CLOUD COMPUTING AND CLOUD MARKETPLACE TOOLKIT PROJECT

Key Concepts in Standard Form Enterprise Cloud Agreements: Tips and Tools for Negotiation and Implementation

ABA Cloud & Enterprise Technology Subcommittee

Prepared by Carolyne R. Dilgard-Clark, Esq.

with assistance from the Subcommittee

August 2023

IMPORTANT NOTE: This presentation quotes language from selected Amazon Web Services (AWS®), Google Cloud®, and Microsoft Azure® agreements as examples.* The presentation aims neither to promote nor criticize those cloud service providers or any of their respective products. To avoid vendor bias, the Subcommittee refers in related work product to services and legal terms offered by various cloud service providers.

* *AWS Customer Agreement*, AWS (updated Apr. 20, 2023), https://aws.amazon.com/agreement; *Google Cloud Platform Terms of Service*, GOOGLE CLOUD (updated July 12, 2023), https://cloud.google.com/terms; *Microsoft Customer Agreement*, MICROSOFT (updated Mar. 1, 2023), https://www.microsoft.com/licensing/docs/customeragreement.

If there is a topic covered or mentioned in this toolkit that you would like to expand on, we welcome your feedback and invite you to participate in building out these resources.

To contact the Toolkit Project coordinators, please email the project's virtual mailbox at cloud-toolkit-project@googlegroups.com

Introduction

Role: In this exercise, we imagine the common situation where an organization—referred to as the *enterprise* or the *enterprise customer*—is looking for a cloud-based technology solution. The business lawyer representing the enterprise is given the cloud provider's or vendor's standard-form "enterprise agreement." We will be focusing on what role our business lawyer can play with respect to the negotiation and implementation of the enterprise agreement, as well as with respect to being a contributor adding value to the larger process.



Timing and Process: Our lawyer may have been brought in during the business team's planning phase as the team identified areas of development and evaluated and selected vendors and the desired products/services. In preparing this exercise, we recognize the practical reality that the lawyer often is brought in by the (internal or external) client to review a contract following the determination of material business decisions and well after negotiations are underway. This exercise is designed with the goal of helping the legal team efficiently identify issues and educate business partners on hybrid issues before commitments to vendors are made.

Introduction

Role: Even when the business lawyer is fully briefed and involved in the early stages of a process, cloud service contracts with major vendors can be one-sided.

- Contracts for enterprise cloud-based services are typically on vendor forms and not subject to material negotiation and modification.
- The major vendors of cloud services have significant leverage.

So, what role can our business lawyer play, knowing that the leverage is not in the enterprise's favor?

Timing and Process: The types of contracts highlighted in this exercise may be for services that carry sensitive and confidential information and/or those that underpin and support critical business operations. Additionally, these contracts may represent a significant portion of an enterprise's budget and cross over multiple business lines. Yet, the process does not typically allow for the enterprise to fully conduct due diligence on the product and/or negotiate for more favorable terms.

