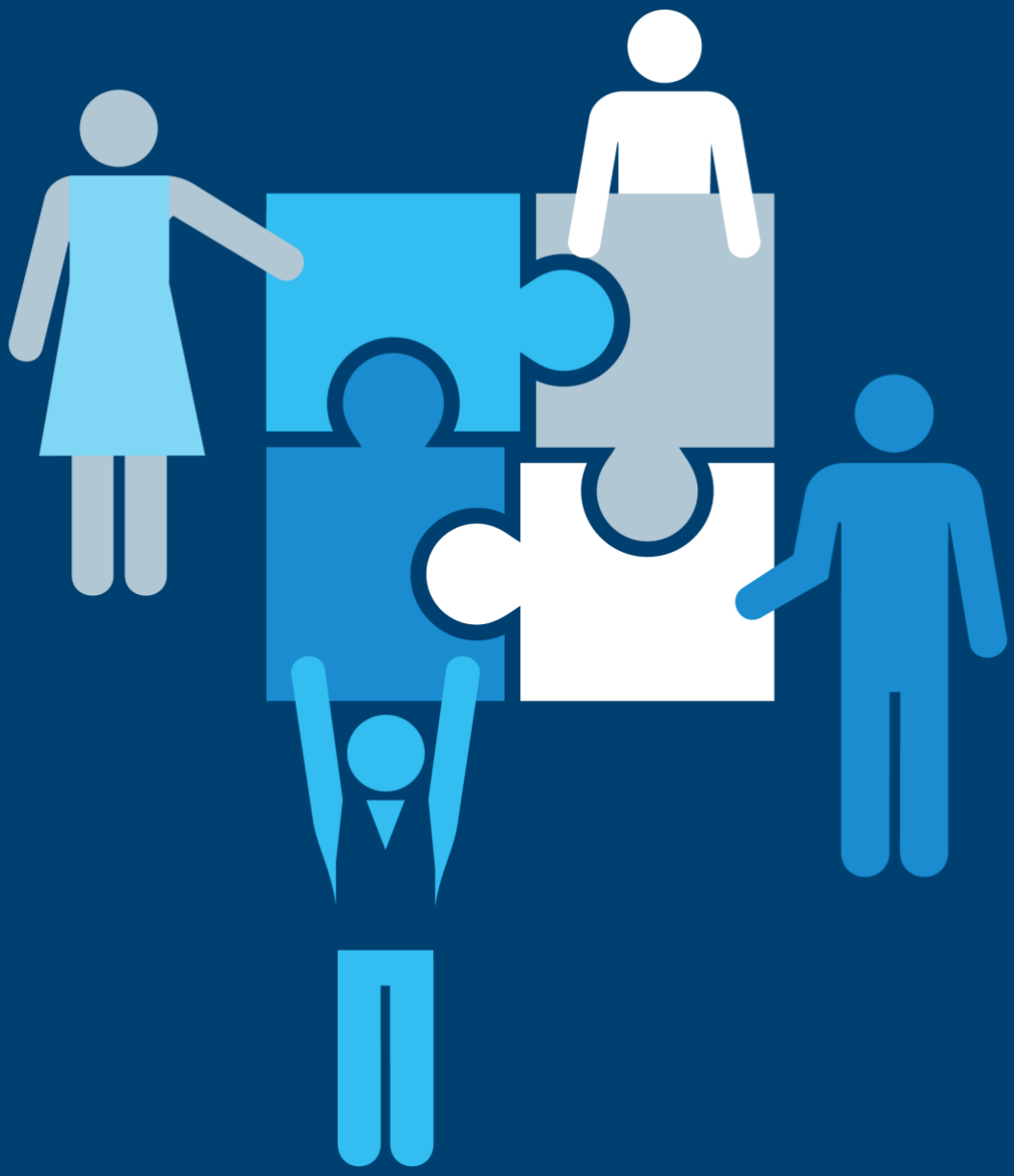
WorldCC Contracting Principles



September 2024

World Commerce & Contracting

Contents

Introduction

These contracting principles have been developed under the auspices of and are endorsed by World Commerce & Contracting and are referred to as the **"WorldCC Contracting Principles"** or just **"Principles."**

They are intended to serve as an international cross-industry 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.

Those who wish to adopt these WorldCC Contracting Principles are free to use them in their entirety or on a more selective basis 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 and negotiate the relevant clauses accordingly.

These Principles are not intended to constitute formal legal advice.

AI Models – Confidentiality, Security, and IP Rights

Background Information for this set of Principles

1. AI can be used for many different purposes and comes in different forms.

Although all AI triggers legal issues and requires legal analysis, the Principles below focus on **generative AI models**.

- **Generative AI** is an advanced branch of deep learning that uses exceptionally large neural networks called large language models (LLMs) that can learn especially abstract patterns to create new content.
- **Deep learning** is a branch of machine learning in which neural networks ingest data and process it through multiple iterations to make increasingly sophisticated predictions in an attempt to mimic how the human brain works.
- **Machine learning** is a branch of AI in which algorithms are utilized to detect patterns and learn to make predictions and recommendations by processing data. AI models are trained using a variety of techniques that enable them to learn from the data and improve their performance. These techniques include supervised training, unsupervised training, semi supervised training and image annotations. Each technique plays a crucial role in enhancing the capabilities of AI models

2. Generative AI models generally consist of either private modeling tools or public ones.

Private AI involves algorithms trained on data specific to a single user or organization and is confined within the organization's internal systems. Public AI (e.g., Chat GPT), on the other hand, is trained on a wide set of publicly available data or provider-selected datasets that are not exclusive to any one user or organization.

3. Increasingly, software applications incorporate AI modeling techniques that use ingested data to enhance the software's performance and value to users.

These techniques can either use data and inputs from one company or a shared model combining data from all customers to enhance the solution's capabilities of the solution for all of the vendor's customer-base.

4. Many countries and over 40 US states are adopting or have adopted AI guidelines and regulations.

- Like data privacy laws, AI guidelines and regulations from different jurisdictions vary and often conflict. Given the changing AI legal landscape, all AI, whether private or public, should undergo a thorough regulatory review before use and regularly thereafter.
- One key regulation is the EU AI Act, which is expected to be enacted in late 2024. The AI Act categorizes AI into three categories, namely unacceptable, high and limited risk.
    - **Unacceptable risk** AI is banned while **high risk** AI must be approved by EU officials before first going to market and also through the product's lifecycle.
    - **Limited risk** AI must be appropriately labelled to notify users.

5. Customers should use a risk-based approach before obtaining and using AI models.

This approach should consider:

- whether the AI model is appropriate and necessary for the use case and the environment in which it will be deployed;
- in the case of automated decision making, whether and to what extent the model provides transparency and details about how it makes its decisions;
- whether the AI tool complies with applicable laws and regulations; and
- whether the algorithm is sufficiently accurate for the intended purpose and can be continuously updated and tested to minimize errors (e.g., "hallucinations") and improve reliability.

6. The following Principles may evolve as the AI field and market practices become clearer, and as best practices gain consensus.

Although this area is in flux, it is still important to develop reasonable guidelines based on current information. These Principles address fair and reasonable negotiating positions within three AI contexts:

- Public generative AI models;
- Private generative AI models; and
- Other software with embedded AI predictive modelling capabilities as part of its basic functionality

The Principles

1. Public Generative AI Tools

1. When using public AI tools, any data entered is merged or aggregated with other inputs. As a result, although suppliers may agree to safeguard the confidentiality of the Training Data following negotiations between the parties, such a confidentiality commitment is less likely compared to private generative AI Models.

2. The AI tool supplier has no control over the tool's outputs and is unlikely to provide warranties as to their accuracy or completeness, warranties of non-infringement, or indemnification for IP infringement claims (but see point 1.3 in the *Applying the Principle*s section below for trends in this area).

3. A third party can enforce intellectual property rights against customers who obtain and use AI output that infringes the third parties' intellectual property. This is especially relevant for generative AI relying on web scraping to retrieve vast amounts of data and create new content. Unauthorized web scraping can potentially lead to claims of:

    a) copyright infringement (when copyright protected content, such as a news article or poem, is scraped);

    b) breach of contract (if data is scraped from a website that prohibits scraping or use with generative AI);

    c) violation of privacy rights (when personal information is scraped and used in violation of applicable data privacy laws);
    or

    d) violations of other applicable laws.

    The validity of such claims against AI developers and deployers is being actively litigated and the law remains unsettled on the merits. The customer should ensure that the supplier

    a) confirms that no unauthorized web scraping was done;
    and

    b) provides substantive details of how data used by the AI tool was obtained from enabling sources.

4. The supplier should be responsible for meeting the representations set forth in any documentation about the functioning of the tool it provides to the customer.

2. Private Generative AI Tools

1. Customers must contractually address the following areas when purchasing or licensing a private (or semi-private) generative AI model for their business use: confidentiality, data security, cyber security, ownership rights, workings and limitations of the AI Model, and intellectual property indemnification obligations.

2. A customer has the right to expect full confidentiality with respect to all of its data used and produced by the tool, provided it takes reasonable steps to keep its infrastructure secure. The contract should require that the private AI Model has adequate security features sufficient to protect the customer's confidential information.

3. For semi-private generative AI tools (where the supplier shuts off all customer's data feeds to keep them confidential, while allowing the customer to benefit from prior training data), the supplier should be responsible for maintaining the privacy and confidentiality of that customer's data and for any "leakage" of the data into the public domain.

4. The supplier may refuse to offer a warranty for the accuracy of the output of a private AI Model, because AI can "hallucinate" (generate inaccurate output and present it as if it were true). However, the supplier should take adequate measures to ensure that the AI Model's output is designed to be reasonably accurate.

5. If a customer obtains a private AI tool and gets full ownership rights to It, then the supplier should:

    a) give the customer all related source code, configuration files, decision logic, training documentation, user/administration documentation and support/maintenance procedure manuals related to the functionality provided by that private AI tool;
    and

    b) not be held responsible for any misuse or reverse engineering of the tool.

6. The supplier should provide the customer with an AI Model Card for any private AI tools it is providing with ongoing support. As the AI Model Card will evolve as the technology advances, the supplier should agree to update the AI Model Card periodically as well as when the supplier materially changes the AI Model or retrains it.

7. The supplier should indemnify the customer for IP (including embedded third-party IP) infringement for the AI Model similar to that offered for other software. The customer should indemnify supplier to the extent customer's training data gives rise to third-party IP infringement claims.

3. Software Applications with Embedded AI Predictive Modelling Capabilities

1. The supplier should indemnify the customer as long as customer's use of the AI Model is in accordance with the documentation and instructions provided by the supplier. *(See Contracting Principle on IP Indemnification for further guidance as to extent of indemnity, remedies, etc.)*

2. The supplier should warrant that the software will perform in accordance with all documentation but should not be required to provide any warranty for the quality of outputs (which are normally dependent on the quality of the inputs) or that the software will meet the specific needs of the customer.

3. To the extent the software is provided as a centralized cloud or SaaS model that learns from all users' inputs, the customer should not expect confidentiality with respect to its input unless it asks the supplier to shut off its data feed. The supplier, when proposing a centralized cloud or SaaS model, should

- **a)** provide adequate information of how customer data is used within the co-located/shared platform;
  and
- **b)** obtain customer's consent before including the customer's data in such platform.

4. The supplier should be held responsible for meeting all applicable software and service specifications and documentation, as long as the customer complies with all requirements, limitations, and prohibitions stated in the contract or documentation.

Applying the Principles to Contract Terms

1. Public Generative AI Tools

Exclusion of Training Data from Confidential Information

1.1. When defining confidential information, if the public generative AI Model will be trained on customer-provided data, the definition should expressly exclude any information that the customer will be including in Training Data, prompts, or inputs into the algorithms, given that such information will become public and the supplier will have no control over their disclosure.

Customer responsibility for AI output use

1.2. A supplier should not accept any responsibility for how AI outputs are used by the customer, and the customer should use the information with all due care as to accuracy, relevance, and completeness as AI Models are notorious for producing inaccurate or faulty information (hallucinations).

Customer liability for third party claims

1.3. The customer may also have to accept all responsibility if its use of the information infringes a third party's patent or copyright rights. However, a growing trend is for suppliers of these tools to offer a limited indemnification against third party copyright infringement claims associated with outputs as a way of encouraging the expansion of the tools in the marketplace and in recognition that the risk of such claims is very low, but it is still too early to determine if this will become the market norm.

Contractually required AI governance

1.4. Customers should require in the contract that suppliers maintain adequate AI governance models and principles that will be adhered to in the development and support of the AI Models, particularly with respect to the ethical standards to be employed and the efforts made to cull out information known to be false.

Although not a contracting principle, it is important that companies relying on public generative AI models establish strict rules for their employees on what can and cannot be entered into the tools given the public dissemination of that data.

- Companies should establish clear policies on use of public AI and data handling and provide training to staff, in addition to employing robust security measures.
- Before using any generative AI Model, employees and individuals should carefully review the supplier's published AI policies.

2. Private Generative AI Models

Prioritizing confidentiality

2.1. Even though parties traditionally focus on IP ownership rights with respect to inputs and outputs of software tools, in dealing with private generative AI Models, the focus should be more on confidentiality and safeguards against public dissemination of customer information. The supplier should be liable if it causes data to enter the public domain through no fault of the customer.

Customer-provided Training Data

2.2. Suppliers should also agree in the contract that they will not claim proprietary or ownership interest in any Training Data or augmentations of the AI models which are provided by the customer or on behalf of the customer by a third party.

Contractually required AI governance

2.3. As above for public AI Models, customers should require in the contract that suppliers maintain adequate AI governance models and principles that will be adhered to in the development and support of the private AI Models.

Customer liability for third party infringement claims

2.4. Principle 1.3 above applies here as well, provided, that suppliers should provide indemnity for any infringement claims based on the AI Model provided (and not the outputs or use thereof).

3. Software Applications with Embedded AI Predictive Modelling Capabilities

Clearly stated ownership and licensing rights

3.1. Ownership rights in AI inputs, Training Data and model improvements should be clearly stated in the contract. All ownership or license rights (e.g., exclusivity, license duration) should be clearly linked to the anticipated use case for the AI tool. Customers should ensure that it has sufficient ownership or license rights for its anticipated uses.

Clearly stated warranties for AI performance

3.2. The contract should clearly state any warranties that the supplier provides in connection with the workings of the software, including but not limited to meeting specifications and documentation that are provided to the customer, how data is absorbed by the AI model, and the extent to which the model training relies on data from external sources.

It may be reasonable, given the customer's use case, that instead of standard performance warranties that the AI complies with published specifications or documentation, the contract should reflect the parties' agreement on a clear list of parameters to determine whether the AI tools meets the contract standards, utilizing quantitative targets and/or functional requirements for the AI tool or the outputs it generates. As examples, performance specifications should be provided that are based on the predictive power of the AI tool, level of accuracy, consistency of outputs, or increased speed of response to customer inputs.

The contract should also specify how performance will be verified and whether the AI tool will be supplemented with a separate accuracy checking solution. Since AI tools are in early stages and will remain so for a considerable amount of time, health checks of their use and output should be conducted at more frequent and shorter intervals than may be done on time-tested software solutions.

Supplier indemnification for third party claims

3.3. The supplier should indemnify the customer with respect to any third party claims that the software improperly relied on a third party's data and that seek to prevent the customer from using the tool to the extent it relies on that Training Data. As an example, in the event that supplier developed the AI Tool using third party data, and the third party whose data was used brings suit to prevent the customer from using the AI tool, the supplier should be fully responsible for protecting the customer from the loss of value resulting from the claim.

Case-by-case allocation of responsibilities

3.4. Due to the uncertainty of the regulatory landscape applicable to AI, the allocation of responsibility between the customer and the supplier should be considered on a case-by-case basis relative to the use of the AI and the determination of which party is best suited to maintain compliance with evolving laws and regulations. As laws in the AI space vary significantly and are being rapidly enacted and revised, the parties should consider a separate provision that supplements the compliance with laws clause with one that addresses the need for periodic, mutual reviews and updates for newly enacted laws and regulations and for corresponding amendments to the contract as appropriate.

Minimizing risk of open-source data or software in Training Data

3.5. To minimize risks of AI tools using open-source software or data incorrectly and/or unlawfully, the parties should agree in the contract on the source of AI Training Data, along with reviews of that Training Data at regular intervals.

The contract should include provisions that if open-source is used, the AI tool will adhere to open-source license terms. Potential issues that can arise include claims of license infringement and claims from the open- source community. To mitigate potential issues, customers should meticulously review and document the source of AI Training Data. The parties should also agree in the relevant contract to implement effective tracking mechanisms, ensure proper attribution, and obtain legal guidance as needed to ensure adherence to open-source licenses and mitigate potential compliance issues.

Defined Terms

AI, or Artificial Intelligence: computer software that is programmed to execute certain algorithms (computer code programmed to perform particular tasks) to recognize patterns in large volumes of data, and to reach conclusions, predict future behavior and patterns, and make informed judgments based thereon.

