Financial Audits

(i) For Financial Audits, records should be limited to those available under the supplier's record retention policies.

(ii) The customer should not have Financial Audit rights to the supplier's subcontractors' records unless the audit cannot achieve its intended purpose in the absence of such rights.

## 3. Operational Audits

(i) Service Quality Audits intended to determine compliance with service levels generally should be limited to relevant customer-specific operational data and should not include on-site audit rights.

(ii) The parties should consider a range of alternatives to address a customer's request to confirm a supplier's compliance with data security obligations in lieu of Compliance Audits. These include but are not limited to:

1. the supplier's submittal of responses to security questionnaires,

2. supplier certifications demonstrating achievement of industry standards; or

3. provision of non-sensitive data security information, which may include summaries of internal audit reports, SSAE 16, ISAE 3402 or similar audit reports (redacted or summarized as appropriate).

(iii) Audit rights should not extend to penetration or other real-time security testing of systems or networks, given the material risks that they could adversely affect suppliers' operations and their other customers.

# DATA SECURITY AND PRIVACY

## A. Definitions

The following definitions apply to this IACCM Contracting Principle:

"**Protected Data**" means personal data (such as personally identifiable information and credit card information) and other highly sensitive data (such as passwords) of a customer or its clients that are in the possession of or accessible by the supplier. Depending on the originator, nature, and location of the data being processed, the definition of Protected Data may be modified to take into account applicable law (e.g., data subject to HIPAA, the European Data Privacy Directive, GDPR, or PIPEDA). (Other types of confidential information may be subject to contractual confidentiality obligations but are not considered Protected Data within the scope of this Principles document.)

"**Protected Data Non-Compliance**" means a failure by the supplier to comply with its obligations regarding the handling or safeguarding of Protected Data under the contract or under data protection/privacy laws or regulations applicable to the supplier.

"**Protected Data Loss**" means the accidental, unauthorised or unlawful destruction, loss, alteration or disclosure of, or access to Protected Data. (Not all Protected Data Losses result from a Protected Data Non-Compliance, such as where hacking takes place despite the supplier's good faith compliance with all applicable obligations.)

## B. IACCM Contracting Principles

These general concepts form the basis for the more detailed IACCM Contracting Principles that follow:

(i) A security environment should be designed based on the assumption that security or process failures may occur and that there needs to be multiple layers of protection to guard against Protected Data Losses.

(ii) Contract terms should reflect a balance of cost and benefit in the security environment. Customers and suppliers can more effectively reduce operational risks of Protected Data Losses by focusing on (and clearly delineating) their respective security obligations rather than by focusing solely on supplier liabilities in the event of a Protected Data Non-Compliance.

(iii) The extent to which a supplier will conform to particular industry security standards or will meet custom/more exacting requirements is a commercial issue that should be negotiated based on the size and scope of the deal (including particular security safeguards) and the nature of the solution (e.g., whether it is a standard service offering for a multi-customer environment or is a dedicated custom-built solution).

(iv) Liability for Protected Data Non-Compliance should be based on the same principles as applied for other contract breaches - liability should be based on sufficient proof of the breach, should be proportionate to fault, and should reflect a fair allocation of risk as

agreed to by the parties. In addition, each party should have an obligation to mitigate damages.

## C. Applying the Principles to Contract Terms

### 1. Scope of Protected Data Obligations

(i) Contract terms should, where possible, provide specificity with regards to the types of Protected Data being exchanged and the access, use, sharing or re-transmission (collectively, "Use") of the Protected Data by the supplier.

(ii) The supplier's data security obligations should be clearly and accurately described based on the role it will perform and should focus on functions and tasks, not outcomes.

(iii) The customer should undertake reasonable steps to safeguard their own Protected Data, such as encryption, firewalls or regular backups.

(iv) The supplier should specify the security standards to which its operations adhere by reference to specific industry standards (such as ISO 27001, PCI-DSS, etc.) or otherwise, and the supplier should provide applicable certifications upon request.

### 2. Compliance with Laws and Regulations

(i) Each party should comply with the data protection/privacy laws, regulations and mandatory industry standards (such as PCI-DSS) that apply to its own operations and activities.

(ii) The supplier's responsibilities with respect to data protection/privacy laws that apply specifically to the customer's operations and activities should be reflected as specific operational obligations rather than a general compliance with law obligation.

(iii) When appropriate, the customer's data protection/privacy compliance activities that are included in the scope of supplier's services should be clearly stated within the contract to avoid misunderstandings or gaps in responsibilities.

(iv) The contract should provide an equitable mechanism to modify the supplier's contract obligations (and charges, where appropriate) based on changes to data protection/privacy laws that have a material impact on the supplier and/or customer.

(v) The supplier should not be expected to provide the customer with independent compliance audit reports that contain highly sensitive information and are generally not created for dissemination. Rather, the parties should adopt an alternative process by which their respective experts can meet to share appropriate information to give the customer assurances relating to security controls. In cases where the customer has an obligation to provide regulators with the suppliers' compliance documentation or where laws or regulations permit regulators to audit the suppliers' compliance with security standards, the contract should address those situations and provide for appropriate safeguards for the supplier's information and operations.

## 3. Allocation of Liability for Protected Data Losses

(i) The supplier should be liable in the event of its Protected Data Non-Compliance, subject to reasonable limitations. The supplier should be accountable only for Protected Data Losses that result from its Protected Data Non-Compliance. If a Protected Data Loss results from multiple points of failure, the supplier should be held responsible only to the extent the loss is the result of its Protected Data Non- Compliance(s).

(ii) For service offerings where the supplier has only incidental access to Protected Data (e.g., business contact information for customer employees) and the risk of damages are small, the supplier's liability for a Protected Data Non-Compliance should be subject to the standard contract limitation of liability (such as a cap at a fixed dollar amount or a multiple of annual charges).