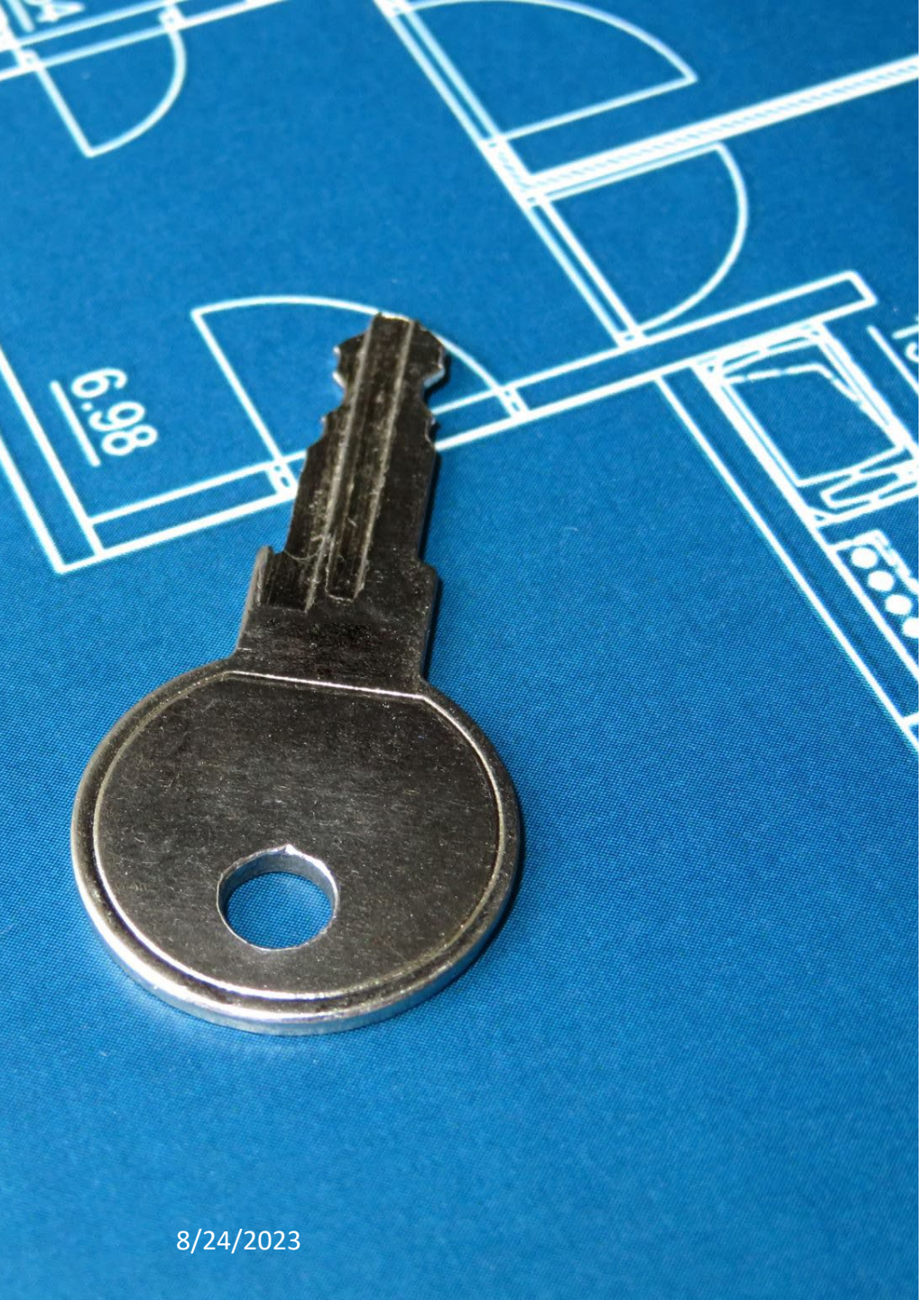


Introduction



Role: This exercise focuses on the role that the business lawyer may play. Key to many potential action items and areas of opportunity is our business lawyer knowing the business, the goals, the expectations, the realities, etc.

Timing and Process: Adding to the complexity of the situation is the reality that an enterprise may have various stakeholders with different and evolving views about client needs and goals, proposed uses and limits of the services, and contingency plans. Reconciling those differences will happen in real time as the agreement with the legal review takes shape. The result can be internal and external negotiations happening simultaneously.



Key Drafting Concepts

The goal is to draft a contract that is essential, wide-reaching, and financially material, yet such contracts can often be difficult to negotiate.

To maximize the business lawyer's impact, we will focus on **five drafting concepts** typically seen in these types of agreements:

1. Scope and Subject Matter
2. Industry-Specific Terms
3. Entire Agreement: What Is the Agreement?
4. Allocation of Risk
5. Endgame: Term and Termination

Pro Tips:

- Take a holistic approach to negotiation and implementation.
- In this type of contract negotiation and implementation (perhaps more than in others), our business lawyer will need to focus on the business counseling aspect of serving as the business lawyer.
- Material changes to vendor contracts may require great negotiation capital and/or additional spend. Material changes may also be entirely out of reach.
- Our business lawyer can educate the enterprise by spotting issues so that (1) negotiation capital and priority can be allocated to the truly KEY issues and (2) the legal team and key stakeholders can collaboratively map out ways to mitigate risk outside of the contract terms.



PRO TIPS:

Our business lawyer will need to have a solid understanding of the business objectives and the enterprise's current and proposed technology landscape.

Our business lawyer will need to match enterprise goals to the vendor's services (as reflected in the contract, not marketing materials).