AI Model: a program that has been trained on a set of data to recognize certain patterns or make certain decisions without further human intervention.

AI Model Card: a short document that provides key information about a machine learning model.

Training Data: data used to train an algorithm or machine learning model to predict the outcome that the model has been designed to predict.

Alternative Dispute Resolution ("ADR")

The Principles

1. Although parties may have diverse views on the effectiveness or propriety of ADR strategies, all contracts should require Direct Negotiation as a means of resolving disputes prior to utilizing either ADR processes or litigation.

2. As compared to most forms of ADR, litigation takes more time due to courts' large caseloads and required pre-trial procedures, can be more costly, and can result in numerous appeals before a final actionable judgment is rendered. ADR is generally conducted in a private forum, which allows the dispute to remain confidential between the parties. Mediation and Arbitration are forms of ADR that allow the parties to choose specialized mediators or arbitrators who are familiar with the parties' industry(ies), and the technical and commercial complexities of the contract.

3. ADR processes should be specified in the relevant agreement so that there is no ambiguity as to intent. Arbitration must be specified in the agreement to be enforceable. If ADR is not contracted for in writing, then litigation becomes the default dispute resolution mechanism for the contract in most legal systems. Under applicable legal doctrine, arbitration clauses are considered independent agreements, separate from the contract in which they appear. ADR clauses should be clear and specific. For Mediation and Arbitration, the chosen ADR Institution's provided sample clauses should be customized and incorporated into the agreement when appropriate.

4. Regardless of what ADR process is used or whether one is used at all, parties should always have the right to seek equitable relief (e.g., temporary restraining orders or injunctions), as permitted under local laws, to avoid irreparable harm while the dispute is being resolved.

Applying the Principles to Contract Terms

1. Direct Negotiation

Escalation as the first attempt to resolve a dispute

1.1. A dispute resolution clause in a commercial contract should require that the parties first attempt Direct Negotiation to resolve the dispute. In some very large relationships, the parties may even set up Dispute Avoidance / Resolution Boards to handle potential or actual disagreements. If Direct Negotiation fails, then, if both parties so agree, Mediation should be pursued, and if the parties are still at an impasse by the end of Mediation, then binding Arbitration may be used.

Escalation process and time frames

1.2. Direct Negotiation provisions should require that the parties escalate the dispute to their designated management (both commercial and legal) for discussion and negotiation in the event of a dispute. The designated executives should be required to use all good faith efforts to resolve the dispute quickly, within a specified time frame (e.g., three weeks) which can be extended upon mutual agreement of the parties. Any resolved disputes should be memorialized in a settlement agreement. Each party will bear its own costs associated with the Direct Negotiations.

2. Direct Negotiation

Mediation ground rules

For Mediation, in accordance with the chosen ADR Institution's sample clauses, the contract provisions should state the following:

a) The Mediation should be confidential and non-binding.

b) Name of mediator(s) (or mediation association) and payment method. The cost of the mediator should be split evenly between the contracting parties.

c) Duration of the Mediation.

d) Parties' requirements to mediate in good faith pursuant to an agreed upon time frame, until either party reasonably determines that it is fruitless to continue.

e) If agreement is reached in Mediation, it should be memorialized in a settlement agreement.

3. Direct Negotiation

Arbitration ground rules

3.1. For Arbitration, in accordance with the chosen ADR Institution's sample clauses, the contract provisions should consider specifying the following (especially as relevant to an ad hoc ADR process):

a) Which ADR Institution (or other organization if very specific technical expertise is needed) will process the Arbitration and which procedural rules of that ADR Institution will apply.

b) Whether the decision will be made by a panel of one or three arbitrators.

c) Place of arbitration.

d) The required qualifications (if any) for the arbitrator(s) (e.g., require legal, finance or business experience, expertise in a particular industry, or nationality), the locale or jurisdiction where Arbitration is to take place (which will also determine applicable procedural law), language (especially if multilingual contracting parties), and choice of applicable law.

e) Whether escrow is to be used to hold and protect funds, intellectual property or other items relevant to the dispute, until an Arbitration award can be made.

f) Any award made in Arbitration shall be accompanied by a final award of the arbitrator(s) giving the reasons for the award and shall be binding upon the parties with no right of appeal. Judgment may be entered upon the Arbitration award in any court having jurisdiction thereof (or a specific court if preferred by the parties).

g) How the costs of the arbitration will be split between the parties (e.g., evenly or based on proportional responsibility for the claims).

Defined Terms

Alternative Dispute Resolution, or ADR: the process for settling disputes without litigation. Arbitration, Direct Negotiation, and Mediation are all different forms of ADR.

Arbitration: a private dispute resolution process by which the parties submit their dispute to one or more appointed arbitrators authorized to reach resolution on the dispute by rendering a final and binding decision called an award.

ADR Institution: an organization commonly chosen to administer Mediations or Arbitrations, as applicable, between disputing parties (e.g., American Arbitration Association or the International Chamber of Commerce).

Direct Negotiation: the escalation of a contract dispute to each of the contracting parties' designated representative (typically, executive level) for resolution if the issues cannot be resolved at the working levels of the parties.

Mediation: a process by which a third-party neutral facilitator is engaged to facilitate discussions between the parties and to encourage compromise and settlement of the issues. If the parties settle the dispute during mediation, they will typically formalize it in a separate agreement.

Assignment and Novation

The Principles

1. Parties should clearly delineate in their contract whether and under what circumstances a party can Transfer the contract to another party. The “assignment and novation” clause should state the consent conditions (including timing), any formal requirements for Transfers, and the operational and commercial impacts, if any, of any Transfer on the original parties and the new one(s).

2. Except as set out in this Principle, the “assignment and novation” clause should exclude or limit the Transfer of contract unless the original counterparty has given its prior consent. A risk for suppliers and customers is ending up in a contract with an unknown party that might have different values, strategies, and abilities, or with a competitor that can negatively affect their business.

3. A Transfer may be necessary to effect important changes in the business of suppliers or customers, such as corporate restructurings, company takeovers or sales of a business. Having commercial contracts that strictly restrict the right to Transfer might decrease the overall attractiveness (and value) of a company’s business to a prospective buyer, as obtaining the required consent from the original counterparty may be difficult. The “assignment and novation” clause should therefore permit either party to Transfer the contract without the prior consent of the other party in certain pre-defined circumstances such as:

    a) a corporate restructuring, allowing the Transfer to an affiliated company under the same control as the original contracting party;
    or

    b) a change of control transaction whether by merger, consolidation, sale of equity interests, sale of all or substantially all assets, or otherwise. In this case, the seller of a business should be able to Transfer the contracts with his customers and suppliers to the buyer and allow the buyer to carry on the business.

4. The validity under the relevant legal system of clauses giving prior consent for a Transfer in certain pre-defined cases should always be verified.

5. When clauses permit a party to Transfer the original contract in some pre-defined cases without the other party’s prior consent, the Transfer should enter into force with respect to the incoming party when the Transfer agreed between the outgoing party and the incoming party is notified to the counterparty or when the counterparty so acknowledges.

6. Suppliers and customers may want to expressly exclude permitted Transfer in certain cases, as specified in the contract, such as when the transferee is an actual or potential competitor of the original counterparty or when the transferee is not capable of meeting obligations (technically or financially) or potential liabilities under the contract.

Applying the Principles to Contract Terms

1. Exclusion and Consent Conditions

Making Transfers conditional

1.3. The “assignment and novation” clause can have the effect of preventing or making conditional a Transfer (e.g., subject to the consent of the original counterparty).

Formal requirements for consent

1.4. When expressly requiring consent, the “assignment and novation” clause should specify the applicable formal requirements (e.g., the consent shall be provided in writing and prior to the effective Transfer).

Reasons for withholding consent

1.5. The clause should also specify whether prior consent, where required, can be withheld solely upon the discretion of the consenting party or whether it can only be withheld based on reasonable grounds.

2. Anticipated or Excluded Consent in Predefined Circumstances

Transfer always permitted

2.1. The “assignment and novation” clause should expressly specify the circumstances, under which the Transfer can occur without the prior consent of the other party.

When consent to Transfer not required

2.2. The clause can feature the right of Transfer without prior consent in predefined circumstances, either as unilateral (i.e., for the supplier or the customer only), or as reciprocal (i.e., for both parties). When focusing on this issue, the respective parties should consider various scenarios, e.g., continuity of business for the customer when the supplier Transfers the contract to another supplier, or, from a supplier perspective, creditworthiness when the customer Transfers the contract to another party.

3. Effects of the Transfer

Clear impacts on the parties

3.1. The “assignment and novation” clause should clearly specify the effects of the Transfer on the original parties as well as whether the contract is binding on their successors and in general their permitted assigns.

Defined Terms

Transfer: the transfer of a contract, in whole or in part, by way of assignment, novation or otherwise, so that a third-party stands in the shoes of one of the original parties to the contract with respects to rights, obligations or both. (Note: Assignment and novation are legal concepts with different meanings under common law and civil law).

Compliance with Laws

The Principles

1. 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.

2. 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.

3. 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.

4. 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 or to either of the parties.

5. 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 (e.g., Change Control) that enables the impact of these changes to be reflected by adjustment of the contract. In some cases, dramatic changes in Applicable Laws having material impacts may even be treated as a force majeure event.

Applying the Principles to Contract Terms

1. What Applicable Laws Apply to Each Party

Compliance with laws applicable to you

1.1. 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. However, it may be reasonable for one party to reasonably collaborate with and support the other party's compliance activities if they are directly related to the products or services under the contract and are anticipated from the outset of the relationship.

Compliance with industry-specific laws

1.2. 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

Consequences of non-compliance

2.1. 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.

Liability for non-compliance

2.2. 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

Damages from violation of Applicable Laws

3.1. 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.

3.2. 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

Compliance

4.1. Companies are required to comply with applicable anti-boycott laws.

International Contracts

4.2. 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 anti-boycott laws.

Defined Terms

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

Confidential Information

The Principles

1. 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, in which case the NDA is normally superseded by the contract language).

2. 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:

    a) that is disclosed in any form by one party to the other or one party has gained from the other party as a result of the relationship;

    and

    b) that a reasonable person would Identify as being confidential to the discloser or that is marked as confidential.

    Confidential Information **should not include** information that:

    a) has already been made public by the Discloser or a third-party;

    b) is independently developed by the Recipient without reliance on the Discloser's Confidential Information;

    c) was obtained by the Recipient from a third-party without restriction;

    or

    d) the Discloser has expressly indicated as not confidential.

3. 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 (if permitted) as soon as reasonably possible to take action to block the order or protect the information.

4. 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:

    a) those entities use the Confidential Information to the same extent as the Recipient may under the agreement between the Discloser and the Recipient;

b) 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

c) the Discloser has given any required consent.

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.

5. 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.

6. The Recipient should also promptly notify the Discloser about all unauthorized disclosures and take measures to mitigate the effects of such events.

7. 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.

8. 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.

9. 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.

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

11. Personal data often gets lumped together with Confidential Information but should typically be treated separately and with different standards of care given the laws and regulations that apply (See WorldCC Contracting Principle *Data Security and Privacy*).

12. 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.

Applying the Principles to Contract Terms

1. Defining Confidential Information

Broad categories of Confidential Information

1.1. 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

a) include in the definition of Confidential Information a phrase such as "*including but not limited to …"* to cover broad categories of information that cannot be predicted at the time the contract is negotiated;

and/or

b) include other language such as "*identified as confidential at the time of disclosure or if nature of the information would reasonably warrant such treatment*".

Specific types of Confidential Information

1.2. 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. A combination of specific and broad may also be warranted.

Exclusions from confidentiality obligations

1.3. While the definition of Confidential Information may be broad and overinclusive, the exclusions can be used to carve out categories of information that will not be deemed to be Confidential Information or that lose any protections when certain events occur (cf. Confidential Information Principle 2, above).

2. Obligations to Safeguard Confidential Information

Degree of care

2.1. 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, but no less than a reasonable degree of care and in accordance with any terms of the Agreement that are specific to standards of safeguards.

Safeguard of Confidential Information in new documents

2.2. 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.

Flow-down of confidentiality obligations

2.3. The confidentiality obligations should be extended to any Recipient's employees, agents, subcontractors, or other third parties to whom Confidential Information is disclosed, consistent with the right to disclose as set out in the Agreement. These obligations should continue to apply for the appropriate period(s) even if any of the individuals change jobs or move to different employers. 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.

Confidential Information disclosure to government

2.4. If 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 reasonably cooperate, 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

Reasonable duration

3.6. 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.

Longer duration

3.7. Trade secrets are examples of information that may warrant longer protection periods (i.e., for as long as the information remains a trade secret). Software source code is another example of Confidential Information that may call for special handling by the Recipient.

Survival of non-disclosure obligations

3.8. Note that non-disclosure obligations typically have 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. The former should not start prior to the agreement start date or extend beyond the agreement expiration/termination date. The latter will often extend past the term of the NDA, in which case the obligations survive the Agreement.

4. Return of Confidential Information

Discloser's right to ask for return or destruction of Confidential Information

4.1. 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.

4.2. 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.

Recipient's right to retain a copy

4.3. 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.

Licensing or transferring ownership of Confidential Information

4.4. If 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

Uncapped liability in stand-alone NDAs

5.1. 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.

Caps and exclusions in broader agreements

5.2. 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 WorldCC Contracting Principle *Liability Caps and Exclusions from Liability*).

Right to seek equitable relief

5.3. 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. Other

Assignment

6.1. 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.

Export laws

6.2. The Recipient should comply with all applicable export laws. This is critical for certain types of sensitive information if a government prohibits the movement of that information to specified countries.

Warranty

6.3. No warranty should be provided on the accuracy of the Confidential Information, and such information should be provided "as is", unless there is an agreed reliance on that accuracy. .

Defined Terms

Confidential Information: non-public information provided by one party to the other, as defined in the Agreement.

Discloser: the party providing Confidential Information to a Recipient.

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

Recipient: the party receiving Confidential Information from a Discloser.

Customer Audit of Suppliers

See also the "Supplier Audit of Customer" Principle

The Principles

1. The extent to which audit rights will be provided to a customer is a commercial issue that should be negotiated based on the size and scope of the deal, and the nature of the solution. The type and extent of audit rights granted should be memorialized in the contract based upon business-to-business discussions.

2. Audits are a tool used by customers to verify that contractual commitments are being met. However, suppliers have a strong interest in ensuring that the scope of customer's audit rights are aligned with the suppliers' obligations so as to mitigate costs, confidentiality issues, disruption and other burdens to suppliers associated with the audit.

3. Audit rights should not be unlimited but should be prescribed based on legitimate customer needs that cannot be otherwise satisfied and should not subject a supplier to undue hardship.

4. Audit rights cannot require the supplier to violate its own legal (pursuant to applicable laws or regulations) or contractual obligations.

Applying the Principles to Contract Terms

1. General Audit Principles

Reasonable audit rights

1.1. All audit rights, whether for Financial Audits, Compliance Audits or Service Quality Audits, should be subject to

- **a)** well-defined parameters on what can be audited;
- **b)** requirements to provide reasonable advance notice; **and**
- **c)** restrictions on frequency.

1.2. One reasonable audit parameter should be the exclusion of third-party information, confidential information (unless proper protections are in place) and supplier highly sensitive information.

Time-bound audit rights	**1.3.**	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 as defined under the applicable laws or regulations of the contract (e.g., statute of limitations or retention rules).
Paying for audits	**1.4.**	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 a Financial Audit discloses material over-billing on the part of the supplier or in the event of other material non-compliance.
Regulatory-driven audits	**1.5.**	Where customers need audit rights to comply with their own auditing and regulatory requirements, supplier's support obligations should be specified in the agreement and should be limited to its provision of services and/or products.
Finding faults	**1.6.**	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.
Audit processes	**1.7.**	Customers and suppliers should agree on audit methodology and on a process to review audit results, correct for disclosed deficiencies, and confirm corrections are completed.
Third-party auditors and confidentiality	**1.8.**	If customers request to use third-party auditors, supplier and customer should ensure appropriate confidentiality obligations and use restrictions are established with that third-party auditor, as well as that the third-party auditor is not a competitor of supplier who could gain competitive advantage through the audit. Audit results should be shared with the supplier.
Auditor must destroy data after audit	**1.9.**	Where feasible, the entity performing the audit should be required to destroy all data gathered during the audit.

2. Financial Audits

Appropriateness of Financial Audits	**2.1.**	Financial Audit rights are appropriate for all types of customer contracts, subject to the general audit principles described above.
Records retention	**2.2.**	For Financial Audits, records should be limited to those available under the supplier's record retention policies.
Audits of subcontractors' records	**2.3.**	The customer should not have Financial Audit rights to supplier's subcontractors.

3. Operational Audits

Scope of Service Quality Audits

3.1. 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.

