IACCM
International Association for
Contract & Commercial Management

IACCM Contracting Principles

Contents

IACCM Contracting Principles 4
Introduction 4
INTELLECTUAL PROPERTY RIGHTS AND INDEMNIFICATION FOR THIRD PARTY IP CLAIMS 5
A. General Concepts 5
B. IACCM Contracting Principles 5
1. Intellectual Property Rights 5
2. Intellectual Property Infringement 6
SLA REMEDIES 7
A. Definitions 7
B. General Concepts 7
C. IACCM Contracting Principles 7
CUSTOMER AUDIT OF SUPPLIERS 9
A. Definitions 9
B. General Concepts 9
C. IACCM Contracting Principles 9
1. General Audit Principles 9
2. Financial Audits 10
3. Operational Audits 10
LIABILITY CAPS AND EXCLUSIONS FROM LIABILITY 11
A. Definitions 11
B. General Concepts 11
C. IACCM Contracting Principles 12
1. Reasonable Liability Caps 12
2. Exclusions from Liability 12
3. Exceptions to Liability Caps or Exclusions from Liability 12
DATA SECURITY AND PRIVACY 14
A. Definitions 14
B. General Concepts 14
C. IACCM Contracting Principles 15
1. Scope of Protected Data Obligations 15
2. Compliance with Laws and Regulations 15
3. Allocation of Liability for Protected Data Losses 15
INDEMNIFICATION OF THIRD PARTY CLAIMS (EXCLUDING INTELLECTUAL PROPERTY CLAIMS) 17
A. Definitions 17

B. General Concepts 17
C. IACCM Contracting Principles 17
1. Scope of Indemnification Obligations 17
2. Applicability of Liability Caps and Exclusions from Liability for Indemnification Obligations 18
3. Conditions for Indemnification 18

IACCM Contracting Principles

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.

INTELLECTUAL PROPERTY RIGHTS AND INDEMNIFICATION FOR THIRD PARTY IP CLAIMS

A. General Concepts

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

1. Intellectual property owned by a party remains that party's property unless expressly transferred under the contract.
2. A party's use of and rights to another party's intellectual property must be expressly specified in the contract.
3. 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.
4. 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. IACCM Contracting Principles

1. Intellectual Property Rights

a. 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.
b. 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.
c. 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.
d. 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.
e. 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.
f. Third-party software, services, and equipment are provided subject to the third party's license terms.

2. Intellectual Property Infringement

a. 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"):
    i. combination of the supplier's service or product with items provided by the customer or others not under the supplier's control;
    ii. modification to the supplier's service or product by someone other than the supplier or others not under the supplier's control;
    iii. the supplier's adherence to the customer's requirements;
    iv. the customer's content; or
    v. use of the service by the customer in breach of contract restrictions or in violation of law.
b. The customer should be responsible to defend and pay/settle any third-party claim against the supplier for Excluded Claims.
c. The obligation to indemnify for third party infringement claims should not be subject to any limitation of liability cap.
d. 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.
e. 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.
f. If the supplier's service or product infringes a third party's IP (or is subject to a claim of infringement), the supplier may:
    i. obtain from the third party the right for the customer to continue its use of the service or product;
    ii. modify the service or product so it is not infringing without materially reducing the functionality or performance of the service; or
    iii. substitute another service or product having substantially the same functionality and performance criteria.

    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.

SLA REMEDIES

A. Definitions

The following definitions apply to this IACCM Contracting Principle:

1. **"Service Level Agreement"** or **"SLA"** means the contractual quantitative standards set for service performance by the parties (e.g., response time, service quality, uptime).
2. **"SLA Credit"** means the credit provided by a supplier to a customer for an SLA Failure.
3. **"SLA Failure"** means the failure of supplier to meet its obligations under an SLA.
4. **"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. General Concepts

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

1. 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.
2. SLAs are intended to underscore supplier's efforts to maintain the service, proactively identify potential problems, and quickly resolve any SLA Failures.
3. 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.
4. 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. IACCM Contracting Principles