Our business lawyer may help key stakeholders understand the business and legal needs, as well as the enterprise's contractual limitations and responsibilities.

Important questions to ask include the following:

- ✓ What do the business teams think they are getting?
- ✓ What does the contract say they are getting?
- ✓ How can any gaps be addressed?

To get the right information communicated across the enterprise, the legal team can participate in interdisciplinary discussions involving the following:

- ✓ IT
- ✓ Procurement
- ✓ Finance
- ✓ Risk Management
- ✓ Users

1. Scope and Subject Matter

Scope of Services and Subject Matter

The first key provisions that our business lawyer will focus on deal with the scope of services provided. To frame the issue, our business lawyer may ask the following questions:

- What is the problem or need that the business team is aiming to address?
- What does the enterprise expect to receive under this contract?
- What is the vendor willing to provide? What does the contract exclude? Does the vendor's contract language match the sales pitch?
- Does this contract solve for the right goal or problem? Are there necessary add-ons or adjustments needed? Can the business create or source appropriate work-arounds?

Pro Tips:

- ❑ Look for what is INCLUDED and what is EXCLUDED in the definition of *services/products/offerings*.
- ❑ Start by looking at the defined terms, and then move on to the affirmative and restrictive covenants affecting use and users.
- ❑ Third-party add-ons and supplemental offerings may be offered under yet additional ancillary terms, which may or may not be provided directly by the vendor. The business team may also need to design its own supplements or work-arounds to meet its full needs.



PRO TIPS:

KEY CONCEPTS & QUESTIONS



What is specifically included? Is it listed? Or is it generically described as vendor's cloud-based or other services/products?

Is there a reference to an exhibit or ancillary document? To a link that may be updated by the vendor (at the vendor's discretion, with or without notice)?

What is excluded (e.g., third-party add-ons and offerings)?

Are ancillary offerings from the vendor, such as technical services, training, and/or professional services, included under this agreement or a separate contract?

Scope of Services – Sample Definitions

Sample Language:

"**Product**" means all Software and Online Services that [Vendor] offers under this Agreement as identified in the Product Terms, including previews, prerelease versions, updates, patches, and Fixes from [Vendor]. Product availability may vary by region. "Product" does not include [Vendor] Products.
"**Non-[Vendor] Product**" means any third party-branded software, data, service, website, or product, unless incorporated by Vendor in a Product.

"Service" means each of the services made available by us or our affiliates, including those web services described in the Service Terms. Services do not include Third-Party Content.

Services Use. During the Term, [Vendor] will provide the Services in accordance with the Agreement, including the SLAs, and Customer may use the Services, and integrate the Services into any Customer Application that has material value independent of the Services, in accordance with the Agreement.

. . .

"Services" means the then-current services described at [link to other terms], excluding any Third-Party Offerings.

"Third-Party Offerings" means (a) third-party services, software, products, and other offerings that are not incorporated into the Services or Software, (b) offerings identified in the "Third-Party Terms" section of the Service Specific Terms, and (c) third-party operating systems.

Scope Limitations: Use Restrictions

The scope of services concept will likely extend beyond the defined terms. Our business lawyer should also focus on the affirmative and restrictive covenants, as they will contain statements of acceptable and prohibited uses.

Sample Language:

Restrictions. Neither you nor any End User will use the [Vendor's] Content or Services in any manner or for any purpose other than as expressly permitted by this Agreement. Neither you nor any End User will, or will attempt to (a) reverse engineer, disassemble, or decompile the Services or [Vendor] Content or apply any other process or procedure to derive the source code of any software included in the Services or [Vendor] Content (except to the extent applicable law doesn't allow this restriction), (b) access or use the Services or [Vendor] Content in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (c) resell the Services or [Vendor] Content. . . .

Scope Limitations: Use Restrictions

Our business lawyer will likely find additional use restrictions in ancillary agreements, such as the Acceptable Use Policy (AUP).

Consider the restrictions, or prohibitions against non-acceptable uses of the services, contained in the Amazon Acceptable Use Policy, found at https://aws.amazon.com/aup/.

You may not use, or facilitate or allow others to use, the Services or the [Vendor] Site:

1. for any illegal or fraudulent activity;
2. to violate the rights of others;
3. to threaten, incite, promote, or actively encourage violence, terrorism, or other serious harm;
4. for any content or activity that promotes child sexual exploitation or abuse;
5. to violate the security, integrity, or availability of any user, network, computer or communications system, software application, or network or computing device;
6. to distribute, publish, send, or facilitate the sending of unsolicited mass email or other messages, promotions, advertising, or solicitations (or "spam").