(iii) Where the supplier is operating within the customer's security environment or has significant access to Protected Data, it may be appropriate for the supplier to be subject to higher liability caps for a Protected Data Non-Compliance.

(iv) The supplier should be subject to uncapped liability for a Protected Data Non-Compliance only if there was an intentional or grossly negligent misuse or release of Protected Data by the supplier.

(v) The contract's general exclusion of indirect, consequential or other categories of damages (e.g., lost profits, revenues, goodwill) should apply in the case of Protected Data Non-Compliance. However, it may be appropriate to identify discrete categories of covered damages for which the supplier will be liable (subject to caps), such as cost of breach notifications, credit monitoring, data recovery (unless the customer's failure to back up its data in a reasonable fashion gave rise to the loss), and regulatory fines. These exclusions and covered categories of liabilities should also apply to the supplier's indemnifications for third party claims attributable to a Protected Data Non-Compliance.

# FORCE MAJEURE

## A. The IACCM Contracting Principles

(i) Performance of contract should be uninterrupted, and a supplier should have general obligations to maintain the appropriate level of contingency plans in place in order to ensure continuity of deliverables. However, either the supplier or the customer should be excused from performing their respective obligations when performance is prevented or delayed by events defined as Force Majeure. Force Majeure should allow contracts to adapt to specific circumstances that are beyond the reasonable control of a party.

(ii) Suppliers and customers should negotiate the Force Majeure clause as part of their risk allocation and in conformance with general industry practices and the level of risks in the applicable geographic areas of operations.

(iii) The generally narrow definition of Force Majeure provided by civil codes – circumstances outside the control of a party, which the party cannot prevent or overcome, and which it could not have reasonably foreseen when the contract was concluded – is a default definition that is usually adjusted by mutual agreement of the parties.

(iv) Suppliers and customers should agree upon a broader definition of Force Majeure that avoids the qualification of Force Majeure as "unforeseeable" in business and operative environments where the probability of disruptions is high and the costs to overcome them are very likely to become disproportionate with regard to the economics of the contract.

(v) The preferred approach to avoid ambiguity as to what constitutes Force Majeure is to address types of "events" that are particularly relevant to the parties or the transaction and that might not typically be classified as Force Majeure.

(vi) When notifying Force Majeure to the other party, the affected party should provide all relevant information, describing at a reasonable level of detail the circumstances and the performance that is affected.

(vii) A Force Majeure event should relieve the affected party from liability for failure to perform, with the time for completion being suspended or postponed.

(viii) To nurture close and mutually beneficial commercial relationships between suppliers and customers, the contract should focus not only on contractual relief but also on securing business continuity and disaster recovery to some reasonable extent.

(ix) The affected party should also (i) continually notify the other party while Force Majeure is ongoing, describing its plan, efforts and any timeline to resume performance to whatever extent possible, and (ii) notify the other party upon the cessation of the event of Force Majeure.

(x) Any notice of Force Majeure should conform to the notice provision of the contract, but should also go to the other party's operations contacts for them to offer their own mitigation suggestions.

(xi) If the Force Majeure event continues for a long period (as defined by the parties according to the criticality of the products or services being provided), each party should have the right to terminate the affected elements of the contract.

(xii) Generally, each party should bear its own costs arising from the Force Majeure event (which may be claimable under its insurance program).

## B. Applying the Principles to Contract Terms

### 1. Definition of Events of Force Majeure

(i) If a list of Force Majeure events is provided, the list should be clearly described as illustrative and non-exhaustive, as well as supplemented by a catch-all definition of Force Majeure, referring to any other circumstances beyond the affected party's reasonable control.

(ii) When the affected party has committed to maintain an appropriate level of contingency plans in order to ensure continuity of meeting obligations under the contract, circumstances should be considered beyond the affected party's reasonable control if and when they cannot be prevented or overcome through specific and defined measures provided for in such contingency plans.

(iii) The list of Force Majeure events should be reasonably detailed so that it is clear which risks are borne by each of the supplier and the customer.

(iv) The following are common examples of events entitling a supplier or a customer to be temporarily excused from their respective obligations:

- Acts of God, natural disasters, earthquakes, fire, explosions, floods, hurricanes, storms or other severe or extraordinary weather conditions, natural disasters,
- Sabotage, contamination, nuclear incidents, epidemics,
- War (civil or other and whether declared or not), military or other hostilities, terrorist acts or similar, riot, rebellion, insurrection, revolution, civil disturbance, or usurped authority,
- Strikes or other industrial disputes that affect an essential portion of the supplies or works, except with respect to workers under the control of the party asking for relief due to this event.

(v) The list of Force Majeure events should be more elaborated when the contract is performed in relation to business and operative environments that are unstable, and may also include, if relevant:

- Non-availability or loss of export permit or license for the products/ solutions to be delivered, or of visas/ permits for supplier's personnel,
- Requisition or compulsory acquisition by any governmental or competent authority, embargo, or other sanctions,
- Currency restrictions, shortage of transport means, general shortage of materials, restrictions on the use of or unavailability or shortage of power or other utilities.

## 2. Notice of Force Majeure

If a party wishes to be excused from performing its obligations on account of an event of Force Majeure, it should give notice of the event to the other party as soon as practically possible after its occurrence.

## 3. Rights and Obligations triggered by an Event of Force Majeure

### a) Relief

(vi) An event of Force Majeure should relieve the affected party from liability for failure to perform its obligations according to the contract, and the consequences of a Force Majeure event should be clearly stated in the contract.

(vii) The same relief should apply if an event of Force Majeure affects a subcontractor of a party.

(viii) The relief should continue for as long as the Force Majeure event prevails. The parties should also use their reasonable efforts to mitigate the effects of the event of Force Majeure upon their performance of the contract. When the supplier is the affected party, it should implement contingency plans whenever feasible, keeping operations running to a reasonable extent and with necessary adjustments (e.g., for employees' safety) or rescheduling programs for the works or deliveries.