Data security audits

3.2. Compliance Audits related to data security should be satisfied by supplier's provision of responses to security questionnaires and non-sensitive data security information, which may include internal audit reports, SSAE 16, ISAE 3402 or similar audit reports (redacted or summarized as appropriate). Certifications demonstrating achievement of industry standards, or the equivalent should serve as validations of compliance with those industry standards.

Testing of security mechanisms

3.3. Audits should not include penetration or other real-time security testing, which could adversely affect suppliers' operations and their customers.

Defined Terms

Compliance Audit: investigation and examination of supplier records and 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).

Financial Audit: investigation and examination of 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) by a supplier.

Service Quality Audit: investigation and examination of supplier records for the purpose of verifying that service levels are being met.

Data Security and Privacy

The Principles

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 (e.g., meeting industry standards, timely notice of data breaches) in a shared responsibility matrix rather than by focusing solely on liabilities in the event of a Protected Data Non-Compliance.

3. The extent to which a party 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 data to be shared and the resources available to each of the parties.

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.

Applying the Principles to Contract Terms

1. Scope of Protected Data Obligations

Defining uses of protected data

1.1. Contract terms should, where possible, provide specificity with regards to the types of Protected Data being exchanged and the access, use (by the parties and third parties), sharing or re-transmission (collectively, “Use”) of the Protected Data by the other party.

Recipient's data protection obligations

1.2. A party's data security obligations should be clearly and accurately described based on the data It receives and should focus on functions and tasks, not outcomes.

Discloser’s protection of its data

1.3. The discloser should undertake reasonable steps to safeguard their own Protected Data, such as encryption, firewalls or regular backups.

Compliance with industry standards

1.4. The recipient 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 recipient should provide applicable certifications upon request.

2. Compliance with Laws and Regulations

Compliance with laws, regulations, industry standards

2.1. 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.

Recipient's responsibilities

2.2. The recipient's responsibilities with respect to data protection/privacy laws that apply specifically to the discloser should be reflected as specific operational obligations rather than a general compliance with law obligation.

Discloser's responsibilities

2.3. When appropriate, the discloser's data protection/privacy compliance activities should be clearly stated within the contract to avoid misunderstandings or gaps in responsibilities.

Changes in data protection laws

2.4. The contract should provide an equitable mechanism to modify the recipient's contract obligations (and charges, where appropriate) based on changes to data protection/privacy laws (e.g., shift away from the EU-US Privacy Shield framework, use of EU Standard Contractual Clauses) that have a material impact on the supplier and/or customer.

Providing evidence of compliance

2.5. The recipient should not be expected to provide the discloser 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 assurances relating to security controls.

Regulators' review of compliance

2.6. In cases where the discloser has an obligation to provide regulators with the recipients' compliance documentation or where laws or regulations permit regulators to audit the recipients' compliance with security standards, the contract should address those situations and provide for appropriate safeguards for the recipients' information and operations.

3. Allocation of Liability for Protected Data Losses

Recipient's liability

3.1. The recipient should be liable to the extent it caused a Protected Data Non-Compliance, subject to reasonable limitations.

3.2. If a Protected Data Loss results from multiple points of failure or proximately caused by the actions of an intervening third-party, the recipient should be held responsible only to the extent the loss is the result of its Protected Data Non-Compliance(s).

Standard liability caps for low-risk data

3.3. It is common for parties to exchange low risk data (e.g., business contact information). For this category of data, standard liability caps are typically sufficient. Additionally, some engagements Involve only incidental access to Protected Data of

the other party, and the risk of damages are small. In these cases, each party's liability for a Protected Data Non-Compliance should be subject to the standard contract limitation of liability.

Higher liability caps for high-risk data

3.4. In some cases, high-risk data may need to be accessed or exchanged by the parties. In these cases, an increased liability structure (e.g., a separate, super cap on liability) may be warranted. For example

a) supplier is operating within the customer's security environment or has significant access to Protected Data,

or

b) customer requires access to supplier personnel's personal Information In order to conduct a background check or drug screening.

Unlimited liability for intentional or grossly negligent misuse of data

3.5. The recipient 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 recipient.

General exclusions from liability

3.6. 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.

Specific types of damages

3.7. However, it may be appropriate to identify discrete categories of covered damages for which the recipient 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.

Indemnification for third-party claims resulting from Protected Data Loss

3.8. Third parties may seek damages if their personal data is involved in a Protected Data Loss. Inasmuch as it is frequently the case that both parties may have contributed to the loss, the parties should share liability to the third-parties proportional to their respective responsibility for the loss, typically through an indemnification. As part of an equitable risk allocation scheme, any higher cap on liability for Protected Data Losses should apply to this indemnification liability.

Defined Terms

Protected Data: personal data (such as personally identifiable information and credit card information) and other highly sensitive data (such as passwords) of a party or its clients that are in the possession of or accessible by the other party. 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: a failure by the recipient to comply with its obligations regarding the handling or safeguarding of Protected Data under the contract or under data protection/privacy laws or regulations.

Protected Data Loss: 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 recipient's good faith compliance with all applicable obligations.)

Force Majeure

The Principles

1. Force Majeure is an unforeseeable circumstance or extraordinary event that prevents a party from fulfilling its contractual obligations. Performance under a 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 may be excused from performing impacted obligations when performance is prevented or delayed by events defined as Force Majeure. Each party remains obligated to perform unimpacted obligations under the contract during Force Majeure and will be obligated to perform impacted obligations after the Force Majeure event subsides.

2. 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.

3. 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 may be adjusted by mutual agreement of the parties.

4. When a contract applies to a highly risky business or operational environment, the definition of a Force Majeure event should be specific to that situation and should expressly deal with the high economic and remedial costs of recovery, which may be disproportionate to the expected benefits flowing to each of the parties.

5. 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.

6. A Force Majeure event should not relieve the affected party from its obligations to perform unless the ability to perform is eliminated or materially impacted during the Force Majeure event. For example, if the Force Majeure event delays performance of an obligation by three days, the impacted party should be permitted to perform their obligation after the delay. However, if the only time to perform the obligation was during the time period of the Force Majeure event, then the obligation to perform is eliminated.

7. 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 the extent reasonable under the circumstances. It is fair to expect each party to prepare to some degree for possible "unexpected" events.

8. The affected party should also:

    a) 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

    b) notify the other party upon the cessation of the event of Force Majeure.

9. 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.

10. Consider whether rights to terminate or modify the contract should be included in the contract in the event of a severe disruption or extended disruption. However, termination or modification should typically be tied to or proportionate with the impacted obligations. For example, in a contract for services provided to multiple sites and only one site is impacted by a Force Majeure event, termination of the services at the other sites may not be proportionate or tied to the impacted obligations.

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

Applying the Principles to Contract Terms

1. Definition of Events of Force Majeure

Illustrative and non-exhaustive definition

1.1. 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.

Reasonably detailed definition

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

- **a)** Acts of God, natural disasters, earthquakes, fire, explosions, floods, hurricanes, epidemics, and pandemics that disrupt normal business activities, storms or other severe or extraordinary weather conditions, natural disasters,
- **b)** Sabotage, contamination, nuclear incidents,
- **c)** 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),
- **d)** Governmental actions, including new laws or regulations that materially impact the purpose of the contract,
  and

e) 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.

Examples of Force Majeure events

1.3. 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:

a) Non-availability or loss of export permit or license for the products/ solutions to be delivered, or of visas/ permits for supplier's personnel,

b) Requisition or compulsory acquisition by any governmental or competent authority, embargo, or other sanctions,

and

c) Currency restrictions, shortage of transport means, general shortage of materials, restrictions on the use of or unavailability or shortage of power or other utilities.

More detailed definition to meet specific needs

1.4. In situations where risks are expected to be higher than usual, the list of Force Majeure events should be more detailed to specify those risks so that it is clear which risks are borne by each of the supplier and the customer.

Force Majeure events and business continuity plans

1.5. When the affected party has committed to maintain an appropriate level of contingency and disaster recovery plans in order to ensure continuity of meeting obligations under the contract, execution of those plans should be linked to Force Majeure events, if applicable, but there should be no guarantee that the plans, even if fully executed, will be able to overcome all impacts of the event - after all, the very nature of Force Majeure is that all aspects of the event are hard to predict. Some obligations may have to be adjusted or delayed (e.g., for employee safety or to give priority to public needs.

2. Notice of Force Majeure

Illustrative and non-exhaustive definition

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

Relief

3.1. An event of Force Majeure should relieve the affected party from its performance obligations during the period of Force Majeure. The obligation to perform should remain (if possible) after the Force Majeure event subsides. Force Majeure relief should:

a) apply if an event of Force Majeure affects a subcontractor of a party;

b) continue for as long as the Force Majeure event prevails. The parties should also use their reasonable efforts – individually and collaboratively – to mitigate the effects of the event of Force Majeure upon their performance of the contract;

c) extend the time for performance, if possible. The 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. Change Control processes may have to be employed if the passage of time has a material impact on the supplier's costs or on the availability of products or services that were originally ordered;

and

d) 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.

Termination of contract

3.2. 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, consider permitting either party to terminate the contract, or relevant part of it, after that period and/or after a reasonable notice period.

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)

The Principles

1. Indemnifications generally do not encompass claims directly between the parties to the contract.

2. Although parties to a contract generally recognize that their acts or omissions under the agreement may affect third parties, the Indemnitor should only be expected to step into the shoes of the Indemnitee in taking on damages directly caused by the Indemnitor's acts or omissions under the contract.

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

4. Indemnitees 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 or by reasonably mitigating any damages incurred by the third-party.)

5. 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.

6. 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.

7. A party's indemnification obligations should be tied to its own acts or omissions under the agreement as well as that of its subcontractors and agents.

8. The indemnitor should have full control over the defense and settlement of the claim; however, the indemnitee should be permitted to approve any settlement that requires non-monetary performance by the indemnitee or requires that the indemnitee admit liability or take a public position that may adversely impact its reputation or market stature.

9. Unnecessary delays in notification to the indemnitor of a third-party claim that negatively impact the defense or settlement should be borne by the indemnitee.

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

Applying the Principles to Contract Terms

1. Scope of Indemnification Obligations

Indemnifications applicable to both parties

1.1. Each party should indemnify the other for third-party claims relating to

- **a)** bodily injury or death to the degree caused by the Indemnitor's fault,
- **b)** real or tangible property damage due to the Indemnitor's fault,

or

- **c)** where relevant to the services provided, employment matters brought by employees of the Indemnitor against the Indemnitee.

Indemnification for data breaches

1.2. Third parties may seek damages if their personal data is involved in a data breach. Inasmuch as it is frequently the case that both parties to the contract may have contributed to the loss, the parties should share liability to the third-parties proportional to their respective responsibility for the loss, typically through an indemnification. As part of an equitable risk allocation scheme, if the parties have agreed to a specific cap on liability for data breaches, it should apply to this indemnification liability.

Supplier indemnification for governmental fines

1.3. 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. The party that is the subject of the regulatory oversight should be the party that defends the fine or penalty.

Customer indemnification for its customers' claims

1.4. In agreements where the supplier may have an increased risk of being sued for the customer's actions, 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.

Specifying indemnitees

1.5. The Indemnitees should encompass the party to the contract and its officers, directors, employees, agents, and, if appropriate, subcontractors but should not include unrelated third parties.

2. Conditions for Indemnification

Obligation to mitigate damages

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

Preconditions for indemnification

2.2. Any obligation to indemnify for third-party claims should be subject to the following:

- **a)** 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.
- **b)** The Indemnitee must give prompt notice of the claim to the Indemnitor or relieve the latter for any incremental liability caused by the delay.
- **c)** The Indemnitee must provide reasonable support to the Indemnitor in defense of the claim.

d) 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.

e) The Indemnitor cannot agree to a settlement or outcome under which the Indemnitee admits to guilt or fault or undertake obligations without the Indemnitee's express written consent.

f) The Indemnitor cannot settle a claim or make any representations in the course of the defense in a way that would bring into question the reputation or goodwill of the Indemnitee without Indemnitee's express written consent.

and

g) 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.

3. Applicability of Liability Caps and Exclusions from Liability for Indemnification Obligation

Application of liability caps

3.1. 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 WorldCC Contracting Principle *Intellectual Property Rights and Indemnification for Third-Party IP Claims*).

Third-party claims treated as direct damages

3.2. Payment of third-party damages pursuant to an indemnification obligation should be treated as direct damages regardless of their nature, e.g., even if the settlement or award Includes consequential or indirect damages (but see an exception under the WorldCC Contracting Principle *Data Security and Privacy*).

Defined Terms

Indemnification: 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.

Intellectual Property Rights and Indemnification for Third-Party IP Claims

The Principles

1. Intellectual property ("IP") 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 IP must be expressly specified in the contract.

3. Where goods or services are provided by a supplier, the focus of the contract with the customer should be on their characteristics and functionality and how the customer can use them, and the customer should be able to rely on the belief that it will not be subject to any third-party IP infringement claims as long as it complies with instructions provided by the supplier and generally accepted practices.

4. The supplier should stand behind all intellectual property incorporated into the products, software and/or services conveyed under the contract and indemnify the customer against third-party claims that relate to them, subject to appropriate limitations.

Applying the Principles to Contract Terms

1. Intellectual Property Rights

Ownership of IPR

1.1. 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.

Customer gets a license to deliverables

1.2. 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 granting or transferring ownership rights are not applicable.

Scope of license

1.3. 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.

Clear license terms

1.4. 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.

Transfer of IP ownership for custom work

1.5. As to customized unique content that is developed for a customer’s sole use in accordance with the customer’s specifications (e.g., a custom software application), 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.

Third-party IP

1.6. Third-party software, services, and equipment are provided subject to the third-party’s license term.

2. Intellectual Property Infringement

Supplier indemnification of third-party claims

2.1. 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 a 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; provided, that the customer does not move the IP to countries that are outside of the jurisdictions permitted by the supplier.

Excluded third-party claims

2.2. The supplier should not be responsible to the extent an infringement claim arises from the following (“Excluded Claims”):

- **a)** combination of the supplier’s service or product with items provided by the customer or others not under the supplier’s control,
- **b)** modification to the supplier’s service or product by someone other than the supplier or others not under the supplier’s control,
- **c)** the supplier’s adherence to the customer’s requirements,
- **d)** the customer’s content,

  or
- **e)** use of the service by the customer in breach of contract restrictions or in violation of law.

Customer indemnification of third-party claims

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

Prompt notification of IP claims

2.4. The indemnified party should have the obligation to promptly notify the indemnifying party of any such claims. The indemnifying party should not be responsible for any incremental losses attributable to a notification delay by the indemnified party.

No liability cap in IP claims

2.5. The obligation to indemnify for third-party infringement claims should not be subject to any limitation of liability cap.

Prompt notification of IP claims

2.6. The indemnified party should have the obligation to promptly notify the indemnifying party of any such claims. The indemnifying party should not be responsible for any incremental losses attributable to a notification delay by the indemnified party.

No additional warranties or representations

2.7. The indemnification of third-party claims is sufficient to protect the customer. Therefore, the supplier should not also be expected to provide a warranty or representation that its services or products do not infringe third-party intellectual property rights. If supplier does provide such a warranty or representation, the sole customer remedy should be indemnity consistent with these Principles.

Supplier's remedies for infringing IP

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

- **a)** obtain from the third-party the right for the customer to continue its use of the IP in the service or product free from claims of infringement,
- **b)** modify the service or product so it is not infringing without materially reducing the functionality or performance of the service,
  or
- **c)** substitute another service or product having substantially the same functionality and performance criteria.

2.9. 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.

Insurance Coverages

The Principles

1. Parties to a contract should have reasonable assurances that if a claim or indemnification obligation were to arise, the liable party will have the financial capability to cover that liability. Having applicable insurance policies in place is one way to mitigate that concern, particularly with companies that may not have the size or capitalization to meet potential contract liabilities.

2. Although it may be appropriate for insurance coverage obligations to apply to both parties, typically, they are imposed on suppliers and subcontractors, given their more active role in contracts with respect to obligations that could give rise to breaches and damages, compared to customers, whose roles tend to trigger less need for insurance (e.g., payment of bills, acceptance of goods) in contracts.

3. While it may be justifiable to include a requirement that a contracting party must obtain third party insurance coverage in a contract, it may also be acceptable for a contracting party to self-insure (either on its own or through a captive insurer) if it is well capitalized with the financial resources to meet any foreseeable exposure under the contract (e.g., it is a Fortune 1000 company or a well-capitalized business and the limitations of liability are quite manageable).

4. Insurance clauses should specify the types of coverages the party(ies) will be required to maintain over the life of the contract and the coverage amounts. These types should reflect the specific risks that are applicable to the contract and relationship rather than based on a one-size-fits all approach. Factors to consider in determining which types of policies a party must maintain are

    a) industry norms,

    b) what products or services are being provided and the risks associated with them,

    c) size or value of the contract and applicable risk allocation(s),

    d) the costs of obtaining the applicable policies,

    and

    e) geographic availability of certain policies from reputable insurers.