Scope Limitations: Use Restrictions

Many vendors prohibit “high risk activities.” This restriction may vary slightly from vendor to vendor but will likely only affect a subset of potential customers.

Sample Language:

3.3 **Restrictions**. Customer will not, and will not allow End Users to, . . . access or use the Services (i) for High Risk Activities. . . .

“High Risk Activities" means activities where the use or failure of the Services would reasonably be expected to lead to death, personal injury, or environmental or property damage (such as the creation or operation of nuclear facilities, air traffic control, life support systems, or weaponry).

Scope Limitations: Use Restrictions

For many customers, avoiding the operation of high-risk activities and avoiding illegal or fraudulent activities may not pose an issue or conflict with the enterprise's goals for the services.

However, if any use restrictions impair the enterprise's objective(s), our business lawyer needs to explore with the stakeholders the legal risks of proceeding with a contract that does not fully meet the business needs. Negotiating an exception to use restrictions may be an uphill and/or expensive battle for our business lawyer. The vendor may see such a change as operationally unfeasible and/or require additional spend or contract commitments to make such an exception. Alternatively, the enterprise may need to develop a work-around in-house and/or find a third party to provide a work-around.

Examples:

- A restriction on handling copyrighted or trademarked works may not be an issue for many customers, but in the higher education space, where fair use exceptions are more routine, the vendor's restriction could be overly burdensome and a potential trigger for vendor termination or suspension of services.

- A restriction on the handling of personal health information ("PHI") may not be an issue in certain industries, but an enterprise customer that has an affiliated health system or for other reasons will handle protected health information may need to separately address PHI restrictions in the agreement.

Scope Limitations: Warranty and Indemnification Exclusions

A vendor may permit combinations and/or modifications by the customer or with third-party add-ons, or may offer "additional services." However, such combinations or modifications, even if necessary in the enterprise's mind to meet its needs and achieve appropriate scope, may void the vendor's warranty and/or create an exclusion to the vendor's indemnification obligations.

Sample Language:

(c) Neither party will have obligations or liability under this [indemnification provision for IP infringement] arising from infringement by combinations of the Services or Your Content, as applicable, with any other product, service, software, data, content or method.

13.3 Exclusions. Sections [Vendor and Customer Indemnification Obligations) will not apply to the extent the underlying allegation arises from . . . (b) a combination of the indemnifying party's technology or Brand Features with materials not provided by the indemnifying party under the Agreement, unless the combination is required by the Agreement, and (c) in the case of Google or any of its Affiliates as the indemnifying party, any Services provided to Customer free of charge.

Pro Tips:

- Match up "scope"—as restricted or limited—with "business need."
- Make a plan for any gaps in expected services.
- Contemplate that additional spend may be a prerequisite to, and/or that there may be additional costs associated with, additional services or a vendor-authorized deviation from use restrictions.
- Look at vendor warranties to confirm appropriate coverage.



PRO TIPS:

Can the vendor's services still "solve" for the problem/goal if they are materially limited in scope?

Our business lawyer will need to consider limits placed on the enterprise's use of the services by focusing on contractual restrictions or limitations on use.

Does the enterprise expect to receive services or conduct activities that are on the "prohibited" or "restricted" list?

Our business lawyer needs to understand what each business unit expects to receive from the "services" to fully appreciate if one business unit needs access to limited or restricted services.

What work-arounds are available if the scope does not equal expectations ?

Can the enterprise obtain "Additional Services" or "Third-Party Services" or develop an in-house work-around?

Will this require additional spend or internal cost? Could this affect the vendor warranties and indemnification?

2. Industry-Specific Terms

Additional Terms for Specific Industries



Our business lawyer should endeavor to help the business team consider industry- or sector-specific needs that might be affected by contract terms beyond use restrictions.

For example, legal services, financial services, health care, and research and education institutions may have regulatory requirements relating to data handling or audits that need to be addressed with supplemental contract terms.



The business team and lawyer, working together, should inquire about sector-specific addenda that cloud providers may offer.

Such additional terms may not be readily accessible from the public website where standard customer agreements are posted.