(ix) During the period of relief, the contract should remain in force with performance thereunder temporary suspended or the affected party having the right to an extension of time for performance.

(x) The suspension or extension of time should be a reasonable period considering the ability of the affected party to resume performance and the interest of the other party to benefit from the performance in spite of the suspension or delay. The affected party should therefore resume performance as soon as reasonably practicable under the circumstances, including through other means or in another location when economically and operationally achievable.

(xi) An event of Force Majeure should not relieve a party from liability for an obligation that arose before the occurrence of that event or from obligations not affected by the event.

### b) Termination of Contract

(i) If the event of Force Majeure continues beyond a reasonable period depending on the criticality of the affected product or service delivery, or can definitively not be overcome, either party should have the right to terminate the contract, or part of it, immediately or after a reasonable notice period.

(ii) Neither party should be entitled to any compensation from the other party for costs or damages incurred as a result of a Force Majeure event. However, if the contract is terminated, the customer should pay the price of any products delivered or services completed up until the date of termination.

# INDEMNIFICATION OF THIRD-PARTY CLAIMS (EXCLUDING INTELLECTUAL PROPERTY CLAIMS)

## A. Definitions

The following definition applies to this IACCM Contracting Principle:

"**Indemnification**" means that the indemnifying party ("Indemnitor") will defend and be responsible for a claim made by a third party against the indemnified party ("Indemnitee") to the extent that the Indemnitor expressly undertook the indemnification obligation with respect to the specific acts or omissions under the agreement that gave rise to the claim.

## B. IACCM Contracting Principles

These general concepts form the basis for the more detailed IACCM Contracting Principles that follow:

(i) Although parties to a contract generally recognize that their acts or omissions under the agreement may affect third parties - particularly where a supplier is enabling a customer to provide its products or services downstream - the supplier should only be expected to step into the shoes of the customer in taking on risks that directly relate to the supplier's acts or omissions under the contract.

(ii) Third parties should not be viewed as beneficiaries of an agreement between customers and suppliers unless expressly made so in the agreement.

(iii) Customers should be expected to undertake commercially reasonable efforts to shield themselves from liability (e.g., by including appropriate flow down terms in their own agreements with their end consumers or by means of appropriate insurance) and should not look to suppliers to act as insurers in the event those efforts are not successful in warding off claims.

(iv) The agreement is not the sole vehicle by which a party can hold the other party accountable for third party claims. A party can also join the other party as a third-party defendant in litigation initiated by a third-party plaintiff.

(v) Indemnification obligations should extend only to the degree that the indemnifying party was responsible for the damages incurred. Proportionate liability should result from situations where multiple parties contributed to an event.

Supplier indemnification obligations should be tied to its own acts or omissions under the agreement as well as that of its subcontractors and agents.

(Note: Indemnification for intellectual property infringement claims is addressed in the IACCM Contracting Principle - Intellectual Property Rights and Indemnification for Third Party IP Claims.)

## C. Applying the Principles to Contract Terms

### 1. Scope of Indemnification Obligations

(i) Each party should indemnify the other for third party claims relating to (i) bodily injury, death, and real or tangible property damage due to a party's negligence or wilful misconduct; and (ii) where relevant to the services provided, employment matters brought by employees of the indemnitor against the indemnitee.

(ii) Supplier should provide indemnification for "Protected Data Losses" to the extent resulting from supplier's "Protected Data Non-Compliance" (as such terms are defined in IACCM Contracting Principles - Data Security and Privacy).

(iii) Supplier's indemnification for governmental or regulatory fines or penalties

(iv) incurred by the customer should be limited to those that are a direct result of the supplier's breach of the agreement with respect to obligations to comply with applicable laws or regulations that apply to it.

(v) Customers should indemnify suppliers for third party claims associated with the customers' business operations, data, or business content that gave rise to the claim except to the degree the suppliers' acts or omissions contributed to the damages.

(vi) The Indemnitees, which should be limited to the contracting party (and possibly also other directly related parties) should be specified in the agreement.

### 2. Applicability of Liability Caps and Exclusions from Liability for Indemnification Obligations

(i) Indemnification obligations should be subject to the same liability caps as would apply for similar claims made between the contracting parties (but see an exception under the IACCM Contracting Principle - Intellectual Property Rights and Indemnification for Third Party IP Claims).

(ii) Third party claims should be treated as direct damages regardless of their nature (but see an exception under the IACCM Contracting Principle - Data Security and Privacy).

### 3. Conditions for Indemnification

The Indemnitee should have the same obligation to mitigate third party damages as it would to mitigate its own.

Any obligation to indemnify for third party claims should be preconditioned upon the following:

(i) The extent of liability for the claim should be proportional to the fault on the part of the Indemnitor vis- -vis the Indemnitee or any other party.

(ii) The Indemnitee must give prompt notice of the claim to the Indemnitor or relieve the latter for any incremental liability caused by the delay.

(iii) The Indemnitee must provide reasonable support to the Indemnitor in defense of the claim.

(iv) The Indemnitee has the right to engage its own counsel (at its own expense) to represent it, provided that the Indemnitor maintains control of the defense of the claim.

(v) The Indemnitor cannot admit to guilt or fault on the Indemnitee's part or agree to an obligation to be undertaken by the indemnitee without the express prior written consent of the latter.

(vi) The Indemnitor cannot take any action in the course of the defense that would bring in to question the reputation or goodwill of the Indemnitee.

(vii) In the event the Indemnitee demands the right to give prior consent to any settlement of the third- party claim, the Indemnitee should accept responsibility for any additional exposure caused by its failure to give consent to any settlement proposed by the Indemnitor.

# INTELLECTUAL PROPERTY RIGHTS AND INDEMNIFICATION FOR THIRD PARTY IP CLAIMS

## A. IACCM Contracting Principles

These general concepts form the basis for the more detailed IACCM Contracting Principles that follow:

(i) Intellectual property owned by a party remains that party's property unless expressly transferred under the contract.