5. Given the current focus on data protection and cyber breaches, there are growing requirements for related insurance coverages, particularly where potential liability for breaches is unlimited or limited by a super cap. Contracts should be clear as to which contracting party is liable in the event of a data breach/cyber loss and to what extent and whose insurance will cover the losses. This clarification is especially important for outsourcing or professional services contracts that provide digital data transfers, in which case the supplier should generally bear the risk for data breach/cyber events caused by the supplier's breach of a contractual obligation.

6. Generally, there are two different insurance products available:

    a) Cyber Liability Insurance, which addresses a supplier's cyber security issues with its network or disclosure of private information;
    and

    b) Data Breach Insurance, which is usually a part of a supplier's Errors & Omissions policy (also known as Professional Liability insurance) and provides coverage for a Supplier's failure of services.

    Policies can also be bundled to include both Cyber Liability and Data Breach.

7. Customers should consider liability carve-outs and limitations of liability, which can dilute the magnitude of any negotiated supplier insurance levels (i.e., liability caps are lower than the required policy amounts).

8. Typically, policy limits are a standard request based on the size of the supplier and the size of the potential claims under the contract (e.g., $2M, $5M, $10M). In general, there should be no need to demand insurance coverages that exceed applicable caps on liability under the contract. Other factors to consider are:

    a) potential damages if something goes wrong,

    b) nature of products or service (i.e., mission critical or minor routine operations),

    c) size of supplier (i.e., large multinational or small startup),

    d) with respect to cyber security, is supplier touching customer's personal data or health information,

    and

    e) what caps are applicable to supplier's liability.

    Generally, policy limits should be realistic, proportional, and commercially reasonable.

9. Contracts should ensure that required insurance policies (and coverages) are maintained through a reputable insurer (using a minimum rating level determined by an independent generally accepted rating agency such as A.M. Best) and that the other party is notified if the coverage is reduced or eliminated during the term of the contract. Certificates of Insurance should be provided upon request to certify that the insurance requirements continue to be met.

10. To the extent permitted under applicable law, parties should waive their respective Rights of Subrogation so as to avoid the other party being held liable for a claim, unless the waiver is prohibited in the applicable policies.

11. The presence of insurance covering a party's breach should not affect the other party's obligation to mitigate the damages and to prove the harm alleged. Nor should the breaching party avoid liability by demanding that the claiming party deduct from a claim what its insurance would cover.

12. Some policies preclude coverage for intentional misconduct or illegal acts - and those breaches may likely be subject to unlimited liability either explicitly under the contract or as a matter of public policy. Accordingly, insurance may not provide the intended protection to the other party in those circumstances.

Applying the Principles to Contract Terms

1. Types of Insurance Policies to Consider

Typical insurance coverages

1.1. Typical insurance coverages may include but are not limited to the following types of policies:

- **a)** Workers' Compensation
- **b)** Employer's Liability
- **c)** Commercial General Liability
- **d)** Motor Vehicle Liability
- **e)** Excess/Umbrella Liability
- **f)** Errors and Omissions
- **g)** Fidelity Bond or Crime
- **h)** Cyber Liability/Data Breach

Compliance with laws

1.2. The coverages should be compliant with any applicable laws or regulations, such as is often the case with respect to Workers' Compensation.

Specialized insurance coverages

1.3. Often, industries have specialized insurance coverages for the specific activities, environments, or risks associated with that market sector.

Coverage for Data Breach and Cyber Liability

1.4. To maximize coverage with respect to cyber liability and data breaches, the contract should clearly state the requirement for "Errors & Omissions / Professional Liability / Cyber Insurance", with a statement that the policy provides for Data Breach coverage and Cyber Liability coverage, including coverage for unauthorized access and use, failure of security, breach of confidential information, privacy perils, and breach mitigation costs and regulatory coverage. This language would cover almost all claims of this type that may arise.

2. Extent of Coverages

Subcontractors' insurance coverage

2.1. Customers should ensure that the suppliers' subcontractors and their acts and omissions are covered by suppliers' policies to the same degree as for suppliers' own employees.

2.2. Although there is a tendency for customers to require that a supplier's subcontractors also maintain relevant insurance coverages, if the supplier is responsible for the acts and omissions of its subcontractors and the subcontractors do not have contractual privity with the customer, that requirement should not be necessary. However, as between the supplier and its subcontractors, the supplier should seek appropriate insurance coverages in the event an act or omission of the subcontractor creates liability for the supplier.

Coverage limits

2.3. Insurance coverage limits should be applicable to each occurrence or to a series of occurrences arising from a single breach.

Data-related claims

2.4. Customers should make sure that suppliers' Data Breach and Cyber Liability coverages cover direct breach claims under the contract as well as third-party (indemnification) claims.

Alignment with supplier's contractual obligations

2.5. Insurance coverage should apply at the same point in time and for the same risks as supplier's contractual obligations. As an example, if supplier takes on liability for using or handling data, then the corresponding policy must also cover those same activities.

Additional Insureds

2.6. Parties typically asked to be named in the other parties' policies as an "Additional Insured". However, care should be taken if there is a potential for issues to arise with respect to who would pay for any retention or who would manage the claim process and coordinate with the insurer. Further, some insurance policy language may be used to avoid coverage if the Additional Insured has its own policy covering the event, or if it is deemed to be a claim against one insured versus another insured (by reason of the Additional Insured coverage).

3. Insurance Coverage Over the Life of the Contract

Right to request insurance certificates

3.1. A party should have the right to request an updated Certificate of Insurance annually, with the party indicated as an Additional Insured, if applicable.

Right to audit the other party's coverage of subcontractors

3.2. A party should also have the right to ensure (through informal requests for information or audits) that the other party's insurance covers acts and omissions of subcontractors, even as they come and go over the life of the contract.

Right to request changes in coverages

3.3. The change control process should be used if changes in scope, geographies or risks warrant revisions to the types of policies needed or the amounts of their coverages.

Defined Terms

Cyber Liability Insurance: generally, means a stand-alone policy consisting of both first-party and third-party coverages. First-party coverages for a cyber incident include
a) investigation costs,
b) costs to repair damaged or lost equipment,
c) lost revenue,
d) notification costs, and
e) credit monitoring and/or lost profits.

Third-party coverages provide protection from lawsuits against related to a cyber incident, and cover the costs related to third party claims such as
a) attorney fees,
b) settlements and/or judgments, and
c) any regulatory fines incurred.

Data Breach Insurance: offers only first-party coverages for losses related to a data breach, hack, or theft of company documents. The policies generally cover expenses associated with informing third parties affected by a breach to minimize the damage. This includes offering affected parties access to support like assistance hotlines and credit monitoring. Data Breach Insurance is usually not a stand-alone policy and is part of an errors & omissions policy.

Subrogation Right: is a right held by an insurance carrier to legally pursue a third party to the degree it caused the loss that is covered by the insurer. This is done in order to recover the amount of the claim paid by the insurance carrier to the insured for the loss.

Liability Caps and Exclusions from Liability

The Principles

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. In that situation, a certain act or omission under the contract will be liable for a pre-set amount even if the liquidated damages are materially higher or lower than the actual damages.

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, for direct damages, is typically set at a level proportional to the value of the deal or contract and 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). Neither party should be held liable for the acts or omissions of third parties not under its control.

6. Exclusions from Liability are generally accepted as a standard in commercial agreements, such as for indirect or consequential damages, 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 willful misconduct.

Note:
Liability Cap and Exclusions from Liability associated with indemnifications of third-party claims are also addressed in the WorldCC Contracting Principles *Indemnification of Third-Party Claims* and *Intellectual Property Rights and Indemnification for Third-Party IP Claims*. For data breaches, see also the WorldCC Contracting Principle *Data Security and Privacy*

Applying the Principles to Contract Terms

1. Reasonable Liability Caps

Liability Cap proportional to value of deal

1.1. 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.

Liability Cap options

1.2. 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.

Liability Cap not a defense against paying invoices

1.3. 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.

Higher Liability Cap for egregious conduct

1.4. 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.

Liability Cap survives contract

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

2. Exclusions from Liability

Exclusions from liability

2.1. 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.

Exclusion for lost revenue not a defense against non-payment of invoices

2.2. 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.

Exclusions from liability survives contract

2.3. 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

No Liability Cap or exclusions for breach of confidentiality or IP infringement claims

3.1. 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.

Willful misconduct and gross negligence

3.2. The liability of the parties for willful 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.

Bodily injury, death, damages to property

3.3. Subject to applicable statutes, liability for bodily injury and death should not be subject to the Liability Cap but may be subject to the Exclusions from Liability.

Additional exceptions to liability

3.4. 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 (super) Liability Cap, compliance with applicable laws, or compliance with tax obligations).

Defined Terms

Exclusions from Liability: 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.

Liability Cap: the monetary cap placed on a party's liability for damages arising under an agreement. Generally, the agreed upon Liability Cap will be:

a) a fixed amount,
b) a percentage of charges invoiced and/or paid over a period of time under the agreement, or
c) a combination of a) and b) (e.g., whichever is greater).

Unlimited Liability: 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.

Managing Price Volatility

The Principles

1. Long term contracts with long term commitments are extremely valuable to suppliers and customers by providing stability and predictability with respect to goods and services. However, those lengthy relationships may also create risks for the parties with respect to pricing, which may be subject to unpredictable changes over that period.

2. It is in the best interests of both parties to include protections within the contract so that neither party is materially harmed in the event of unforeseen price volatility during the term of the contract.

3. The most common causes of pricing volatility include:
    - **a)** Inflation that increases (or decreases) beyond what was reasonably foreseeable,
    - **b)** Labor rate adjustments that exceed expected trends,
    - **c)** Supply chain restrictions/materials cost increases that are impacting the industry more broadly,
    - **d)** Global trade policy changes (e.g., change in tariffs, duties),
    - **e)** Currency and/or exchange rate changes that go beyond expected trends, affecting cross-border transactions,

      and

    - **f)** Changes in interest rates for financed-based offerings.

4. The objective should be to create a pricing scheme that is fair to both parties, enabling the supplier to maintain a reasonable margin on its goods and services throughout the life of the contract while at the same time protecting the customer from material price increases that are imposed with little or no warning or are above market levels, without recourse.

Applying the Principles to Contract Terms

1. If Managing Price Fluctuations is not Warranted:

Short contract term	**1.1.**	The contract is for a relatively short period, and the prices can be fixed without the fear of unforeseeable, extreme external conditions affecting prices;
Small likelihood of volatility	**1.2.**	The solution is not materially impacted by price volatility (e.g., one-time fee paid for perpetual license, all charges are incurred within a relatively short period);
No minimum purchase	**1.3.**	There is no minimum purchase commitment;
Multiple alternatives in the market	**1.4.**	Multiple alternative sources exist in the market for commoditized, easily replicated solutions, so the customer is not locked into prices charged by just one supplier.

2. If Managing Pricing Fluctuations is Warranted:

Risk-adjusted pricing	**2.1.**	Consider negotiating a price that takes into consideration some level of pricing volatility. This allows the parties to share in the risk. Combining this approach with one or more of the other options below may enable a multi-prong approach to risk management
Discounts off of list prices	**2.2.**	Enable some level of pricing variation (up and down) while ensuring that value still falls to the customer via the discount. Since the discount will be based on a published list price, customer can be more confident that they will not be singled out by the supplier for price increases. This is especially useful for commoditized solutions.
Rate reviews	**2.3.**	Bring the parties together to review pricing on a periodic basis without the formality of benchmarking (covered below). Published indices and historical trends can be used in this exercise. However, the more a customer is prescriptive about how services are provided, the less a supplier may be able to mitigate against inflation, and so inflationary risks may have to be shared in those situations.
Benchmarking	**2.4.**	Allow for a periodic review of pricing to ensure that the parties are still sharing in the value of the deal. Benchmarking often utilizes an objective trigger (e.g., period of time, inflation rate, exchange rates). Note that while time-based triggers are very common in benchmarking clauses, this creates an artificial trigger point that may not be as effective in managing the pricing volatility risk.
Change orders	**2.5.**	Apply automated triggers and/or opportunities to amend the contract if the parties cannot reach mutual agreement on new price levels. For example, consider a clause that states that the parties will move into the Change Control process if inflation (or another quantifiable trigger) increases by more than X percent over a 12-month period.

Fixed price term

2.6. Provide fixed pricing for a term (either initial term or a term shorter than the term of the agreement). This helps lock in pricing for a period, while not necessarily locking in the pricing for the full term or for renewals. By shortening the locked-in period, pricing risk is mitigated.

Auto-adjustment

2.7. Another common method is to utilize an auto-adjustment such that the price is automatically adjusted by an agreed amount each year (e.g., price will increase by xx% each year on the anniversary date of the contract). This approach works best for solutions with a predictable pricing change over time and benefits customers by allowing them to budget for anticipated increases. However, it is not as useful for situations with significant price volatility.

Capped adjustment

2.8. In some cases, customers may be willing to absorb higher prices in order to achieve greater price predictability. In these cases, a limited right to price adjustment with a cap may be the ideal approach. For example, the parties may agree to modify pricing after a specified trigger, but also agree that pricing will never increase by more than xx% per year.

Changes in prices linked to inflation indices

2.9. Give the supplier the right to increase prices periodically in line with changes in an agreed, generally accepted inflation index, such as the Consumer Price Index or a local equivalent, in exchange for foregoing other pricing increases. However, the parties should decide whether the index selected is a good barometer of price changes within the industry or for the types of goods or services relevant to the contract.

3. Reasonable Advance Notice of Price Changes and Recourse if the New Price is Unacceptable

Amount of advance notice

3.1. The amount of advance notice of price increases should be a function of how long it would reasonably take to internally evaluate the change and how long it would take to assess market prices and obtain an alternative supplier if necessary.

Shorter notice period

3.2. The notice period can be shorter if the contract has a definitive price change mechanism so that the customer is well aware of the timing of possible changes and can predict the magnitude of the change (e.g., links to published inflation indices).

Customer's recourses for unacceptable price changes

3.3. Customers should have recourses if a price increase is above reasonable expectations and is higher than market levels. These actions can include cancellation rights, the right to dispute the increase, or the right to change quantities or volumes. The parties will need to ensure that the remedies are in line with the overall structure of the transaction and the types of goods and services involved. Where there are no alternatives in the marketplace or what is being provided is unique or customized for the customer, the recourses available to the customer may be more limited, but equity dictates that the customer is not subject to unfair price increases by the supplier.

4. Other

Right to change prices must be explicitly agreed

4.1. Customers should take care that their contract with the supplier specifically states whether a price increase can or cannot be made. If the contract is silent on this point, the supplier may seek to impose price increases on the basis that they are not specifically precluded. Specific language will also aid the customer in seeking recourse if they do not believe the price increase is supported.

Supplier's reasonable efforts to mitigate price increases

4.2. Suppliers should be under the obligation to use reasonable efforts to mitigate price increases. While it may not be practical in many situations to specify what those actions may be, the parties may be able to identify some specific steps the supplier can take given the specific products or services involved, their geographic locations, the duration of the contract, etc.

Opportunity for price reductions

4.3. In some cases, pricing volatility may also result in the opportunity for price reductions. Fairness dictates that the contract allow for bi-directional fluctuations, and the price protection clause should also allow for both up and down pricing adjustments under comparable rules.

Non-Solicitation

The Principles

1. Non-Solicitation provisions are appropriate in cases where one party is providing professional services or other services requiring unique skills to another party and wants to prevent its resources from being taken away by the other party.
The service provider may wish to use a Non-Solicitation provision to ensure it has resources to provide continuity of services to all of its customers and to prevent losses related to intellectual property, confidential information, and investments it has made hiring and training its Employees. Similarly, a customer may seek a Non-Solicitation clause to prevent a supplier from enticing people with industry knowledge or other marketable skills to benefit the supplier.

2. Non-Solicitation provisions may be unilateral or mutual. While seeking mutuality may help ensure the language is drafted fairly, there may be a rationale for unilateral terms. In case of using a unilateral Non-Solicitation provision, it may be useful to briefly indicate:

    a) that all parties agree that the unilateral provision is a fair requirement considering the nature of the transaction/purpose of the contract between the parties,

    and

    b) a brief description as to why a unilateral provision is necessary.
    Crafting of a unilateral provision in this manner may avoid challenges by the other party (under the Non-Solicitation obligation).

3. Non-Solicitation clauses should not prohibit a party from hiring people who respond to a General Solicitation or as a result of an individual seeking employment on his or her own initiative. Often companies do not have safeguards in place to comply with the terms of a Non-Solicitation provision that prohibits those sorts of activities in the job market. Further, such a restrictive covenant may not be enforceable if it restricts competition or the ability of Employees to have reasonable employment opportunities.