Public Institutions

Public institutions or governmental entities may be governed by additional or different terms.

Does the contract provide for an alternate set of rules; and, if so, how/when do those rules apply to the enterprise?

Sample Language:

14.12 U.S. Governing Law.

(a) For U.S. City, County, and State Government Entities. If Customer is a U.S. city, county, or state government entity, then the Agreement will be silent regarding governing law and venue.

(b) For U.S. Federal Government Entities. If Customer is a U.S. federal government entity, then the following applies: ALL CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SERVICES WILL BE GOVERNED BY THE LAWS OF THE UNITED STATES OF AMERICA, EXCLUDING ITS CONFLICT OF LAWS RULES. SOLELY TO THE EXTENT PERMITTED BY FEDERAL LAW, (I) THE LAWS OF THE STATE OF CALIFORNIA (EXCLUDING CALIFORNIA'S CONFLICT OF LAWS RULES) WILL APPLY IN THE ABSENCE OF APPLICABLE FEDERAL LAW; AND (II) FOR ALL CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SERVICES, THE PARTIES CONSENT TO PERSONAL JURISDICTION IN, AND THE EXCLUSIVE VENUE OF, THE COURTS IN SANTA CLARA COUNTY, CALIFORNIA.

(c) For All Other Entities. If Customer is any entity not identified in Section 14.12(a) (U.S. Governing Law for U.S. City, County, and State Government Entities) or (b) (U.S. Governing Law for Federal Government Entities), then the following applies: ALL CLAIMS ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SERVICES WILL BE GOVERNED BY CALIFORNIA LAW, EXCLUDING THAT STATE'S CONFLICT OF LAWS RULES, AND WILL BE LITIGATED EXCLUSIVELY IN THE FEDERAL OR STATE COURTS OF SANTA CLARA COUNTY, CALIFORNIA, USA; THE PARTIES CONSENT TO PERSONAL JURISDICTION IN THOSE COURTS.

Health-Related Services

Enterprises in health-care-related or health-care ancillary industries, particularly any industry involving PHI, may require additional agreements or different terms (e.g., business associate agreement ("BAA"), special services agreement).

Sample Language:

Customer Obligations

Customer is solely responsible for: (1) the accuracy and adequacy of information and Data furnished through use of the Azure Health Bot Service; (2) implementing a secure application-to-application authentication method between the Customer Health Bot Application and the Azure Health Bot Service; (3) obtaining appropriate consent from end users in connection with their use of the Customer Health Bot Application; and (4) displaying appropriate warnings, disclaimers, and acknowledgements to end users in connection with their use of the Customer Health Bot Application, including, as applicable, those set forth in the following form.

(Azure Health Bot Service)

When using the third party vendor workforce option of Amazon Augmented AI, you are responsible for ensuring that the vendor meets any compliance requirements applicable to any personal data or confidential information in your data or content. You may not share data or content that contains protected health information with the third party vendor workforce.

(AWS)

Customer will not, and will not allow End Users . . . (viii) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA.

(Google Cloud)

Publishers and Third-Party Content Providers

Similarly, in industries and business operations where the enterprise is hosting content, there may be additional obligations under the enterprise agreement, as well as the AUP and other ancillary agreements.

Sample Language:

3.6 Third-Party Content Enforcement. If Customer's primary use of the Services is to host third-party content or facilitate the sale of goods or services between third parties on its platform, Customer will take the following steps to enforce compliance with the AUP: (a) publish policies defining what content is prohibited on its platform (e.g., illegal content); (b) maintain a publicly accessible method (e.g., webform or email alias) to receive notices of violation of that policy (in addition to a monitored communications channel for Google); and (c) promptly review and address any such notices, and remove content where appropriate.

Other Specific Industries

Vendors may have a list of restrictions for various industries, including those related to crypto, telecommunications, or, as noted earlier, PHI. In addition, there may be restrictions prohibiting "illegal" activities, which may be general or refer to specific laws.

Sample Language:

3.3 Restrictions. Customer will not, and will not allow End Users to, . . . access or use the Services (i) for High Risk Activities; (ii) in violation of the AUP; . . . (iv) to engage in cryptocurrency mining without [Vendor's] prior written approval; (v) to operate or enable any telecommunications service or in connection with any Customer Application that allows End Users to place calls or to receive calls from any public switched telephone network, unless otherwise described in the Service Specific Terms; (vi) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (vii) in a manner that breaches, or causes the breach of, Export Control Laws; or (viii) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA.