(ii) A party's use of and rights to another party's intellectual property must be expressly specified in the contract.

(iii) Where services are provided by a supplier, the focus of the contract with the customer should be on the services and not on the intellectual property of the underlying components that are used in the provision of the services.

(iv) The supplier should stand behind all intellectual property incorporated into the services and indemnify the customer against third party claims that relate to the services and any elements thereof, subject to appropriate limitations (see below).

## B. Applying the Principles to Contract Terms

### 1. Intellectual Property Rights

(i) Each party owns the intellectual property it creates before, during and after the contract term, except as may be specifically provided in a contract or an attachment thereto.

(ii) As between the parties to a contract, the party furnishing information or materials to the other retains its intellectual property rights in such information or materials, subject to any license rights that are granted by the furnishing party (or by a third- party licensor). Generally, where services do not contemplate software development, "work-for-hire" and similar provisions allocating ownership rights are not applicable.

(iii) The customer should have the right to use the supplier's intellectual property as necessary to use the services for the customer's business needs throughout the duration of the contract.

(iv) In circumstances where broader (or longer duration) license terms (e.g., to software or customer- specific deliverables) are appropriate, those rights should be specifically provided in the contract.

(v) As to customized unique content (such as a custom software application) that is developed for a customer's sole use in accordance with the customer's specifications, a provision granting the customer ownership or exclusive use of such content may be appropriate if the supplier is not retaining the right to re-use the content for other customers.

(vi) Third-party software, services, and equipment are provided subject to the third party's license terms.

## 2. Intellectual Property Infringement

(i) The supplier should be responsible for defending and paying/settling any third-party claim against the customer alleging that the supplier's services or products infringe the third party's intellectual property rights in any country in which the service or product is provided or where the services/deliverables are intended to be used. The supplier should not be responsible to the extent an infringement claim arises from the following ("Excluded Claims"):

1. combination of the supplier's service or product with items provided by the customer or others not under the supplier's control;

2. modification to the supplier's service or product by someone other than the supplier or others not under the supplier's control;

3. the supplier's adherence to the customer's requirements;

4. the customer's content; or

5. use of the service by the customer in breach of contract restrictions or in violation of law.

(ii) The customer should be responsible to defend and pay/settle any third-party claim against the supplier for Excluded Claims.

(iii) The obligation to indemnify for third party infringement claims should not be subject to any limitation of liability cap.

(iv) The indemnified party should have the obligation to promptly notify the indemnifying party of any such claims, and the indemnified party will not be responsible for any losses attributable to a notification delay.

(v) The indemnification of third-party claims is sufficient to protect the customer, and therefore, the supplier should not be expected to provide a warranty or representation that its services or products do not infringe third party intellectual property rights.

(vi) If the supplier's service or product infringes a third party's IP (or is subject to a claim of infringement), the supplier may:

1. obtain from the third party the right for the customer to continue its use of the service or product;

2. modify the service or product so it is not infringing without materially reducing the functionality or performance of the service; or

3. substitute another service or product having substantially the same functionality and performance criteria.

(vii) If the supplier is unable to implement any of these measures through commercially reasonable efforts, the supplier may cease providing the service or accept a return of the product that is subject to the third party claim and refund any prepaid charges or refund the current market value of the product, as the case may be.

# LIABILITY CAPS AND EXCLUSIONS FROM LIABILITY

## A. Definitions

The following definitions apply to this IACCM Contracting Principle:

"**Liability Cap**" means the monetary cap placed on a party's liability for damages arising under an agreement. Generally, the agreed upon Liability Cap will be a (i) fixed amount, (ii) percentage of charges invoiced and/or paid over a period of time under the agreement, or (iii) combination of (i) and (ii) (e.g., whichever is greater).

"**Exclusions from Liability**" means categories of damages for which a party is not contractually liable. Examples include consequential, punitive and other indirect damages that do not flow proximately from the breach. Damages such as lost profits, loss of business revenues, loss of anticipated savings, and loss of goodwill are also typically excluded.

"**Unlimited Liability**" means that the monetary Liability Cap (or, in some cases, the Exclusions from Liability) does not apply to specified breaches of the agreement or there is no Liability Cap designated for a party.

## B. IACCM Contracting Principles

These general concepts form the basis for the more detailed IACCM Contracting Principles that follow:

(i) A party's liability under an agreement should be solely related to a failure to meet obligations specified in the agreement.

(ii) A party seeking damages pursuant to an agreement has the burden of proof for the amount of those damages unless the agreement specifies liquidated damages in the particular situation.

(iii) The parties to a commercial relationship owe duties to their respective stakeholders to limit their risks and exposure to a reasonable and foreseeable degree to maintain their fiscal integrity. The Liability Cap in an agreement, typically set at a level proportional to the value of the deal, is a key way for the supplier - and even the customer - to protect itself from catastrophic financial impacts that far exceed that value.

(iv) A damaged party should have the responsibility to mitigate its damages to the extent reasonable under the circumstances. This obligation should be either pursuant to governing law or explicitly stated in the agreement.

(v) Damages caused by the contributory acts or omissions of both parties should be apportioned to both parties, and each should be liable only for those flowing from its fault (including negligence).

(vi) Exclusions from Liability are generally accepted as a standard in commercial agreements, although exceptions to those exclusions may be carved out for particular

breaches. Possible carve-outs are breach of confidentiality* (where the main damages that flow from the breach would otherwise be excluded in their entirety) and some indemnifications (where the indemnitor should be obligated to deal with the applicable claims whatever they may be).

(vii) In many jurisdictions, public policy prohibits parties from limiting their liability in certain instances where parties are expected to take full responsibility for their acts or omissions, such as bodily injury or death, or for damages proximately caused by a party's gross negligence or willful misconduct.

(viii) Liability Cap and Exclusions from Liability associated with indemnifications of third party claims are also addressed in the IACCM Contracting Principles - Indemnifications and IACCM Contracting Principles - IP. See also IACCM Contracting Principles - Data Security and Privacy.