Applying the Principles to Contract Terms

Restriction of Solicitation

1.1. The word solicit means to ask and Non-Solicitation may refer to a number of different activities. Accordingly, the contract should clearly define Non-Solicitation as restricting a party from employing, seeking to employ, or otherwise enticing away the Employees of the other party. To increase the likelihood that a Non-Solicitation provision is enforceable, the language should be narrowly crafted to meet the business purpose. For example, a Non-Solicitation provision may be limited to a specific group of key Employees, such as the Employees that are providing particular services under the agreement.

Non-Solicitation Period

1.2. The Non-Solicitation Period should be clearly defined in the agreement. Typically, the period of time will be the term of the agreement and a reasonable period of time after the termination of the agreement, such as six months or a year.

Severability

1.3. Even a carefully drafted Non-Solicitation provision may be found to be unenforceable. Therefore, it is important to have a sufficient severability clause in the Agreement to cover that situation, or else the Agreement may be considered to be voidable/void/invalid.

Liquidated Damages

1.4. In some cases, the parties may wish to define liquidated damages related to a breach of a Non-Solicitation provision. The damages could be stated as a flat amount or as a percentage of the salary to be paid to the individual by the soliciting party.

Permitted General Solicitation

1.5. General Solicitation activities should be specifically excluded from being categorized as prohibited Non-Solicitation activities so as not to unfairly stifle employers' and employees' hiring and employment efforts. However, even if a person is hired by the other party pursuant to a permitted General Solicitation, the confidentiality language of the contract should be drafted to ensure that person continues to be obligated to protect the Confidential Information of their previous employer (see WorldCC Contracting Principle *Confidential Information*).

Defined Terms

Direct Solicitation: the act of one party actively seeking to hire, or hiring, a particular person or group of people to work for that party, either as direct hire or as a contractor, through a directed communication.

Employee: an employee, independent contractor, agent or other similar personnel of a contracting party and/or its subcontractors.

General Solicitation: using a general or widely distributed method to solicit or hire people or groups of people to work for a party, such as posting a general advertisement for hire or using a third-party intermediary hiring agency without focusing on particular or targeted individuals.

Non-Solicitation: prohibition of a party(ies) from employing, seeking to employ, or otherwise enticing away the Employees of the other party(ies).

Non-Solicitation Period: the period of time that one party must refrain from soliciting the Employees of another party.

Order of Precedence

The Principles

1. Parties should include an order of precedence clause in contracts whenever multiple documents form the complete contractual relationship between the parties and there is a possibility of discrepancies or inconsistencies among the documents. This helps to reduce the risk of interpreting the contract in a manner that differs from the intent of the parties at the time of entering into the contract.

2. The order of precedence must be clear, either in
   a) "ascending order of precedence" – meaning the top document in the list has the lowest priority, or
   b) "descending order of precedence" – meaning the top document in the list has the highest priority.

3. Order of precedence typically follows two key rules:
   a) more specific documents take precedence over more general documents, and
   b) documents entered into later in time take precedence over documents entered into earlier in time.

   Clarity in order of precedence clauses is especially important when deviating from these standards.

4. Order of precedence clauses do not apply where there is no conflict between two documents. If one document states that it specifically modifies a term in another document, then there is no conflict in terms. The same is true if one document covers a topic, situation, obligation, or liability not covered in another document.

5. Order of precedence clauses should cover all the components of a contract that may contradict each other presently or in the future, such as the main terms and conditions of a Master Service Agreement and attached Statements of Work (SOWs), orders, or exhibits that may differ from the umbrella terms for specific transactions or situations.

Applying the Principles to Contract Terms

1. Crafting an Order of Precedence Clause

Identifying the contract documents

1.1. Identify the various documents that make up a contract. Common documents that supplement the main terms and conditions include Quotations, Order Forms, Statements of Work/Service Descriptions, Product Warranty Statements, and Product Specifications. Other documents may include Data Privacy Terms, Cybersecurity Terms, Business Conduct (anti-bribery, sanctions, modern slavery,

human rights) Terms, and Site Requirements. Do not forget linked documents (e.g. terms on a website that are incorporated by reference) and documents or amendments that might be added after the initial execution of the agreement.

Order of precedence of secondary documents

1.2. Consider the order of application of appendices, addenda, exhibits, schedules, and attachments to the document. For example, if the main document covers all terms for most cases, but a secondary document modifies some terms for a special case, that secondary document should take precedence for that case. Ideally, best practice would be to explicitly highlight those deviations in the secondary document, but, for the sake of clarity and completeness, the secondary document should be higher in the order of precedence.

Setting out the order of precedence

1.3. Identify and rank the documents based on which should take priority if there is a conflict in the terms. Decide whether to list them in ascending or descending order.

Consider each party's practical concerns

1.4. If a party has internal business limitations or concerns (e.g., not having legal oversight of documents such as order forms that might include legal terms), these should be considered when setting the order of precedence. The parties can either agree to a less-than-ideal order of precedence to address the concerns (e.g., having the MSA take precedence of any orders), or the concerned party can agree to mitigate the concerns within that party's internal administrative processes.

Order of precedence review as the contract evolves

1.5. The order of precedence may need periodic review, especially if the agreement is frequently amended, new documents are added, or there are significant changes from the original scope.

2. When Order of Precedence is Not Relevant

Express precedence language in clauses

2.1. If only certain clauses in a document need to take precedence, state that clearly within the clause itself to eliminate the conflict. For example, state "*Notwithstanding anything to the contrary in Section x.x of Document Y, this Section z.z shall take precedence*." This explicit language removes uncertainty, and the issue of order of precedence will not arise.

When provisions do not overlap

2.2. If documents do not overlap in terms of obligations, rights, liabilities, etc., then the order of precedence is not applicable. For example, if one document specifies payment terms and the other does not, there is no conflict between the two documents, and the order of precedence is not relevant.

Payment Terms

The Principles

1. Payment Terms should specifically address when payment is due, invoicing requirements, early payment discounts, invoice dispute resolution procedures, methods of payment and acceptable currencies, supplier protections against late and non-payments, and any applicable Setoff Rights.

2. Payment terms should be fair and balanced, taking into account the financial interests of both supplier and customer and the criticality of the goods or services provided to the customer.

    a) A supplier has an interest in minimizing its financial exposure by reducing the amount of time between delivery of goods or services and time of payment, so as to reduce the time to recoup its investment in the provided goods and services and pay any related expenses.

    b) A customer has an interest in extending the period of time between delivery and payment, so as to provide customer with additional time to use the available monies for other business activities and to inspect and test the goods or services to confirm they are satisfactory.

3. Suspension or termination or even a formal allegation contending breach of contract should be a last resort to late or non-payment and should be used only after all other remedial actions (e.g., written notice of breach, escalation) have been exhausted.

4. Remuneration should be due after the customer has an opportunity to inspect the goods or services to ensure they conform to specifications set forth in the contract or, if none are stated, to generally accepted standards.

5. Significant recurring payments for ongoing services should preferably be made in such manner as to provide the supplier with a neutral cash flow (i.e. the time of payment receipt closely approximates to the time the supplier needs to make payments for resources used to provide the services), which helps the supplier to provide its best pricing. Invoicing and payments for charges for one-off services (e.g., time and material) or usage-based services (e.g., user-based licenses or minutes-of-use charges) should be in arrears.

6. Advance payment provisions (such as for deposits or one-time payments) are appropriate for circumstances such as when a supplier needs the funds to offset the costs of special parts or equipment it needs to provide the goods or services, or when a supplier is providing custom goods with limited resale value.

7. Optional advance payment provisions may be used to provide benefits to both supplier and customer, especially if the customer is given a payment discount or other preferential terms in exchange for the optional advance payment.

Applying the Principles to Contract Terms

1. Payment Terms

Clear timing for payments

1.1. The contract should state a fixed period of time (e.g., 30 days) for when payment is due following the customer's receipt of the invoice or a defined period of time after the invoice is sent. In some industries, such as construction, the parties can agree that payment is made when the payor receives funds from a third party ("pay when paid" or "pay if paid").

Electronic Invoicing

1.2. When possible, invoices should be sent electronically in a trackable receipt format. If not sent electronically, the parties may contractually agree that the supplier will notify the customer when the invoice is sent, and the customer will notify the supplier when the invoice is received. If the customer does not notify of receipt or of failure to receive, then the invoice should be deemed received within the predefined period of time after being sent. Where possible, suppliers should maintain an online repository of invoices accessible by customers as a backup for records of invoices sent. If a customer requires that a supplier use a specific invoicing system, that must be specified in the contract. The parties should address any extraordinary costs incurred by the supplier in interfacing with that system.

Invoice details

1.3. Invoices should reference applicable purchase order(s) and be clear so as to provide sufficient detail for the customer to identify the goods and services to which the billed amounts (and taxes and surcharges as applicable) relate. A clear linkage between the invoiced amounts and the applicable contract or order will minimize disputes and hasten payment.

2. Dispute Rights

Right to dispute invoices in good faith

Customer should always have the right to dispute invoiced amounts in good faith and for a reasonable time period as agreed in the contract. To exercise this right, customer should provide written notice or as otherwise determined in the contract (e.g., dispute resolution clauses) of the disputed amount and the basis for the dispute. All amounts that are not disputed should be paid within the required payment period. Fairness dictates that interest should not be imposed in cases where a charge is disputed in good faith and based on reasonable grounds but ultimately found to be legitimate and payable.

3. Interest and Late Payment Charges

Supplier right to charge interest on late payments

3.1. To protect against late payments, supplier should have the right to assess a reasonable interest charge on undisputed late payment amounts after all notification obligations are exhausted. The rate of interest set forth in the contract must be clearly stated and cannot violate applicable Usury Laws.

Supplier right to recover collection costs

3.2. Supplier should also have the right to recover its substantiated and reasonable costs to collect the late payments; provided that such collection costs are reasonable and customary for the type of debt owed.

4. Additional Assurances

Supplier right to demand proof of ability to pay

4.1. Where appropriate, the supplier should have protection rights for when the supplier has reasonable uncertainty about customer's ability to pay (e.g., history of late payments, negative change in customer's credit rating). The supplier should have the right to demand adequate assurances that payment will be made based on the facts and circumstances that gave rise to the uncertainty.

Examples of assurances

4.2. Examples of such assurances are:

- **a)** The customer issuing a letter of credit to respond to the supplier's concerns about customer's financial situation;
- **b)** The supplier requesting a guaranty from customer's parent company or investor if customer's creditworthiness is at issue;
  and
- **c)** The customer's payment of all outstanding invoices and payment of future invoices in an abbreviated payment period, if customer has a history of chronic late or non-payments. Once customer shows it can timely meet its payment obligations, the customary payment period can be reinstated.

5. Setoff Rights

Setoff Rights

5.1. Contractual Setoff Rights may be appropriate where supplier and customer are engaged in multiple transactions with purchases being made by both parties from the other, and supplier and buyer have mutual payment obligations (i.e., where supplier regularly sells to and buys from customer).

Exercising Setoff Rights

5.2. If Setoff Rights are permitted, the contract should include what debts may be setoff, the amount of notice required to effectuate the setoff, and the procedure for setting off amounts if different currencies are used.

Waiver of Setoff Rights

5.3. If a Setoff Right is not to be used, the contract might include an express waiver of the parties' common law and statutory Setoff Rights (a/k/a. no setoff provision) to make it clear those rights are not intended to apply.

Defined Terms

Payment Terms: the terms applicable to how and when a customer pays the charges for goods or services provided by a supplier and they may address penalties for late or non-payment.

Setoff Right: the right of either party, as applicable, to set off and keep any payment that is otherwise owed to the other party against amounts that are owed to the paying party.

Usury Laws: the laws of the applicable territory which limit the amount of interest that may be imposed on late payments in the course of business-to-business transactions.

Prices and Charges

The Principles

1. The parties to a contract must clearly document how much will be charged for goods or services; the structure of the charges (e.g., fixed, time and material, volume based), when and where the charges will be invoiced; the currency that will be invoiced and paid; and when the invoices must be paid. These elements can be specified in the contract (typically, Pricing Schedules) or in orders or Statements of Work that are executed pursuant to the contract.

2. Suppliers should not have the right to change Charges during a fixed term of the contract, except under circumstances explicitly stated in the contract. Appropriate prior notice should be given to the customer in the event of any increase in Charges, giving the customer reasonable time to migrate the products or services to a different supplier at the end of the current term if it chooses not to accept the increases. The parties may choose to agree on a cap on the size of any increase in any specified period (perhaps linked to a specified inflation index) or to periodic adjustments (typically at intervals of no more than twelve months). See WorldCC Contracting Principle *Managing Price Volatility*.

3. The ability of a supplier to back-bill for Charges that were erroneously omitted from past invoices as well as the ability for a customer to contest Charges in past invoices should be restricted to specified timeframes (perhaps linked to the frequency of audits, per the bullet below), and, in fairness to both parties, should be the same period for both sides.

4. Customers should have a right to review and audit supplier records to confirm the accuracy of invoiced amounts. Similarly, suppliers should have an audit right if Charges are volume dependent, such as number of users. Any such reviews or audits should be conducted pursuant to mutually agreed processes, scopes, and times and should be limited to once per year unless the customer has good reason based on criteria set forth in the contract. The parties should decide on who bears any audit costs (e.g., each party bears its own costs unless errors in excess of an agreed level are found). Audit provisions should also allow for audits conducted by regulators, if applicable.

5. To the extent a supplier has a right to charge a customer for certain items, but the specific amounts are not known in advance (such as travel, costs of refurbishing supplier equipment after customer's misuse, or requests for activities not within the original scope of the contract), the customer should be given as much prior notice as possible of the imposition of those Charges and an estimate of how much they will be. In some cases, change control processes can apply so that the customer is able to approve the exact additional Charges in advance. In other cases, a cap on these charges may be specified, with express written approval required to exceed that limit.

Applying the Principles to Contract Terms

1. Structure of Charges

Clear explanation of Charges

1.1. A clear explanation of how Charges will be calculated will minimize uncertainty and disputes when the customer receives invoices from the supplier. Invoices should have appropriate supporting documentation as required by the contract. In addition, if certain events trigger the imposition of Charges, those should be clearly defined. (e.g., are Charges for goods invoiced upon shipment, delivery, installation, or acceptance? Are Charges invoiced in advance of the provision of services or in arrears?) In situations involving the international shipment of goods, references to specific Incoterms will dictate which party is responsible for the payment of costs associated with the transit.

Use of explanatory examples

1.2. If there is any degree of complexity in calculating the charges, examples in the pricing schedules or exhibits will provide clarity.

Types of Charges

1.3. Charges often fall into several categories, which should be clearly set forth in the contract:

- **a)** Those that are one-time (e.g., installation Charges, purchase price for goods, up-front software license fees that are not dependent on user or other variable quantities, milestone payments, or termination Charges).
- **b)** Those that are recurring and fixed for periods of time, e.g., monthly, quarterly, or annually.
- **c)** Those that are based on volumes that vary during each billing cycle, e.g., usage fees or variable software license fees based on the number of users.
- **d)** Charges that are variable but follow a pre-set mechanism, e.g., a base monthly fee but one that increases if the number of users exceeds a certain threshold; or Charges that follow a step function (increasing or decreasing when a different pricing band applies).

Prompt notice of one-off Charges

1.4. When an event would trigger Charges, unless it is an event readily apparent to the customer, the contract should require prompt notice to the customer that the event has taken place so that the customer can anticipate the Charges and ensure the invoice will be handled appropriately when it arrives.

2. Taxes and Other Governmental Fees

Applicable taxes

Although not within the scope of this Contracting Principle, tax language is typically included within the Charges clause in contracts. Here, too, the contract should be clear on where invoices will be issued and delivered and what tax obligations apply.

3. Exchange Rates

Currency conversions

3.1. If billing will be in a different currency than the Charges listed in the contract, order, or Statement of Work, the parties should agree on how the conversion is to take place. Is the exchange rate fixed for a certain period or will the exchange rate be

calculated for every invoice based on a rate published by a particular bank when the invoice is created? The customer's accounts payable department should be able to confirm that the right amount is being invoiced based on documentation provided to it either in the governing documents or in the invoice itself.

4. Central vs Local Billing

Location of invoicing

4.1. Customers may want to stipulate where they receive invoices (and whether they are to be submitted physically or electronically) and whether they want to have subsidiaries invoiced directly for the goods and services they receive. This may require a local country agreement between the respective local entities of the customer and supplier or, at least, a local order that flows down the terms of a global contract to the respective local affiliates.

Consequences of cross-border billing

4.2. The parties should fully understand the tax consequences of central vs local billing and whether cross-border billing creates an unintended taxable presence on the part of the supplier within a country. Similarly, Charges may be dependent on whether goods flow between countries or where cloud-based services are provided.

5. Audit Rights

Extent of audit rights

5.1. See the WorldCC Contracting Principle *Customer Audit of Suppliers* for additional guidance on the structure of audits as it applies to audits related to the accuracy of invoices.