Pro Tips:

- ❑ All enterprises need to consider how the standard terms fit with their specific business needs, as well as how they may expect their relationship with suppliers, customers, and affiliates in restricted industries to be affected.

- ❑ There are industry-specific terms—some of which are more restrictive—that highlight the need of our business lawyer to think about standard terms as they apply to specific business needs.

- ❑ An opportunity is presented for our business lawyer to add value by considering not only the current industry and the role of customers, suppliers, and affiliates, but also the enterprise's plans for expansion.



3. Entire Agreement: What Is the Agreement?

Which Agreement Applies?

Many cloud service providers offer their standard terms on their (or their resellers') websites. Will (or should) those terms apply to your client?

Perhaps you have negotiated a separate enterprise contract—directly with the vendor OR a reseller. Which terms will (or should) apply to your enterprise and/or your users? The standard terms provided online or the terms in the separately negotiated enterprise contract?

Will the enterprise's location, industry, user profile (who will use the services via the enterprise, e.g. designated employees versus members of the public), or other factor make a difference as to which agreement applies?

Sample Language:

If you signed an offline variant of this Agreement for use of the [Cloud Platform Services] under the same [Cloud Platform Account], the terms below do not apply to you, and your offline terms govern your use of the [Cloud Platform Services].

*If your address is in India, please review the [Customer Agreement], which governs your access to and use of the Service Offerings.

*Please note that as of July 1, 2018, customers located in Europe, the Middle East, or Africa (other than South Africa) contract with our European based [Vendor] Contracting Party, as provided in Section 12. See the [Vendor] Europe FAQ for more information.

Other Terms Incorporated by Reference

Often, there will be vendor ancillary agreements, and even third-party terms, incorporated by reference. Hyperlinked terms extend agreements beyond their four corners. (This drafting practice is not unique to cloud service agreements.)

The incorporated terms can be material and may contain key definitions and requirements, such as with respect to the scope of services, privacy, security, data management, and termination (as further discussed in this exercise). Yet, such terms can be subject to unilateral change by the vendor simply with notice to the enterprise.

Sample Language:

- "Service Specific Terms" means the then-current terms specific to one or more Services stated at https://cloud.google.com/terms/service-terms.
- "Services" means the then-current services described at https://cloud.google.com/terms/services, excluding any Third-Party Offerings.

- "DPA" means the Microsoft Products and Services Data Protection Addendum, as updated from time to time, published at https://aka.ms/DPA or a successor site and any additional data protection terms that Microsoft presents with this Agreement.

- "Privacy Notice" means the privacy notice located at http://aws.amazon.com/privacy (and any successor or related locations designated by us), as may be updated by us from time to time.

Priority of Terms and Ability to Amend

We know that there may be multiple pieces to this arrangement. The precedence given the various pieces of the agreement should be set out in the merger clause (the "Entire Agreement" provision).

Consider the sample, which places terms presented when an order is placed (presumably later in time) subordinate to general, earlier agreed terms.

Consider also how the Entire Agreement provision may tie in with the vendor's ability to unilaterally update.

Sample Language:

Order of precedence. If there is a conflict between any documents in this Agreement that is not expressly resolved in those documents, their terms will control in the following order, from highest to lowest priority: (1) DPA [Data Protection Addendum]; (2) these General Terms; (3) Product Terms; (4) SLA [Service Level Agreement]; and (5) any additional terms presented when an order is placed. Terms in an amendment control over the amended document and any prior amendments concerning the same subject matter.

14.15 Entire Agreement. This Agreement . . . supersedes all other agreements between the parties relating to its subject matter. . . . The URL Terms are incorporated by reference into the Agreement. After the Effective Date, Vendor may provide an updated URL in place of any URL in this Agreement.

Priority of Terms and Ability to Amend

Sample Language:

(b) To the Agreement. Vendor may make changes to this Agreement (including the URL Terms) and pricing from time to time. Unless otherwise noted by Vendor , material changes to the Agreement will become effective 30 days after they are posted, except to the extent the changes apply to new functionality or the Cloud Data Processing Addendum, or are required by applicable law, in which case they will be effective immediately. Google will provide at least 90 days' advance notice for materially adverse changes to any SLAs by . . . If Customer does not agree to the revised Agreement, Customer may stop using the Services. Customer may also terminate this Agreement for convenience under Section 8.4 (Termination for Convenience). Customer's continued use of the Services after such material change will constitute Customer's consent to such changes. Vendor will post any modification to this Agreement to [link to terms].