* Data breaches are not included here and are dealt with in a separate IACCM Contracting Principle - Data Security and Privacy.

## C. Applying the Principles to Contract Terms

### 1. Reasonable Liability Caps

(i) The monetary Liability Cap in an agreement should have proportionality to the monetary value of the applicable scope, generally specified in larger transactions (perhaps over $1M in value) as the greater of a multiple of annual revenues paid (or payable) during the six or twelve months preceding a claim, or a fixed dollar amount. During the first year of the relationship, the parties may specify a revenue number based on the anticipated volume of business following any ramp- up. For smaller deals, a fixed dollar Liability Cap should suffice.

(ii) The Liability Cap may be either on a per incident basis or over a period of time (annual or life of the contract) or can be a set of co-existing Liability Caps per incident and for the time period as a whole.

(iii) Customers should not rely on a Liability Cap as a defense against supplier claims for non-payment of invoices, nor should suppliers do the same with respect to SLA credits or reversals of billing errors.

(iv) Higher Liability Caps may be warranted for certain breaches that may reasonably result in direct damages that exceed the overall Liability Cap in the agreement and where particular breach(es) would likely have a catastrophic effect on the customer and is recognized as resulting from egregious conduct by the supplier.

(v) The Liability Cap clause should survive any termination of the agreement to apply to claims raised post-termination.

### 2. Exclusions from Liability

(i) Except as set out in section 3 below, parties to the agreement should not be subject to claims for damages listed in the Exclusions from Liability clause.

(ii) Claims for payment of charges under the agreement should not be rejected by a customer by relying on a clause excluding liability for lost revenues.

(iii) The Exclusions from Liability clause should survive any termination of the agreement to apply to post-termination claims.

### 3. Exceptions to Liability Caps or Exclusions from Liability

(i) Unless the agreed upon clauses for confidentiality and indemnification for intellectual property infringement claims pose unusual risk to a party, claims for breaches of those provisions should not be subject to either the Liability Cap or the Exclusions from Liability clauses.

(ii) The liability of the parties for wilful misconduct and (if it cannot be limited under applicable law) gross negligence should not be subject to the Liability Cap or the Exclusions from Liability.

(iii) Liability for bodily injury and death and damages to real or tangible personal property (not including data) should not be subject to the Liability Cap but should be subject to the Exclusions from Liability.

(iv) Additional exceptions from Liability Caps and/or Exclusions from Liability may also be considered in specific situations (e.g., data breach subject to a separate Liability Cap, compliance with applicable laws, or compliance with tax obligations).

# SAFEGUARDING CONFIDENTIAL INFORMATION

## A. Definitions

The following definitions apply to this IACCM Contracting Principle:

1. "Confidential Information" generally means non-public information belonging to a party. (Note: As further explained in this Principle, parties will likely want to define Confidential Information with more particularity.)

2. "Discloser" means the party providing Confidential Information to a Recipient during discussions or activities associated with a Purpose.

3. "Purpose" means the specific activities to be undertaken by one or both of the parties for which or during which Confidential Information is shared.

4. "Recipient" means the party receiving Confidential Information from a Discloser.

## B. IACCM Contracting Principles

(i) If parties intend to share Confidential Information in anticipation of, or during a business relationship, it should be subject to the protections of a separate non-disclosure agreement or of a confidentiality clause within the contract documenting the relationship (perhaps entered into subsequent to the NDA).

(ii) In a typical business relationship, the determination of what information is deemed to be Confidential Information is an issue in the absence of clear markings, particularly when information is conveyed verbally or when the parties do not want impediments to the free flow of information between the parties. Accordingly, the most efficient and practical approach is to define Confidential Information as being all information, (i) that is disclosed in any form by one party to the other, or (ii) of which one party has gained knowledge from the other party as a result of carrying out the Purpose. Confidential Information should not include information that (i) has already been made public by the Discloser or a third party; (ii) is independently developed by the Recipient without reliance on the Discloser's Confidential Information; (ii) was obtained by the Recipient from a third party without restriction; or (iv) the Discloser has expressly indicated as not confidential.

(iii) The Recipient must be given the right to hand over Confidential Information pursuant to a governmental or court order, provided that the Discloser is notified as soon as reasonably possible to take action to block the order or protect the information.

(iv) A Discloser's Confidential Information should only be shared with the Recipient's employees as required for the Purpose. In the event the parties contemplate that their respective affiliates or third parties (e.g., agents, consultants, subcontractors) will be involved in furtherance of the Purpose, Confidential Information should be shared with those entities only if (i) those entities use the Confidential Information to the same extent as the Recipient may under the agreement between the Discloser and the Recipient, (ii) the Recipient ensures that those entities will comply with confidentiality obligations comparable to the ones contained in the agreement between the Discloser and the Recipient and (iii) any necessary Discloser consent has been given. In establishing

disclosure rules applicable to third parties, the parties should also address any issues if the Recipient may be sharing Confidential Information with any competitors of the Discloser or if there are any anti-trust or collusion concerns.

(v) The degree of care given by the Recipient for safeguarding a Discloser's Confidential Information should be no less than that it gives to its own similar confidential information.

(vi) The Recipient should also promptly notify the Discloser about all losses or wrongful disclosures and take measures to mitigate the effects of such events.

(vii) Violating confidentiality obligations can cause irreparable harm that goes beyond mere direct monetary damages and may include both indirect and consequential damages, loss of revenues, profits, or the like.

(viii) The duration of the confidentiality obligations should be a function of the expected period over which the Confidential Information continues to be of value to the Discloser if kept non-public. Factors to be considered include the pace at which technology is changing, whether the information is a trade secret, whether the information is expected to become stale or will likely become public at some point, and standards for the particular market segment or geography.