Applicability of invoice audits to subcontractors

5.2. To the extent that Charges are related to volumes or activities on the part of the supplier's subcontractors, those entities may need to be subject to a customer's audit rights. Care needs to be taken by the supplier to ensure that its contract(s) with relevant subcontractor(s) contain flow-down provisions enabling those audits to take place. See the WorldCC Contracting Principle *Subcontracting*.

Defined Terms

Charges: any prices and charges that will be invoiced by the supplier to the customer during the term of a contract, whether on:

a) a one-time basis (e.g., installation or termination Charges);
b) a per-event basis (e.g., time and material, milestone, or consulting Charges);
c) volume-based (e.g., usage or user license Charges);or
d) an ongoing basis (e.g., flat monthly recurring Charges).

As used in this Contracting Principle, Charges exclude applicable value added, sales and use, and similar taxes, governmental fees and surcharges, etc.

Requirements for Accessing the Other Party's Assets

The Principles

1. Every business has a right to take reasonable steps to safeguard its employees, assets and operations. This includes the right to require its business partners to comply with reasonable rules if they have access to those assets, which may include internal systems, data, equipment, or proprietary operational processes.

2. The security requirements that can be imposed on the other party can go beyond mere confidentiality and data protection (see WorldCC Contracting Principles *Confidential Information* and *Data Security and Privacy*), particularly when it is anticipated that a supplier's Personnel[1] will have direct – and perhaps unsupervised – access to valuable and sensitive assets.

3. The security and screening requirements imposed on a supplier's Personnel should be proportional to the degree to which they have access to assets (either remotely or in person), the sensitivity of those assets, and the degree of access (e.g., read-only vs. ability to download or modify). These requirements may be comparable to those that apply to the customer's employees when being hired or during periodic checks.

4. If supplier Personnel may be visiting the customer's premises from time to time but will be escorted during those visits, it is reasonable that they merely be required to follow the same rules that generally apply to visitors to those facilities (e.g., sign-in, picture on temporary badge, limits on where they can go).

5. In no instance should a customer impose requirements on supplier Personnel that violate any applicable laws or regulations (particularly with respect to privacy and confidentiality).

6. Parties should anticipate the possibility that security and screening requirements may change over the life of the contract either due to new types of risks or threats or due to changes in applicable laws or regulations.

7. The parties to the contract should look to each other for liability for failure to comply with these requirements or for damages due to the acts or omissions of Personnel. It is unreasonable to require that Personnel have personal liability to a customer for any wrongful act, and any requirement that creates that exposure, such as a mandate that Personnel sign personal confidentiality agreements with a customer, may deter the most capable people from performing needed work.

[1] Although this Principle has been written under the more prevalent scenario where it is the customer who is seeking protection of its assets from suppliers who access the customer systems or premises, there may be instances where the reverse is the case. In those situations, the same Principles should apply, but the obligations would be switched.

Applying the Principles to Contract Terms

1. Establishing Reasonable Requirements

Requirements tailored on type of access

1.1. Parties should not rely on a one-size-fits-all approach in setting requirements for supplier Personnel. Rather, the requirements should be tailored to the functions performed by the Personnel and the types of assets to which they have access. In all cases, access should be limited to only that required to meet the supplier's obligations under the contract.

Criteria to distinguish Personnel

1.2. For example, Personnel might be distinguished by any of the following criteria, with each having different security or screening requirements:

- **a)** Will they be badged by the customer and permitted relatively free access within the customer's premises?
- **b)** Will they always be escorted while in the customer's facilities?
- **c)** Will they have password access to internal customer systems and data?
- **d)** Will they only operate outside of the customer's firewalls or be permitted only to read but not modify or download Personal Data?

Examples of requirements

1.3. The customized requirements for these or other classifications may include, but not be limited to

- **a)** assuring that the Personnel are screened and undergo background checks at the time of employment,
- **b)** undergoing the same level of scrutiny that the customer's employees undergo,
- **c)** having the supplier be responsible for ensuring that all Personnel comply with confidentiality obligations,
- **d)** requiring that Personnel comply with the customer's Code of Conduct,
- **e)** limiting the manner in which passwords, data and other sensitive information are stored or transmitted,

and

- **f)** having Personnel undergo appropriate Data Privacy training to ensure compliance with customer policies.

Supplier responsible for Personnel's confidentiality obligations

1.4. Consistent with Principle 7, above, it is not recommended that Personnel be asked to execute personal confidentiality agreements with customers. The supplier should be prepared to accept responsibility and liability for any wrongful acts on the part of Personnel, particularly in connection with breach of confidentiality or misuse of assets.

2. Meeting Obligations in Light of the Requirements

Considering background checks and other screening procedures

2.1. When setting timelines for deliverables or project completions, suppliers should take into account the time required to comply with agreed security and screening requirements. Background checks and other screening procedures take time, and some Personnel might not agree to undergo the process or may actually fail the checks, necessitating a search for qualified replacements.

Maintaining compliance

2.2. The requirements will apply throughout the life of the contract, so Personnel changes (including those that are unforeseen) will necessitate additional administrative actions to maintain compliance. This should be taken into consideration by the supplier in staffing for the relationship and in setting contractual commitments.

Customer's right to refuse particular Personnel on reasonable and lawful grounds

2.3. Customers should retain the right to refuse the use of any particular Personnel based on reasonable and lawful grounds, e.g., failure to comply with standards of conduct or requirements of the contract.

2.4. Suppliers should have the right to be notified in writing of the grounds of the rejection and opportunity to cure (if curable).

2.5. Any dispute arising from the denial of access should be handled pursuant to the dispute resolution clause of the contract.

2.6. In the event that Personnel must be replaced at the request of the customer, the supplier should be given a reasonable timeframe to identify a replacement and to comply with any applicable screening requirements.

2.7. Inasmuch as the supplier should be held accountable for all acts and omissions of its Personnel while performing pursuant to the contract, it should be liable for any missed deadlines or disruption in deliverables due to the transition to new Personnel.

2.8. On the other hand, the supplier should be relieved of its relevant obligations if the customer acted unreasonably in denying access.

2.9. Lastly, the parties may want to provide for equitable relief to the supplier if the incident that gave rise to the denial of access was totally unpredictable and unpreventable.

3. Who Bears Costs

Costs to meet special requirements

3.1. The customer should bear the out-of-pocket costs incurred by the supplier to meet any requirements that are above and beyond what the supplier would have expended in its normal course of business or that do not have a reasonable basis. These costs can either be included in the costs of goods sold when setting prices or invoiced separately.

Possible exceptions

3.2. In some cases, such as when a background check is to be conducted just prior to Personnel being given customer badges and the supplier would not have otherwise performed a background check at that time, the parties should agree on who bears the out-of-pocket costs.

Costs for training

3.3. In the event that the customer requires that Personnel participate in any special training associated with proper conduct while on the customer's premises or when accessing certain assets, the parties should also agree on who pays for that training.

4. Privacy of Personal Information

Lawful processing and disclosure of personal information

4.1. Typically, personal information pertaining to the Personnel is central to these requirements. Local laws and regulations will not only dictate what screening information can be collected, but also the degree to which the information can be shared with the customer. To the extent the customer requires that a background check be conducted, a certification by the supplier that the Personnel has successfully completed the process should be sufficient without sharing the details of the check.

Supplier performs background checks

4.2. Although customers often ask for a contractual right to conduct background checks of supplier Personnel, given the sensitivity of the information involved, the supplier should be the one performing this exercise.

Scope of inquiry and disclosed findings

4.3. The parties should agree on the scope of the inquiries, consistent with local laws and regulations, and that the check will be conducted using generally accepted processes and agencies.

4.4. Generally, there is no need for the customer to be given the background check findings, but rather, the contract should stipulate that the supplier will only use Personnel who have passed the background check.

Customer's audit rights

4.5. The customer may demand audit rights to ensure the proper procedures are being followed, but the customer (or its auditor) should not have access to the personal information related to any Personnel (i.e., the personal information should be redacted in any records shown during the audit).

5. Accommodating Changes in Requirements

Addressing impacts of changes equitably

5.1. The contract should anticipate that security and screening requirements may change over the life of the contract due to the identification of new risks or changes in market standards. Any changes that materially affect then current Personnel, result in incremental costs to the supplier, or impact the availability of skilled Personnel for the work should go through change control procedures to ensure that impacts are equitably addressed.

Customer must give advance notice of changes

5.2. The customer should be required to give the supplier as much advance notice as practicable of these changes.

Defined Terms

Personnel: a party's employees, agents, and consultants and those of its subcontractors.

Service Level Agreement Remedies

The Principles

1. While suppliers intend to provide high quality services, SLA Failures can occur over time given the complex nature of technology services. SLA Failures, by themselves and in the absence of negligence or willful misconduct, should not be deemed to rise to the level of a material 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.

5. In some cases, the parties may wish to supplement or replace SLAs with Key Performance Indicators (KPIs) and/or Service Level Objectives (SLOs), which specify additional performance parameters that will be tracked and objectives that the supplier will strive for but not be liable for if not met.

Applying the Principles to Contract Terms

Reporting	**1.1.**	Suppliers should make performance reports available on a regular basis.
SLAs tailored to services	**1.2.**	SLAs should take into account both the complexity and the criticality of the services. More robust SLAs also provide opportunities for suppliers to earn SLA Credits back for extended periods of good performance following an isolated failure. This provides an incentive for lost term remediations.
SLA credits based on quantitative standards	**1.3.**	SLA Credits should be based on quantified performance standards set out in the contract.

SLA credits not penalties

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

SLA remedies are sole and exclusive

1.5. SLA Credits should be the sole and exclusive remedy available to the customer for Service Level Failures, other than for Chronic SLA Failures.

Termination as a remedy

1.6. In the event of a Chronic SLA Failure, customers should have the additional right to terminate the affected service without penalty, following executive escalation.

Exclusions from SLA responsibilities

1.7. 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 Failure occurs 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,
  and/or
- **g)** customer's use of non-standard products and services not approved for use by supplier.

Defined Terms

Chronic SLA Failure: 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.

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

SLA Credit: the credit provided by a supplier to a customer for an SLA Failure.

SLA Failure: the failure of supplier to meet its obligations under an SLA.

Step-In Rights

The Principles

1. A party should have the right to take appropriate steps to ensure it receives the negotiated benefits of a contract if the other party fails to deliver on its promises under the contract and is deemed incapable of delivering in the future. More times than not, the aggrieved party will seek monetary damages.

2. However, Step-In Rights may be more important to a customer[1] than just breach of contract damages if the goods or services being provided are specialized, mission critical, and/or alternate services are not available for cover during the period in which Supplier is unable to perform.

3. The nature of the transaction and the customer's ability to take over the supplier's obligations will dictate whether Step-In Rights can achieve the desired results. Factors such as the complexity of the deliverables, availability of necessary knowledge and skills, needed licenses and access to software code, and the presence of alternative suppliers in the marketplace will determine the practicality of Step-In Rights as a viable remedy.

4. Before negotiating Step-In Rights, the customer should thoroughly evaluate the potential scenarios that would give rise to exercising those rights, how long it would take to implement them, the associated incremental costs above and beyond the original prices paid (which, in many jurisdictions would be considered direct damages), and likelihood of the successful assumption of the obligations.

5. When software is involved, either as the deliverable itself or as part of a product, the exercise of Step-In Rights, particularly when maintenance of the software is required, may entail the need to access source code and to be able to fix bugs in what may be very complex programs and algorithms.

6. The dependency on trade secrets may interfere with Step-In Rights if the supplier is not obligated to disclose them.

7. In some cases, equitable relief leading to a court order compelling the supplier to comply with contract terms may be a viable route, but if the supplier is just not capable of delivering the goods or services, Step-In Rights may be the only solution.

8. When exercising Step-In Rights, the customer continues to have the obligation to mitigate its damages and to take reasonable steps under the circumstances so as not to unreasonably overstate its damages.

[1] Although either party to a contract can demand Step-In Rights, for simplicity, this Principle assumes that in a typical commercial transaction, it is the customer who normally asks for them.

Applying the Principles to Contract Terms

1. Parameters for Exercising Step-In Rights

Reasonable time to remedy breach

1.1. As with any breach remedy, the party wishing to exercise Step-In Rights should provide a reasonable time for the other party to cure the applicable breach before the rights can be exercised.

Step-In Rights only for specific breaches

1.2. Given the magnitude of the decision that one party will take on the obligations of the other party, the parties should try to specify the scenarios that would give rise to the Step-In. All other breaches should be dealt with through other remedies such as claims for damages or termination rights.

Additional damages on top of Step-In Rights

1.3. Consider whether the customer should be entitled to breach damages from the supplier in addition to its Step-In Rights. If the Step-In Rights make the customer whole, then additional rights to traditional breach of contract claims may not be warranted.

However, if the Step-In Rights are partial, then additional claims or causes of action should be permitted.

Further, any out-of-pocket costs incurred by the customer in Stepping In (e.g., hiring of skilled employees or contractors, training, purchases of additional equipment) should be considered direct damages for which the supplier should be liable if those costs exceed what the customer would have paid the supplier in the normal course.

No interference with supplier's obligations to other customers

1.4. In situations where a supplier is providing a service to multiple customers, the parties need to ensure that the customer can exercise its Step-In Rights for its own benefits without interfering with the supplier's obligations to its other customers.

Protecting supplier confidential information

1.5. Additional protections may need to be put in place to protect supplier Confidential Information if the customer has to bring in third parties to perform key functions.

2. Step-In Rights VS. Hiring a New Supplier

Hiring a new supplier more prudent than Step-In

2.1. In cases where alternative suppliers are available in the marketplace, it may be more prudent to declare a material breach on the part of the supplier and exercise termination rights, leading to a new contract with a different supplier instead of Step-In Rights.

Factors guiding the decision to Step-In vs. hiring a new supplier

2.2. The decision on which route to follow will depend on, among other factors:

a) the time necessary to implement the Step-In Rights vs. the time to select a new supplier and get it up to speed on the requirements;

b) the availability of a supplier with comparable qualifications as the original supplier;

c) the ability to use another supplier that is a competitor of the original supplier without divulging sensitive confidential information belonging to the original supplier;

and

d) the willingness of the new supplier to pick up where the first supplier left off.

Extra costs of hiring a new supplier = direct damages

2.3. As stated in Section 1.3, above, the incremental costs of the new supplier over that of the original one is treated as cost-of-cover, i.e., direct damages, in many jurisdictions.

3. Can the Customer "Step-Out" After it has Stepped-In?

Specified duration of Step-In Rights

3.1. Step-In Rights may be needed to complete a specific project or to perform ongoing activities (e.g., maintenance) over an extended period. The parties may want to specify the duration of the Step-In Rights either based on time or upon certain milestones.

Transition plan to move obligations back to the supplier

3.2. Upon the end of the exercise of the Step-In Rights, if the parties wish to continue their relationship under the contract (which may not be tenable given the acrimony that usually accompanies the exercise of Step-In Rights), they will want to establish a transition plan to move the obligations back to the supplier with a new set of obligations that are appropriate – and achievable – under the circumstances. This will require the transfer of information as part of the transition to ensure the original supplier is back up-to-speed on the services' current state.

Defined Terms

Step-In Rights: the right of a party to take over the obligations of the other party to satisfy all relevant terms of the contract in the event that the other party fails to perform its obligations under the contract.

Subcontracting

The Principles

1. As solutions to customers' needs and the breadth of offerings become more complex and require expertise and technology not necessarily resident in one single supplier, it is common for suppliers to "team" or "partner" with other companies to meet those customer requirements. However, customers rightfully look to suppliers to serve as their sole contracting party (i.e., prime contractor) with respect to the entire solution or scope of work being provided.

2. The supplier should take full responsibility for ensuring that the entire solution works, or the entire scope of work is delivered and performed as contracted for, including those elements provided by Subcontractors, as if the supplier was providing the solution/scope of work entirely by itself. Accordingly, the supplier should accept liability (subject to the applicable limitations and exclusions) for all acts and omissions of Subcontractors in connection with the transaction.

3. If the customer and supplier have agreed to certain terms that apply, either explicitly or implicitly, to Subcontractors, it is the supplier's responsibility to ensure that those terms are flowed down to the Subcontractors as appropriate. Similarly, terms mandated by a Subcontractor may have to be flowed up to the customer to ensure that the supplier, who may be liable to the Subcontractor for acts or omissions of the customer, is not in breach of the Subcontractor contract.

4. With respect to software licenses, it may be appropriate for Subcontractor licenses to flow directly to the customer, in which case those licenses create contractual privity between the customer and the Subcontractor for that limited purpose.

5. Except as set forth in Principles 6 through 10 below, as far as possible, the sharing of responsibilities between the supplier and its Subcontractors should be transparent to the customer, and the customer should not have to undertake any role in overseeing the activities of Subcontractors.