. . .

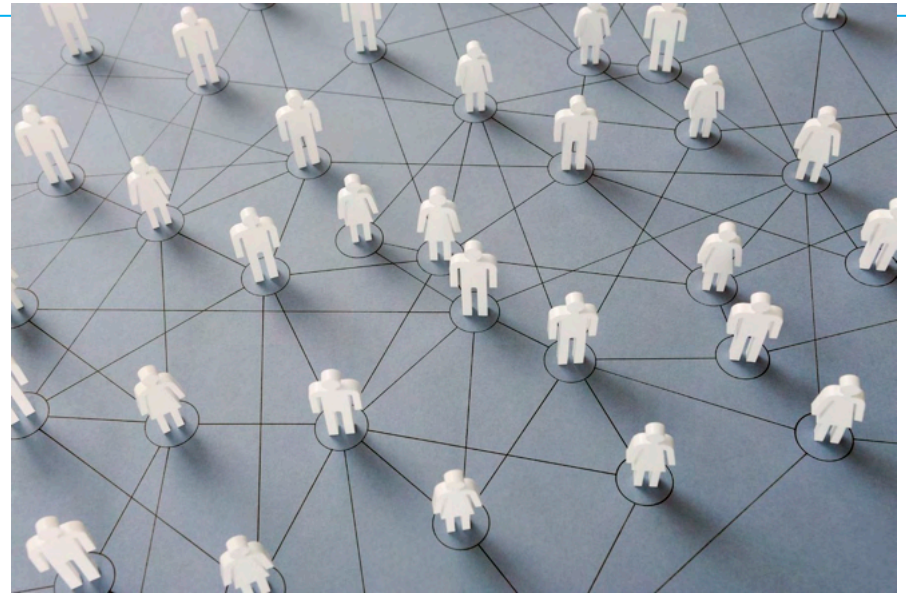
If Vendor makes a material change to the Cloud Data Processing Addendum in accordance with this Section 1.4(c) (Modifications: To the Cloud Data Processing Addendum), Vendor will post the change at the webpage containing the Cloud Data Processing Addendum.

Role of Third-Party Applications

Third-party applications and software may be made available and may even be required for effective use of the services.

However, they will likely be specifically excluded from the definition and scope of *services*. Additional terms with respect to these applications may be included or incorporated directly in a hyperlink or in a different document and/or a separate transaction.

Attention should be paid to how third-party applications may affect indemnification and warranty obligations, as well as payment obligations and affirmative and restrictive covenants.



Role of Third-Party Applications

Key Questions

Does the enterprise have visibility with regard to the scope of use and operation of these third-party applications?

How are third-party applications and software governed? Is there a separate agreement? Can the enterprise negotiate terms?

Can the enterprise "opt out" or use a different vendor for such applications? How does this affect pricing and scope of use?

How does the use of third-party applications affect the indemnification provisions? The vendor's warranty on the services?

Role of Third-Party Applications

Sample Language, generally:

Software. [Vendor] may make Software available to Customer, including third-party software. Customer's use of any Software is subject to the applicable provisions in the Service Specific Terms.

Termination Rights

We may also terminate this Agreement immediately upon notice to you …, (B) if our relationship with a third-party partner who provides software or other technology we use to provide the Services expires, terminates or requires us to change the way we provide the software or other technology as part of the Services, …

Sample Language, for specific products:

Non-Microsoft Products

Non-Microsoft Products are provided under separate terms by the Publishers of such products. Customer will have an opportunity to review those terms prior to placing an order for a Non-Microsoft Product through a Microsoft online store or Online Service. Microsoft is not a party to the terms between Customer and the Publisher. Microsoft may provide Customer's contact information and transaction details to the Publisher. Microsoft makes no warranties and assumes no responsibility or liability whatsoever for Non-Microsoft Products. Customer is solely responsible and liable for its use of any Non-Microsoft Product.. . .