(ix) Parties often do not maintain corporate memory of documents that need to be returned at the end of discussions or an engagement, so a more practical approach to returning Confidential Information to the Discloser is to have the Discloser ask for the return of the information if it is of sufficient importance to take that step.

(x) The same principles relating to assignments of obligations to third parties that are typically applied in transactional agreements should also apply in NDAs.

(xi) Personal data provided by one party to another is certainly Confidential Information but should be typically treated separately and with different standards of care given the laws and regulations that apply (See IACCM Contracting Principle – Data Security and Privacy).

(xii) Ownership of intellectual property rights in Confidential Information is not transferred as a result of mere disclosure and any license given to the Recipient to use the Confidential Information, including the intellectual property right therein, is limited to activities related to the Purpose.

## C. Applying the Principles to Contract Terms

### 1. Defining Confidential Information

(i) If there is uncertainty as to the scope of Confidential Information that will be shared over the course of a relationship and one or both of the parties are reluctant to agree that all information shared is to be treated as confidential, it may be worthwhile to supplement the definition of Confidential Information with a list of examples, using the phrase "including, but not limited to, …" to provide broad categories of likely information. On the other hand, if, at the outset, specific information is expected to be shared and must be safeguarded, it is prudent to refer to them explicitly to avoid any doubt. The definition of Confidential Information should also include categories of information that will not be

deemed to be Confidential Information or that lose any protections when certain events occur (cf. Section B(2), above).

### 2. Obligations to Safeguard Confidential Information

(i) The Recipient should protect the Discloser's Confidential Information with the same degree of care and protection as it treats its own similar Confidential Information, and no less than a reasonable degree of safeguards.

(ii) To the extent the other party's Confidential Information is incorporated into documents created by the Recipient, the portions of new document containing the Confidential Information need to be protected pursuant to the non-disclosure obligations.

(iii) The confidentiality obligations should be extended to any Recipient's employees, agents, subcontractors, or other third parties to whom the Recipient is expressly authorized to disclose Confidential Information. The Recipient should be responsible for any acts or omissions (intentional or negligent) of those persons or entities if they fail to comply with the obligations as if the Recipient would have failed to comply with them.

(iv) In the event that the Recipient is subject to a governmental subpoena or request for the Discloser's Confidential Information, if the Discloser requires the Recipient's assistance in efforts to obtain protection for the Confidential Information, the Recipient should cooperate to as reasonable, at the Discloser's expense. Regardless of the outcome, the Recipient should not be expected to expose itself to penalty for violation of a legitimate order.

### 3. Duration of Obligations

The obligation to protect Confidential Information should be for a set duration (e.g., 3 or 5 years) based on a reasonable expectation of how long information of that nature remains relevant and valuable to the Discloser. Trade secrets, consumer personal information, and proprietary software source code are examples of information that warrant indefinite protection. (Note: An NDA typically has two terms: one for the period during which information will be transmitted between the parties for the Purpose, and a second for how long the information shall be treated as confidential by the Recipient(s). The latter could extend past the term of the NDA, in which case the obligations survive the agreement.)

### 4. Return of Confidential Information

(i) The Discloser should have the right to ask the Recipient for the return or destruction of its Confidential Information at any time and can ask for a certification that any destruction of both originals and copies of the Confidential Information has taken place.

(ii) At the end of any relevant activity for the Purpose, documents (paper or electronic) containing Confidential Information should, upon the request of the Discloser, be returned or destroyed. In the absence of any such request, the obligations continue until the expiration of the term of confidentiality, as specified in the agreement.

(iii) The Recipient should have the right to retain a copy of the Discloser's Confidential Information for archival or regulatory purposes as long as the storage medium has appropriate safeguards.

(iv) In the event that ownership of or license to Confidential Information or underlying intellectual property is intended to be transferred from or granted by the Discloser to the Recipient during the course of a relationship, that must be expressly defined in the applicable contract along with any conditions, limitations, and/or compensation.

## 5. Remedies for Breaches of Confidentiality

(i) Typically, stand-alone NDAs do not contain clauses that cap liability or exclude types of damages (e.g., indirect, consequential damages or lost profits) for breach of confidentiality.

(ii) With respect to confidentiality clauses contained within broader agreements, the applicability of the limitation of liability clause to a breach of confidentiality should follow generally accepted practices within a jurisdiction. Caps or exclusions on liability generally should not apply to such breaches (See IACCM Contracting Principle – Liability Caps and Exclusions from Liability).

(iii) Given that monetary damages may not be an adequate remedy for the Discloser, it should be given the right to seek equitable relief (e.g., a restraining order) from a court having proper jurisdiction. (Any language that presupposes that the Discloser is entitled to that relief detracts from the Recipient's right to oppose that relief on the basis that it is not warranted.)

## 6. Assignment

In cases where either party is allowed to assign/novate its rights and obligations under an NDA, the assignee must have the capability to meet relevant obligations. This may be more difficult in cases where the assignor retains possession and control over documents containing the Confidential Information. Any assignment in that situation should account for the transfer of those materials or limit the obligations only to Confidential Information disclosed after the effective date of the assignment.

# SLA REMEDIES

## A. Definitions

The following definitions apply to this IACCM Contracting Principle:

"**Service Level Agreement"** or "**SLA**" means the contractual quantitative standards set for service performance by the parties (e.g., response time, service quality, uptime).

"**SLA Credit**" means the credit provided by a supplier to a customer for an SLA Failure. "**SLA Failure**" means the failure of supplier to meet its obligations under an SLA.

"**Chronic SLA Failure**" means repeated or persistent SLA Failures, the occurrence of which is agreed by the parties to justify a remedy or remedies in addition to the award of SLA Credit(s), such as termination of the impacted services.

## B. IACCM Contracting Principles

These general concepts form the basis for the more detailed IACCM Contracting Principles that follow:

(i) While suppliers intend to provide high quality services, SLA Failures can occur over time given the complex nature of technology services. SLA Failures should not be deemed to rise to the level of a breach of contract.