6. The extent to which a customer should have the right to pre-approve Subcontractors should be a function of the access any Subcontractor has to the customer's sensitive information or internal networks or databases or if the Subcontractor will be badged or given the freedom to work in a customer location on an unescorted basis. Customers may also have a right to pre-approve any Subcontractor if it will be providing a very large proportion of the overall solution or work. However, if the supplier will be unable to provide its solution/services/product without the use of certain Subcontractors, it is important that the supplier should request for pre-approval of the use of such Subcontractors in the contract itself (as opposed to waiting to ask for that consent post-contract) and, If need be, state that without use of that Subcontractor, it may be impossible for the supplier to provide the solution/service/product to the customer at the agreed price or under the same terms (e.g., SLA).

7. A customer should have a right to approve or reject a Subcontractor if it is a competitor to the customer (albeit in some cases the customer may not have a choice but to approve a competitor if it is the only provider of a key component of the solution, in which case it is fair that the customer impose additional confidentiality safeguards to protect its interests).

8. Customers have a right to impose the same requirements on Subcontractor employees as they do on supplier employees (e.g., background checks, adherence to confidentiality obligations, prohibitions to human trafficking and child labor, compliance with security policies) if the Subcontractor personnel will be performing particular functions or activities that are the subject of those requirements under the customer-supplier contract.

9. A customer should have the right to require the supplier to remove and replace a Subcontractor or a Subcontractor's employee if either engages in activities that violates applicable customer policies or procedures or that are illegal.

10. The supplier should ensure that any audit rights a customer may have under the contract are extended to its Subcontractors who are performing functions or have obligations that fall within the scope of permitted audits (e.g., audits related to activities that form the basis for charges).

11. Personal data handling, data protection, and the movement of data across jurisdictional lines need to reflect activities of Subcontractors and not just the supplier. Subcontractors' roles will determine the applicability of GDPR and other laws and regulations to those activities, particularly with respect to whether they are Processors or Controllers. These must be explicitly handled in the relevant contract provisions.

Applying the Principles to Contract Terms

1. Back-to-Back Contracting

Aligning liability and performance

1.1. It may not be practical for a Subcontractor to be liable to the supplier to the same degree that the supplier would be liable to the customer if a Subcontractor fails in its obligations (such as a failure to meet SLA performance targets, and the credits to the customer are more than the credits the supplier gets from the Subcontractor). Typically, the supplier is receiving more revenue from the customer than the Subcontractor is receiving for its part of the deal, so the at-risk amounts could be different, and therefore the supplier and Subcontractor may want to take this into account when allocating liabilities. However, there may be situations where the Subcontractor's role is so critical to the overall success of the transaction that the supplier and Subcontractor agree for the latter to indemnify the former for a failure to deliver that essential element.

Aligning timeframes

1.2. When setting timeframes for certain actions that will require involvement of Subcontractors (e.g., notice of cancellations, change orders, relaying of key

information among the parties), it is prudent for the supplier to take into account internal turnaround times and the time needed to communicate with a Subcontractor when committing to contractual deadlines (*e.g., within x days, supplier shall…*)

Aligning compliance

1.3. If the supplier-Subcontractor contract is under a different governing law than the customer-supplier contract or if the Subcontractor is subject to rules or regulations that are inconsistent with the obligations under the customer-supplier contract, those aspects of the relationships must be recognized and built into the relevant contracts so as not to cause incompatibilities down the road.

2. Categorizing Subcontractors

Categorizing Subcontractors

2.1. In order to balance a customer's desire to pre-approve Subcontractors with suppliers' need for flexibility in selecting Subcontractors without the added time to get those pre-approvals, it may be prudent to divide Subcontractors into categories: those in sensitive/strategic roles where pre-approvals are critical for customers, and those that do not pose any concerns to customers. In this way, additional levels of scrutiny and governance can apply only to the first subset.

Flow-downs dependent on Subcontractor type

2.2. The categorization of Subcontractors may also be useful in determining which flow-downs should apply to each subset. Subcontractors who provide commodity items or who never access customers' sensitive information may not need to be subject to many of the security, background checks, and audit requirements that apply to the supplier itself. Nonetheless, a Subcontractor's adherence to regulations or customer policies that are directly related to its activities should still be required.

Pre-approvals of Subcontractor assignments

2.3. The differentiation of Subcontractors may also be relevant if and when a Subcontractor wants to assign its obligations to a third-party. The supplier-Subcontractor contract typically deals with that situation in the Assignment clause, but the extent to which a customer would want to pre-approve such an event should be a function of that Subcontractor's role and whether it is characterized as a sensitive/strategic Subcontractor.

3. Changes to Subcontractors

Grounds to request removal of a Subcontractor

3.1. The right of customers to demand the removal or replacement of a Subcontractor or a Subcontractor employee or representative should be limited to lawful and reasonable grounds. If the reason for the demand is not due to the wrongdoing of the supplier or could not have been reasonably foreseen by the supplier, the parties should agree, in good faith, on a reasonable transition to a new Subcontractor (including any applicable pre-approval by customer, training, hiring of personnel, etc.) without penalty to the supplier during this period if there is a reasonable disruption to performance. In addition, if the new Subcontractor represents a change in costs to the supplier, the parties should agree to an equitable impact on prices (perhaps through a change control process).

Supplier responsibilities in changing Subcontractors

3.2. If the supplier wants to change Subcontractors, mandated pre-approvals, if any, should be processed, and the supplier should be responsible for ensuring that the handover does not materially impact its obligations under the customer contract. Any required return or destruction of customer confidential information held by the old Subcontractor must be enforced by the supplier.

Step-in rights

3.3. If a customer has "Step-In rights," (i.e., the customer can take over a supplier's function such as maintenance if the supplier – or its Subcontractor – fails to perform) both the customer-supplier and the suppler-Subcontractor contracts should deal with the potential situation when the trigger event is caused by the Subcontractor (see WorldCC Contracting Principle *Step-In Rights*). To what extent are the supplier's financials affected? How do all the parties collaborate on the transition? What is the Subcontractor's liability for the reduction in revenue that the supplier experiences?

4. Solicitation of Employment of Subcontractor Personnel

Non-solicitation must be explicitly agreed

4.1. A customer's right to solicit supplier employees for employment either during or after the contract term should not be assumed to apply to Subcontractor employees. That must be dealt with explicitly in the contract and must be consistent with the terms of the supplier-Subcontractor contract (see WorldCC Contracting Principle *Non-Solicitation*).

Permitted solicitation to maintain customer business continuity

4.2. Particularly in outsourcing situations, a customer may need certain personnel to move into the supplier's organization at the beginning of the relationship and/or move into the customer's or successor supplier's organization at its end to maintain business continuity for the customer. Subcontractors or their employees may be involved in those movements of people, and local laws such as TUPE in the UK, may be relevant. These all must be set forth explicitly in both the customer-supplier contract and in the supplier-Subcontractor contract.

5. Data Privacy and Protection

Flow-downs and flow-ups related to data privacy and data breaches

5.1. Given the high focus on data privacy and the flow of personal data across jurisdictional borders, it is important for customers and suppliers to have a common understanding of where personal data flows and what each party does with the other party's personal data. This analysis must encompass the roles of Subcontractors.

Customer audits related to data protection compliance

5.2. See the WorldCC Contracting Principles *Data Security and Privacy* and *Customer Audit of Suppliers* for additional guidance in the event that personal data is relevant to Subcontractor activities (which, in most cases will be applicable even if just the handling of customer contact information) and the customer wants the right to audit Subcontractor handling of that data.

Defined Terms

Subcontractor: a third-party, working under the direction and control of a supplier, who provides a product or service that makes up part of the solution or scope of work being provided to a customer.

In these Principles, Subcontractors do not include entities that a customer contracts with directly even though that entity's offerings may form part of the overall solution (e.g., the customer is contracting directly with Company A, a software supplier, for an application to be used with equipment provided by an OEM – Company A is not a Subcontractor of the OEM). Nor does the definition include suppliers or service providers who provide goods and services to suppliers for internal consumption and are not under contract for any specific customer (e.g., an OEM purchases hard drives from Company A for inclusion in computers it is selling to the customer – Company A is not deemed a Subcontractor in the *Subcontracting* Principle).

Supplier Audit of Customers

See also the "Customer Audit of Suppliers" Principle

The Principles

1. Supplier audits of customers are appropriate when the supplier grants specific rights to customers under certain terms and conditions (which may include restrictions), and the supplier cannot independently verify that the customer is complying with those terms.

2. Audit rights should be restricted to assessing the customer's compliance with its contractual obligations and restrictions. The audit's scope and frequency should be reasonable and proportioned to the risks to the supplier if the contract terms are breached.

3. Audits should be conducted by the supplier or a third-party auditor appointed by the supplier and reasonably acceptable to the customer, at the expense of the supplier. If the audit shows a material non-compliance by the customer, the supplier may seek reimbursement of reasonable audit expenses from the customer.

4. Audits should not interfere with a customer's rights (e.g., to privacy, confidentiality), contractual commitments with respect to its other relationships, or its day-to-day operations. Audits must comply with applicable laws, regulations, any applicable terms of the agreement, and generally accepted auditing practices to ensure fairness and impartiality.

5. The customer should have the right to review any preliminary audit report and request reasonable changes if it contains material inaccuracies. The customer should also be given an opportunity to correct any issues found during the audit within the same timeframe allowed for curing contract breaches.

Applying the Principles to Contract Terms

Reasonable scope and frequency

1. Audits should focus only on information necessary to verify compliance with the obligations and restrictions under the contract that are expressly subject to audit. Audits should be limited to one per year, unless:
   - **a)** more frequent audits are required by law or regulation;

     or
   - **b)** previous audits found material deficiencies needing confirmation of corrective actions.

Remote vs.. on-site audits	**2.**	Audits should be conducted remotely whenever the necessary information can be reviewed electronically. If on-site audits are necessary, they should be carried out with minimum disruption to the customer's premises, in the presence of a customer representative, and in accordance with the customer's reasonable visitor policies (e.g., health and safety rules, access control, confidentiality).
Time-bound audit rights	**3.**	Audit rights should apply during the term and any other periods during which the customer is contractually bound to remain compliant with the terms of the contract (e.g., post-contract retention of supplier confidential information), but they should not apply beyond the period for which a breach claim or remedy is permitted under the contract or as defined under the applicable laws or regulations of the contract (i.e., statute of limitations).
Notice of audits	**4.**	The supplier should provide reasonable notice before conducting the audit to allow the customer to gather the necessary data without interfering with ongoing operations. Notice must be in writing and include details as to the audit's purpose, scope of information sought, and proposed timing.
Audit methodology	**5.**	The audit's details, such as time, place, scope, and methodology, should be agreed by the parties, but they must allow the supplier to meet its reasonable audit goals.
Confidentiality and data protection	**6.**	The auditing party, and any appointed third-party auditor, should maintain strict confidentiality and data protection measures throughout the audit and for as long as the audited party's information is being held. Any information gathered, including sensitive business data and proprietary information, should be treated with the utmost confidentiality and used solely for the audit. The customer should have the right to withhold any trade secrets or other highly sensitive information.
Audits of invoiced amounts	**7.**	If the audit finds invoice inaccuracies (such as when charges or fees are calculated for each invoice based on a defined volume or usage), necessary adjustments or payments must be made promptly.
Cost of audits	**8.**	The supplier should cover all audit costs (e.g., auditor fees, travel expenses, administrative costs), unless the audit shows a material non-compliance by the customer.

Suspension Rights

The Principles

1. Suspension should only be considered if it is necessary under the circumstances or is a preferred alternative to contract termination. 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. Similarly, suppliers should have an expectation that its customers will live up to their promises to pay for everything ordered and to meet all other contractual obligations. Although Suspension is typically undertaken by a supplier, this Principle reflects the possibility that either party to a contract has a right to exercise a Suspension.

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

3. 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 Suspension may cause material harm to the other party.

4. Causes for Suspensions should be expressly set forth in the contract and should not be left to the unlimited discretion of either party.

5. A Suspension should not come as a surprise to the other party, except in emergency situations where there is an imminent threat of harm to the suspending party.

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

7. 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.

8. Any notice of a Suspension should be pursuant to the notice provision of the contract but should also be to the other party's operations contacts so as to speed that party's responses.

9. 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.

Applying the Principles to Contract Terms

1. Grounds for Suspension

Examples of grounds for Suspension by suppliers

1.1. The following are examples of situations in which a supplier should have a right to temporarily suspend:

- **a)** 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, its customers, or third-parties.
- **b)** Customer's use of service or goods that is a violation of Applicable Laws (see WorldCC Contracting Principle *Compliance with Laws*).
- **c)** 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).
- **d)** The Suspension is ordered by a governmental or regulatory body.
- **e)** For non-payment of applicable non-disputed charges or fees, after reasonable attempts at collection have failed.
- **f)** For potential harm to property (including supplier assets) or persons that cannot be avoided otherwise

Examples of grounds for Suspension by customers

1.2. The following are examples of situations in which a customer should have a right to temporarily suspend:

- **a)** Products are being delivered in non-conforming condition, and efforts are underway by the supplier to fix the issue(s).
- **b)** The customer cannot update newly released software updates until it makes its own systems compatible with the changes.
- **c)** The customer does not accept certain supplier personnel onto its premises to perform agreed work until security or other background checks are completed.

Grounds for Suspension should be listed in the contract

1.3. All potential grounds for a Suspension should be expressly set forth in the contract.

Scope of Suspension

1.4. 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 or event should not be subject to Suspension.

2. Notice of Suspension

Prior notice of Suspension

2.1. 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 or regulation, the supplier should give a customer a prior notice so that they have reasonable opportunity to cure or mitigate the basis for the Suspension prior to the actual Suspension.

When notification of Suspension is not possible

2.2. 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

Payment during Suspension

3.1. 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. However, if the period of suspension is significant, the supplier should have the right to adjust prices if it had that right in the absence of the suspension (see WorldCC Contracting Principle *Managing Price Volatility*).

Mitigation of causes

3.2. 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.

Suspension ordered by a regulator

3.3. 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.

Defined Terms

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

Suspension: a temporary cessation of performance by the customer or 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.)

Term and Termination

The Principles

1. Customers and suppliers alike benefit from a clearly defined Term (including start date and end date) in both individual transactions (orders or Statements of Work (SOWs)) and broader relationships (under an MSA). This helps each party plan operationally and financially, ensuring stable supply chains for customers and predictable revenues streams and production requirements for suppliers.

2. MSAs should clearly differentiate between the Term of the MSA itself and the Term for any orders or SOWs under it. The MSA must be in full force and effect for as long as orders and SOWs remain active under it. Overly long Terms of an MSA should not necessarily worry the parties as an MSA with no active orders or SOWs normally poses minimal risks. There are more risks associated with excessively long Terms for orders or SOWs.

3. The length of the Term should be a balance between:

    a) the parties' desire to continue the business relationship for as long as it is mutually beneficial;

    and

    b) each party's desire for a clearly defined exit path should it want to end the relationship.

    Suppliers generally want longer Terms to lock in customers and minimize windows for them to seek competitive alternatives, while customers generally want more frequent exit opportunities. However, a balance between the two should be achieved through:

    a) pricing structures (e.g., greater discounts for longer Terms),

    b) an initial Term long enough to enable suppliers to recover any start-up costs followed by shorter renewal Terms;

    and

    c) possibly allowing for terminations for convenience with reasonable termination charges.

    Depending on the nature of the transaction and the respective investments and commitments made by the parties, termination rights of the parties do not necessarily have to be the same.

4. Term renewals should not come as a surprise to customers. They should not find themselves locked into a new Term without having had an opportunity to make a conscious decision to extend the relationship, particularly if automatic price increases or unilateral changes to terms and conditions apply.

5. A party's right to Terminate for Cause should be based on clear reasons and processes. The breaching party should be given:

a) written notice of the alleged breach and non-breaching party's intent to terminate;

and

b) a reasonable opportunity to cure the breach (if possible) before the effective termination date.

6. A party's right to Terminate for Convenience during a Term (particularly during an initial Term) should be considered an exception rather than the rule. If such right is agreed, either at order/SOW or MSA level, the terminating party should compensate the other party to put it in a comparable economic position it would have been in had the relationship or transaction lasted through the current Term.

Applying the Principles to Contract Terms

1. Terminations at Times of Term Renewals

Sufficiently long notice period

1.1. The notice period for termination should be sufficiently long to enable the other party to seek an alternative supplier or shift resources to other customers, as the case may be. Notice periods of 30 or 60 days are frequently used. However, those may not be sufficient if the goods or services being provided are complex or unique it is particularly difficult to transition to a new relationship, or because of industry-specific norms. It may be reasonable for customers to benefit from a longer notice period of a supplier's termination than vice versa, given the longer lead time needed for the customer to select and contract with a substitute supplier.

Notices for auto-renewals

1.2. Suppliers should provide advance notice of upcoming auto-renewals, particularly if the customer does not have the means of tracking renewal dates on its own.

Sufficient time to negotiate changes or terminate before renewals

1.3. If the supplier plans to change prices or if either party wants to change terms and conditions or other material elements of the relationship at the time of renewal, they must give written notice of those changes well before the non-renewal deadline. This allows the other party enough time to review and negotiate the changes and/or decide whether to terminate before the termination notice deadline.