1. Suppliers should make performance reports available on a regular basis.
2. SLAs should take into account both the complexity and the criticality of the services.
3. SLA Credits should be based on quantified performance standards set out in the contract.
4. It should be agreed by the parties that SLA Credits are not penalties, which are not enforceable in some jurisdictions.
5. SLA Credits should be the sole and exclusive remedy available to the customer for Service Level Failures, except for Chronic SLA Failures.
6. In the event of a Chronic SLA Failure, Customers should have the additional right to terminate the affected service without penalty, following executive escalation.
7. 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. a force majeure event;
   b. acts or omissions on the part of customer or any other third party over which the supplier has no control;

c. scheduled maintenance by the customer or entities under the customer's direction or control;
d. scheduled maintenance by the supplier or its subcontractors within maintenance windows;
e. lapses of service or performance issues related to non-supplier-provided and/or maintained equipment at a customer site;
f. customer's use of the services in violation of the agreement, which violation caused the problem; and/or
g. customer's use of non-standard products and services not approved for use by supplier.

CUSTOMER AUDIT OF SUPPLIERS

A. Definitions

The following definitions apply to this IACCM Contracting Principle:

1. **"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).
2. **"Service Quality Audit"** means investigation and examination of the supplier's records for the purpose of verifying that service levels are being met.
3. **"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. General Concepts

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

1. 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).
2. 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.
3. The customer's audit rights should not require the supplier to violate its own legal or contractual obligations to third parties.

C. IACCM Contracting Principles

1. General Audit Principles

a. When audit rights, whether for Financial Audits, Compliance Audits or Service Quality Audits, are agreed to by the parties, they should be subject to:
   i. reasonable parameters on what can be audited;
   ii. requirements to provide reasonable advance notice; and
   iii. restrictions on frequency.

   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).

b. 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.
c. 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.
d. 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.
e. 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).
f. 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.
g. 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

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

a. 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.
b. 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:
    i. the supplier's submittal of responses to security questionnaires,
    ii. supplier certifications demonstrating achievement of industry standards; or
    iii. 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*)*.
c. 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.

LIABILITY CAPS AND EXCLUSIONS FROM LIABILITY

A. Definitions

The following definitions apply to this IACCM Contracting Principle:

1. "**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).
2. "**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.
3. "**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. General Concepts

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

1. A party's liability under an agreement should be solely related to a failure to meet obligations specified in the agreement.
2. 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.
3. 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.
4. 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.
5. 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).
6. 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).
7. 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 wilful misconduct.

8. 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. IACCM Contracting Principles

1. Reasonable Liability Caps

a. 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.
b. 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.
c. 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.
d. 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.
e. The Liability Cap clause should survive any termination of the agreement to apply to claims raised post-termination.

2. Exclusions from Liability

a. 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.
b. 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.
c. 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

a. 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.

b. 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.
c. 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.
d. 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).

DATA SECURITY AND PRIVACY

A. Definitions

The following definitions apply to this IACCM Contracting Principle:

1. "**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.)
2. "**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.
3. "**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. General Concepts

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

1. 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.
2. 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.
3. 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).
4. 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. IACCM Contracting Principles

1. Scope of Protected Data Obligations

a. 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.
b. 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.
c. The customer should undertake reasonable steps to safeguard their own Protected Data, such as encryption, firewalls or regular backups.
d. 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

a. 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.
b. 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.
c. 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.
d. 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.
e. 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

a. 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).
b. 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).

c. 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.
d. 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.
e. 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.

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. General Concepts

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

1. 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.
2. Third parties should not be viewed as beneficiaries of an agreement between customers and suppliers unless expressly made so in the agreement.
3. 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.
4. 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.
5. 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.
6. 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. IACCM Contracting Principles

1. Scope of Indemnification Obligations

a. 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.

b. 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).
c. Supplier's indemnification for governmental or regulatory fines or penalties 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.
d. 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.
e. 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

a. 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).
b. 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

a. The Indemnitee should have the same obligation to mitigate third party damages as it would to mitigate its own.
b. Any obligation to indemnify for third party claims should be preconditioned upon the following:
    1. The extent of liability for the claim should be proportional to the fault on the part of the Indemnitor vis-à-vis the Indemnitee or any other party.
    2. The Indemnitee must give prompt notice of the claim to the Indemnitor or relieve the latter for any incremental liability caused by the delay.
    3. The Indemnitee must provide reasonable support to the Indemnitor in defense of the claim.
    4. 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.
    5. 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.
    6. 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.
    7. 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.