(ii) SLAs are intended to underscore supplier's efforts to maintain the service, proactively identify potential problems, and quickly resolve any SLA Failures.

(iii) SLA targets and SLA Credits should be set at levels that drive high performance but do not create financial windfalls for customers or unreasonable financial exposure for suppliers.

(iv) SLA performance targets should be measurable and verifiable and should reflect minimum acceptable levels of supplier performance, focusing on critical service elements that are essential to the value of the service being provided.

## C. Applying the Principles to Contract Terms

(i) Suppliers should make performance reports available on a regular basis.

(ii) SLAs should take into account both the complexity and the criticality of the services.

(iii) SLA Credits should be based on quantified performance standards set out in the contract.

(iv) It should be agreed by the parties that SLA Credits are not penalties, which are not enforceable in some jurisdictions.

(v) SLA Credits should be the sole and exclusive remedy available to the customer for Service Level Failures, except for Chronic SLA Failures.

(vi) In the event of a Chronic SLA Failure, Customers should have the additional right to terminate the affected service without penalty, following executive escalation.

(vii) An SLA Failure should not be deemed to have occurred in situations where the failure is due to a customer-controlled issue or is otherwise out of the control of the supplier. Examples are when an SLA is not met due to:

- a force majeure event;
- acts or omissions on the part of customer or any other third party over which the supplier has no control;
- scheduled maintenance by the customer or entities under the customer's direction or control;
- scheduled maintenance by the supplier or its subcontractors within maintenance windows;
- lapses of service or performance issues related to non-supplier-provided and/or maintained equipment at a customer site;
- customer's use of the services in violation of the agreement, which violation caused the problem; and/or
- customer's use of non-standard products and services not approved for use by supplier.

# SUSPENSION RIGHTS

## A. Definitions

The following definition applies to this IACCM Contracting Principle:

"**Suspension**" means a temporary cessation of performance by the supplier, as permitted under a contract. (A Suspension may lead to a permanent termination if the grounds for the Suspension are not mitigated, cured or removed.)

## B. The IACCM Contracting Principles

(i) Customers should have an expectation of continual provision of the services or goods for which they contracted as long as they do not materially breach the contract. Suspension is a very serious step and should not be invoked unless all other remedies have been exhausted, including use of governance and dispute resolution principles, and exploration of creative cures for the breach. Suspension should only be considered if it is necessary under the circumstances or is a preferred alternative to contract termination.

(ii) Suspension should only be undertaken by the supplier under circumstances that are not reasonably capable of mitigation or other remedies, or when instructed by the customer (either when the supplier is in breach of its obligations or for the customer's own convenience reasons). If a customer suspends for convenience, then the customer should pay for all suspension costs and some agreed upon portion of the charges that would have otherwise been due to the supplier so that the supplier is kept whole.

(iii) Suspension rights may not be exercisable in certain situations, such as in the case of bankruptcy proceedings wherein a stay has been issued, or may not be fair to exercise during other situations, such as formal contract dispute proceedings.

(iv) The interests of both the customer and supplier should be balanced when defining the circumstances under which Suspensions are permitted under the contract, particularly when the applicable services or goods are mission critical to the customer.

(v) Causes for Suspensions should be expressly set forth in the contract and should not be left to the unlimited discretion of the supplier.

(vi) A Suspension should not come as a surprise to the customer, except in emergency situations where there is an imminent threat of harm to the supplier or others.

(vii) The duration of prior notice of a Suspension should be balanced between the reasonable time needed by the customer to prepare for the Suspension (particularly when the service or good is mission critical) with the urgent need for the supplier to avoid or eliminate damages.

(viii) A Suspension could be appropriate even if the underlying cause was outside the control of one party or the other or even of both parties.

(ix) Any notice of a Suspension should be pursuant to the notice provision of the contract but should also be to the customer's operations contacts so as to speed the customer's internal responses.

(x) Any notice should contain the specific services or goods that are suspended, clear reasons for the Suspension, and the events that would lead to performance restoration.

## C. Applying the Principles to Contract Terms

### 1. Grounds for Suspensions

(i) The following are examples of situations in which a supplier should have a right to temporarily suspend:

- Acts by a customer or its employees or agents that (i) are in material breach of the contract (including but not limited to a violation of an Acceptable Use Policy or similar contractual rules applicable to use of the service) and (ii) pose a material threat of harm to the supplier or its other customers.
- Customer's use of service or goods that is a violation of Applicable Laws (cf. separate IACCM Principles, "Compliance with Laws").
- Any customer breach of the contract for which a monetary claim is not available as a remedy to the supplier (e.g., the breach would significantly damage supplier's goodwill or reputation).
- The Suspension is ordered by a governmental or regulatory body.
- For non-payment of applicable non-disputed charges or fees, after all attempts at collection have failed.
- For potential harm to property (including supplier assets) or persons that cannot be avoided otherwise.

(ii) All potential grounds for a Suspension should be expressly set forth in the contract.

(iii) Only relevant services or goods should be suspended as a result of an enumerated breach or event. Services or goods that are not affected by or associated with the breach should not be subject to Suspension.

### 2. Notice of Suspension

(i) Except for emergency situations where the risk of harm is material and imminent or when the supplier is precluded from giving prior notice by a governmental body, the supplier should give a customer a reasonable opportunity to cure or mitigate the basis for the Suspension prior to the actual Suspension.

(ii) Where a cure is not possible or not relevant to the situation, reasonable prior written notice of the Suspension should be given. However, if there is ongoing damage to the supplier or its other customers or there is a material risk of imminent damage to any of

them, the supplier should have the right to take immediate action to suspend but should still provide written notice as quickly as possible thereafter.

### 3. Obligations During Suspensions

(i) The supplier should have the obligation to restore the suspended services or goods as soon as possible after the cause of the Suspension has been corrected or eliminated.