2. Termination of MSAs vs. Orders or SOWs

Order vs. MSA breaches and appropriate termination rights

2.1. Relationships should continue for as long as they provide benefits to both parties, and therefore contracts should be drafted to limit the repercussions of breaches to the extent reasonably possible. Accordingly, if an uncured breach affects an individual order/SOW under an MSA rather than with respect to the entire MSA, only that applicable order/SOW should be subject to termination. A Termination for Cause of an MSA should also terminate all existing orders or SOWs directly

affected by the breach that gave rise to the termination. However, if an MSA breach affects all transactions under the MSA or is so severe and damaging that the non-breaching party wants to end the relationship completely (e.g., non-compliance with anti-corruption and bribery laws, breach of confidentiality, bankruptcy, sanctions violations), then termination of the MSA and all work under it may be appropriate.

MSA termination for convenience should not affect SOWs

2.2. Termination for Convenience of an MSA should not automatically end ongoing orders or SOWs; these should remain in effect until their completion. However, in some regulated settings (like government procurement), all existing orders or SOWs might need to be terminated as well. No new orders or SOWs should be executed after the date of termination notice.

3. Quid Pro Quo for Termination for Convenience

Supplier compensation

3.1. If a party (typically the customer) wants the right to Terminate for Convenience, it should agree to provide appropriate compensation to the supplier for ending the relationship early. This compensation should ensure that the supplier is made financially whole and may be either a fixed termination charge or based on a formula (e.g., time remaining in the Term).

Payment of all charges

3.2. Fairness and equity may require a customer Terminating for Convenience to pay for all charges for the rest of the current Term if the supplier has already booked those revenues and will incur a significant loss if that income were to be reversed. Alternatively, the termination charge may be based on supplier's non-recoverable costs, such as investments made in inventory or other resources that cannot be used for other customers, non-refundable payments to subcontractors, and/or demobilization costs. If the supplier saves variable or fungible expenses due to early termination, the customer should get some relief from its liability.

No supplier rights to mid-term Termination for Convenience

3.3. Suppliers typically should not have a right to Terminate for Convenience mid-Term, except under exceptional circumstances (e.g., governmental action outside of its control). The supplier should wait until the next Term renewal to terminate. If a supplier is given a right to Terminate for Convenience mid-term, it should be responsible for compensating the customer to mitigate the impact. This may include refunding prepaid amounts, covering transition costs, or off-setting higher replacement costs for the remainder of the Term.

Avoiding penalty language

3.4. Payments due to a supplier for Termination for Convenience should not be characterized as cancellation penalties in the contract, as penalties are not enforceable in certain jurisdictions.

Government contracts

3.5. Termination for Convenience rights are more common for customers who are government entities, as the right may be imposed by governing statutes or regulations. The supplier should still be entitled to reasonable, specified termination charges.

4. Cure Periods Prior to Termination for Cause

Appropriate periods for curing breach

4.1. In establishing the length of the cure period for alleged breaches, the parties should take into account the potential breaches by each party and the mitigatable and non-mitigatable impacts on the non-breaching party as it waits for the breach to be cured. The parties should also allow for agreed extensions of the period if the breaching party will need more time to remedy the problem, particularly where both parties do not want the incident to scuttle what was otherwise a mutually beneficial relationship and the impacts of the breach on the non-breaching party are manageable.

Mitigation of damages

4.2. During the cure period, as is required under the law in many jurisdictions, both parties should be obligated to mitigate damages that might flow from the breach.

5. Termination due to a Force Majeure Event

Reasonable period to exercise termination rights

5.1. A force majeure event allows the affected party to avoid liability for failing to meet its obligations during that period (see the *Force Majeure Contracting Principle*). More often, it is the supplier who encounters a force majeure event in the delivery of products or services.

The customer should not have to wait too long for the supplier to resume performance, especially if the product or service it provides is mission-critical to the customer. The wait time before the customer can exercise its right to terminate should be fair to both parties, given that there is no fault involved.

The factors to consider when deciding on the period should include, for example, the criticality of the products or services to the customer, the ability of the customer to mitigate the impacts of the delays, the time it would take for the customer to contract with an alternative supplier, and the ability of the supplier to rely on disaster recovery and business continuity plans to recover from the event.

Remedies for force majeure events

5.2. Neither party should face any claim for damages due to the force majeure event or resulting termination. However, if the supplier's negligence or failure to implement required mitigation plans caused or aggravated the impacts of the event, that should be treated as a basis for a damages claim. In all cases where the supplier experienced the force majeure event, the customer should be entitled to a refund of any prepaid amounts for services or products not provided due to the event and/or any resulting termination.

6. Payment of Charges upon Termination for Cause

If customer terminates for cause

6.1. If a customer Terminates for Cause, it should still be responsible to pay for goods or services properly delivered up to the effective date of the termination. It should not be able to withhold those payments as a set-off for possible recovery of damages due to the breach. Those damages should be sought separately.

If supplier terminates for cause

6.2. If a supplier Terminates for Cause, it should have the right to collect all charges and payments it would have received had the customer Terminated for Convenience, plus any other damages for breach to which It would be entitled.

However, the supplier should not receive more than what it is rightfully owed (i.e., all amounts it receives should not exceed:

a) the total charges it would have invoiced had no breach occurred;

plus

b) the incremental direct damages caused by the breach).

Defined Terms

MSA, or Master Services Agreement: any umbrella or framework agreement under which various orders or Statements of Work (SOWs) may be executed by the parties, all of which will be subject to the terms and conditions of the MSA.

Term: the specified period during which the overarching agreement (e.g., MSA), order or Statement of Work, as the case may be, will be in full force and effect. Note that some rights and obligations (e.g., confidentiality, return of data) may survive the end of a Term if so enumerated in the applicable terms and conditions.

Termination for Cause: the right of a party to terminate a contract, order or Statement of Work, as the case may be, due to specified events, including but not limited to an uncured breach of the contract by the other party, the other party entering into bankruptcy, a force majeure event affecting the other party that lasts beyond a prescribed duration.

Termination for Convenience: the right of one party to terminate a contract, order, or Sow, as the case may be, for any reason or for no reason at all. For the purposes of this Principle, Termination of Convenience does not refer to the exercise of a right not to renew a contract, order or SOW at the end of its current Term.

Termination Assistance

The Principles

1. Termination rights and obligations, including high-level principles for Termination Assistance, should be addressed in the contract so that the 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.

2. 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.

3. The goal of Termination Assistance is to secure customer business continuity by making any 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.

4. 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).

5. The contract (or Exit Plan) must clearly specify if there are any assets (e.g., intellectual property, confidential information, personal 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.

6. 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 be 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.

Applying the Principles to Contract Terms

1. Services to be Provided During Termination Assistance

Same scope of services	**1.1.**	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.
Customization of Termination Assistance	**1.2.**	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.
Application of SLAs	**1.3.**	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

Supplier's right to require additional terms	**2.1.**	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.
Force Majeure	**2.2.**	Force majeure provisions should be applicable to Termination Assistance obligations.
Fair commercial terms	**2.3.**	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.
Unexpected contingencies	**2.4.**	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

New supplier's confidentiality obligation

3.1. 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.

Transfer of data and work product

3.2. Customer 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. It is particularly important to ensure that personal data belonging to the customer be returned or destroyed to avoid any potential data breach and to comply with applicable laws and regulations.

Transfer of personnel

3.3. 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. In the United Kingdom, TUPE rules may apply here, and any analogous laws and regulations may apply in other countries.

Transfer of equipment, software, licenses and IP

3.4. 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's 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.

Assignment of third-party contracts

3.5. 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 referral assistance to customer in its efforts to engage those third parties directly.

Knowledge transfer and training

3.6. 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 Exit Plan should set out any specific training applicable to each stage of the Termination Assistance.

Winding down of services

3.7. For services that are volume priced or have charges that are dependent on fixed and variable costs, care must be taken to anticipate a wind-down of the services over time and to build a charging model that is fair to both parties as the transition comes to an end. Relatively small volumes should not skew BAU models to a point where they become unreasonable for either party.

Defined Terms

Exit Plan: the written disengagement or Termination Assistance plan agreed upon by the parties.

Termination Assistance: 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 to minimize any disruption to the customer's business activities that relied on that service.

Warranties

The Principles

1. The contract should specify any Express Warranties for the applicable products, software, or services that are reasonable in light of the characteristics of the products, software, or services and that form the basis for the transaction.

2. Express Warranties should not be in the form of a promise that the product or service will be free of all defects (which does not reflect reality) but rather should focus on the specific remedies to be provided by the supplier in case of defects or non-conformity with the specifications that are provided.

3. Express Warranties should define a reasonable time frame for the customer to notify the supplier of a defect or non-conformity.

4. The Express Warranty period should be calculated either from the delivery to the customer of the product, software, or services (according to the agreed delivery terms); from the acceptance of the product, software, or services as agreed in the contract; or from first usage of a product or software.

5. The duration of the Warranty period will generally be shorter for software than for tangible products (equipment or hardware), as software versions have a shorter lifetime, and software suppliers typically request their customers to implement the newest software versions The parties need to specify when the customer must begin to pay for maintenance and support plans, if purchased. The timing will depend, in part, on whether the supplier requires a maintenance/support plan to be effect before it provides software updates and new releases.

6. The parties should agree on whether the supplier is entitled to full payment for products, software, or services found to be defective or nonconforming upon delivery or installation, as the case may be. Regardless of whether full payment is made, the supplier has an obligation to correct any deficiencies on a timely basis. If they cannot be corrected, the customer would be entitled to a refund of any applicable payments made

Applying the Principles to Contract Terms

1. Express Warranty

Avoiding unintended Express Warranties

1.1. Care should be taken to avoid unintended Express Warranties. The word “warrant” does not need to be used to create an Express Warranty. Instead, any statement in a contract that is a future promise about the products, software or, services that is understood to create the basis of the contract may be considered to be an Express Warranty.

Types of Express Warranties

1.2. Express Warranties should be clearly stated in the contract:

a) **Product Warranty**: Express Warranties for products and product deliverables should address all agreed requirements related to the products or product deliverables, such as quality, condition, functionality, quantity, or performance. To ensure the Express Warranty is clear and aligned with product or deliverable requirements, it is a best practice to warrant that the products or product deliverables will perform in accordance with the agreed specifications in the contract. When enhancements of already delivered software functionalities are provided, the supplier does not generally provide any warranty regarding such enhancements, and support services regarding such enhancements should be specified in a separate services contract.

b) **Service Warranty:** Express Warranties for services will be promises generally aligned with the manner in which the services will be performed. As an illustration, the parties may agree to reference industry standards or other terms that have been interpreted by case law, such as that the services are to be performed in a professional, and workmanlike manner.

c) **Other Warranties:** Depending on the contract subject matter, parties may seek warranties that are relevant to the products, software, or services to be delivered, such as: non-infringement of third-party rights; promises to obtain licenses; and authority to enter into the contract or to operate in the manner or in jurisdictions anticipated by the other party.

Express Warranty conditions

1.3. Parties may wish to agree that certain conditions must be met for an Express Warranty to apply, such as:

a) The product, software, or service deliverable must be used and maintained under normal conditions and in accordance with the documents, information, and advice furnished by the supplier;

b) The customer must give supplier written notice of defects, non-conformities, or deviations from the agreed specifications before the expiration of the applicable Warranty period;

c) Any defect, non-conformity, or deviation is not caused by products or software provided by third parties outside of the contract;

d) The customer has given supplier the opportunity to inspect and remedy the defect, non-conformity, or deviation;

e) The customer has implemented, within a reasonable time period, the software updates provided from time to time by supplier during the Warranty period;

or

f) The failure was not caused by the customer's unauthorized modification of the product, software, or service deliverable.

2. Notice and Warranty Period

Clear process to provide notice

2.1. A Warranty provision should address any specific process requirements for providing notice of a breach or non-conforming delivery and for claiming remedies.

Reasonable Warranty period

2.2. The Warranty period during which the customer may give notice of any breach or non-conforming delivery should be aligned with a reasonable time period, in light of

the type and characteristics (technical, functional, visual, etc.) of product, software, or service deliverable. Generally, the Warranty Period should be at least as long as the industry standard.

3. Disclaimers of Warranty

Content of disclaimers

3.1. Disclaimer of Warranties should specify that the parties are only relying on the Express Warranties and are not relying on any other representations (oral or written), course of dealing, or course of performance.

Specific and conspicuous disclaimers

3.2. Warranty disclaimers should be clear and specific. In some common law jurisdictions, it is a best practice for disclaimers of Warranties to be in all capitals and to explicitly disclaim all Implied Warranties, including, specifically, the Implied Warranty of Merchantability and fitness for a particular purpose.

4. Remedies

Repair or replacement

4.1. A common remedy for breach of a Warranty or for a non-conforming delivery is repair or replacement of the defective products, software, or services deliverables. If the parties agree that the appropriate remedy is to repair, the terms of the agreement should set forth parameters for the reasonable amount of time it takes to repair or the number of times the supplier may attempt to correct the defective or nonconforming product, software, or services deliverables before the customer can avail itself of another remedy, such as termination of the sales contract, recovery of costs of having others make the correction, or refund. If appropriate, the parties may also wish to specify what warranty and remedies come with repaired and replacement items.

Warranty service commitments

4.2. Should the customer want to obtain commitments on specific response times or performance levels in order to supplement supplier's Warranty undertakings, such commitments should be specified in a separate service level agreement (see WorldCC Contracting Principle *Service Level Agreement Remedies*). The supplier should take care, however, to ensure that a failure to meet a certain agreed standard does not give rise to the customer having two remedies – one for the failure to satisfy the service level agreement and another for breach of an Express Warranty.

Remedies for breach of Warranty

4.3. It may be appropriate to limit the remedies and liabilities for breach of Warranty or non-conforming delivery, given the nature of the products, software, or services (where applicable). Unless otherwise limited by contract, potential recourse for breach of contract may include a number of remedies, such as specific performance and restitution and not just compensation for damages. Inappropriate remedies can be avoided by specifying the types of damages that can be claimed and expressly excluding all other recourse.

Sole and exclusive remedies

4.4. It is common for the parties to agree that specified recourse(s) will be the sole and exclusive remedies for breach of Warranties or non-conformity with delivery obligations.

Choice of remedy

4.5. Typically, the supplier has the right to choose the Warranty remedy to be applied in any given situation, but the customer may want to dictate what remedies apply in specific scenarios that affect mission-critical operations.

Who bears Warranty costs

4.6. While it is customary for suppliers to bear the cost of Warranty repair or replacement, certain ancillary costs, such as transportation costs, and risk of loss during shipment may be subject to negotiation and should be expressly stated in the contract to avoid any surprises or misunderstandings. .

5. Liability Clauses

Limitation of liability for breach of Warranty

5.1. Liability clauses should be aligned with the Warranties and may include limitations of liability related to breach of Warranty or non-conforming delivery obligation, as set out in the WorldCC Contracting Principle *Liability Caps and Exclusions from Liability*.

Defined Terms

Warranty: under these Contracting Principles encompasses both common law and civil law definitions[1].

a) In common law, a warranty is a promise, typically made by the supplier, about the character or quality of a tangible product (equipment or hardware), software, or a service.

b) In civil law, the statutory warranty is not a promise but an obligation for the supplier to deliver products, whether tangible (equipment or hardware) or intangible (software) free of defects. Defects can be either:

1) material defects, which are visible (patent) or hidden (latent), or
2) legal defects as to the right to use the products or software.

With regard to services, a statutory warranty can only cover results of services or deliverables resulting from those services.

[1] While the legal definitions may differ between common law and civil law systems, there is a great degree of freedom in drafting individual contracts between parties so that claims for defects can be expanded or restricted to meet the needs of both parties or, in some cases, precluded. Accordingly, these Contracting Principles apply in both common law and civil law jurisdictions.

Cont. →

Defined Terms (continued)

Express Warranty: a Warranty explicitly set forth in the contract.

Implied Warranty: a Warranty established by law and does not need to be expressly set forth in the contract terms. Applicable Implied Warranties will depend on a number of factors, including: the type of product, software, or services; negotiated prices; applicable laws; and understandings between the parties about how the products or software may be used. The Implied Warranties that usually apply to sales of products may include the following, unless otherwise expressly excluded in the contract:

a) **"Implied Warranty of Merchantability"** generally applies to the sale of most products and allows the customer to rely on the products being of average quality and fit for ordinary purposes.

b) **"Implied Warranty of Fitness for a Particular Purpose"** will apply if the supplier knows the intended use for the product and allows the customer to rely on the supplier having knowledge that the products are to be appropriate for that use.

c) **"Implied Warranty of Title and Against Infringement"** allows the customer to rely on the supplier having all rights necessary to sell the products without liens or encumbrances (or with only those liens and encumbrances that were declared by the supplier at the time of the sale) and without claims that the products infringe any third-party rights.