(ii) The customer should be obligated to continue to pay for the services or goods suspended if the Suspension was due to customer's breach of the contract. If the underlying cause was outside the control of the customer or its employees or agents, payment obligations should also be suspended for the relevant period.

(iii) If the underlying cause is outside the control of the parties, the parties should use reasonable efforts to mitigate the effects of the cause that has led to Suspension.

(iv) If the Suspension is due to a governmental or regulatory order prompted by an act or omission of the supplier, the Suspension of service should be treated as any other disruption of service caused by the supplier under the contract (e.g., pursuant to any SLA and not as a force majeure event). The supplier should have an obligation to keep the customer informed of efforts to resolve the basis for the Suspension and of the expected timeline for resolution. Customer's termination rights would remain available.

# TERMINATION ASSISTANCE

## D. Definitions

**Exit Plan**: the written disengagement or termination assistance plan agreed upon by the parties.

**Termination Assistance**: means the efforts made by a supplier, in conjunction with the customer, to enable the customer to migrate from a service being terminated (for whatever reason) to another supplier's service so as to minimize any disruption to the customer's business activities that relied on that service.

## E. The IACCM Contracting Principles

(i) Termination rights and obligations, including high-level principles for Termination Assistance, should be addressed in the contract so that entire life cycle of services and/or the relationship – from start to finish – is addressed in a comprehensive manner and so that the customer does not perceive that its key operations may be placed in jeopardy at the end of the relationship.

(ii) The extent of Termination Assistance that is appropriate will vary based on the type of services being provided and the environment in which they are provided (e.g., business process outsourcer, multi-supplier environment) during the service term.

(iii) The goal of Termination Assistance is to secure business continuity by making transition as seamless as possible for both supplier and customer. The assistance should enable the customer to take over the services directly or obtain them through a replacement third party in an orderly fashion.

(iv) Supplier should be able to recover any of its physical assets that were on the customer's premises following the completion of the termination services, unless the parties agree that title to them passes to the customer (with any applicable payment as agreed).

(v) The contract (or Exit Plan) must clearly specify if there are any assets (e.g., intellectual property, confidential information, data or personnel) that were transferred by one party to the other during the course of the contract or were created by the supplier during the relationship that must be returned to the customer or supplier, as the case may be, during the Exit Plan. This may be particularly critical to the customer if its ongoing operations are dependent on return of data that it owns and for which there is no internal back-up.

(vi) Any information, personnel, licenses, and/or customer-specific equipment that the parties agree will be given to customer as part of Termination Assistance may also have to be provided to customer's replacement supplier. The supplier has a right to require that appropriate confidentiality safeguards have been put in place with the new supplier before any confidential information is handed over. The disclosure obligation to the new supplier should be limited to the specific items that are necessary for continued services.

## F. Applying the Principles to Contract Terms

## 1. Services to be Provided During Termination Assistance

(i) As long as it is reasonably able to do so, Supplier should provide the same services to customers during Termination Assistance as during the term of the contract for a period that is mutually agreed by the parties as being sufficient for transition by the customer to a replacement supplier or alternate solution.

(ii) The customer should be able to choose the specific Termination Assistance needed for its unique situation and should not have to elect a one-size-fits-all approach, provided that there is a meeting of the minds of what can be reasonably accomplished at fair cost. Volume commitments should not apply during any transition.

(iii) To the extent services continue to be provided during the Exit Plan as was the case previously, particularly if the services are mission-critical to the customer, SLAs should continue to apply as they are explicitly set forth in the Exit Plan, except that any outages due to transition activities should not give rise to remedies such as credits.

## 2. Contractual Obligations/Rights During Termination Assistance

(i) If termination is due to a material breach of the customer, including non-payment, then supplier should have the right to require additional terms to ensure compliance prior to providing any Termination Assistance services.

(ii) Force majeure provisions should be applicable to termination assistance obligations.

(iii) Termination Assistance should be on commercial terms similar to what supplier offers for the same type of services to other customers of similar size to customer, based on the volume and nature of the services as they are reduced over the life of the Exit Plan. Supplier should receive fair remuneration for Termination Assistance that is not otherwise covered in the normal course of providing the services. These additional costs should be specified in the Exit Plan.

(iv) The parties should agree in the contract on contingencies for Termination Assistance to handle events such as a Supplier's bankruptcy, liquidation, change in control etc. Examples of areas to cover are relevant documentation, plans and code to be held in escrow with regular updates and releases to the Customer upon the happening of a triggering event so that the Customer is ensured of service continuity.

## 3. Transition Activities During Termination Assistance

(i) If Customer requests supplier to provide the services or process production elements directly to a replacement supplier, then Customer should be first obligated to ensure the replacement supplier maintains the confidentiality of all information received and cannot use it to gain a competitive advantage over supplier.

(ii) Customers should have access to all data and work product that relates to Customer's use of the Services for purposes of knowledge transfer and training. All such data and work product should be transferred in an agreed format to avoid unnecessary data entry or conversion costs.

(iii) The Exit Plan may designate those supplier personnel, if any, who customer may recruit for itself or the alternate Supplier. In this case, supplier should agree to waive any non-compete provisions with respect to those identified personnel.

(iv) The Exit Plan should designate the equipment, software and other intellectual property that will be provided to customer. The Exit Plan should also designate both Customer's and supplier specific license or ownership rights with respect to software or other intellectual property as well as Customer's rights to pass confidential product or service information on to other suppliers.

(v) The parties should agree in the Exit Plan which third party contracts will need to be assigned to Customer as part of termination assistance. Generally, third-party contracts that are used by Supplier to support multiple customer accounts or which contain provisions against assignment should be exempt from assignment. Where exempt, supplier should provide reasonable assistance to Customer in engaging those third parties directly.

(vi) The Exit Plan should specify knowledge transfer and documentation to be given to customer so that customer and its new supplier can reasonably assume service provisioning. The applicable Exit Plan should set out the specific wind-down terms applicable to each stage of the Termination Assistance, including how volume changes will affect the services provisioning.