Pro Tips:

- Identify the universe of documents, agreements, T&Cs, order forms, etc., that may be involved with the enterprise's use of the services.
- Keep in mind that third-party applications may be desired and/or required, adding to the universe.
- Appreciate the priority of all such ancillary materials for interpretation of the enterprise's main agreement with the vendor. Be mindful of any conflicting or absent language across ancillary materials (e.g., different approaches to dispute resolution, limitations of liability, etc.).
- Don't forget about typical boilerplate provisions, like "Entire Agreement," "Amendment," and "Third-Party Beneficiary" provisions, and how those may affect specific services, clients, and industries.



4. Allocation of Risk

Approach to Risk Allocation: Shared Responsibility



Our business lawyer understands that cloud services are complex and varied—customers have many options to select products and services at different layers in the "technology stack."

Responsibility for selecting, implementing, and managing many of the services commonly will fall to the enterprise. This may be referred to as the "shared responsibility" model.

The vendor is providing the enterprise with tools and accepts some base liability for those tools; however, the risks of when, where, why, and how the enterprise chooses to use those tools often is allocated, as between the two parties, to the enterprise.

Approach to Risk Allocation: Shared Responsibility



- Enterprise responsibilities will be different for software as a service ("SaaS"), platform as a service ("PaaS"), and infrastructure as a service ("IaaS"). There may be further differentiation by industry and scale/spend.
- Market factors may also affect the balance of the risk allocation between the vendor and the enterprise.
- Generally, this will not be an area of opportunity for material negotiation. Still, the business lawyer who appreciates areas of potential movement and scope of assumed risk can add value to the process.

Shared Responsibility: Generally

Sample Language:

3. Customer Obligations.
3.1 *Compliance.* Customer will (a) ensure that Customer and its End Users' use of the Services complies with the Agreement, (b) use commercially reasonable efforts to prevent and terminate any unauthorized use of, or access to, the Services, and (c) promptly notify Google of any unauthorized use of, or access to, the Services, Account, or Customer's password of which Customer becomes aware. Google reserves the right to investigate any potential violation of the AUP by Customer, which may include reviewing Customer Applications, Customer Data, or Projects.
3.2 *Privacy.* Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Services and (b) [Vendor's] accessing, storing, and processing of data provided by Customer (including Customer Data, if applicable) under the Agreement.

Your Security and Backup. You [customer] are responsible for properly configuring and using the Services and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content.

. . .

End Users. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Services. You are responsible for End Users' use of Your Content and the Services, and for their compliance with your obligations under this Agreement.

Allocation of Risk: Customer Data

Generally, the terms *customer data* and *customer content* align closely with the ordinary meaning of those words. Where these terms tend to differentiate is in the responsibilities relating to data or content.

Data and content concepts are closely tied to the discussion of risk and liability; depending on how the services are used and the type of data involved, the risk profile will shift.

Sample Language:

"Customer Data" means all data, including all text, sound, video or image files, and software, that are provided to [Vendor] or its Affiliates by, or on behalf of, Customer and its Affiliates through use of Online Services. Customer Data does not include Professional Services Data.

"Customer Data" means data provided to [Vendor] by Customer or End Users through the Services under the Account, and data that Customer or End Users derive from that data through their use of the Services.

"Content" means software (including machine images), data, text, audio, video, or images.
. . .

"Your Content" means Content that you or any End User transfers to us for processing, storage or hosting by the Services in connection with your …account and any computational results that you or any End User derive from the foregoing through their use of the Services. For example, Your Content includes Content that you or any End User stores …. Your Content does not include Account Information.

Allocation of Risk: Use of Data

The enterprise will likely be responsible for deciding where to put its data for processing and storage, including the specific region/geography, the type of security, and the type of services.

Note how the vendor may require enterprise responsibility for all consents as well as compliance with all laws and applicable terms.

Sample Language:

Before providing Personal Data to [Vendor], Customer will obtain all required consents from third parties (including Customer's contacts, Partners, distributors, administrators, and employees) under applicable privacy and data protection laws.

Your Content. You are responsible for Your Content. You will ensure that Your Content and your and End Users' use of Your Content or the Services will not violate any of the Policies or any applicable law.

1.4 Data Privacy. You may specify the [Vendor designated geographic regions] in which Your Content will be stored. You consent to the storage of Your Content in, and transfer of Your Content into, the [Vendor designated geographic regions] you select.

Allocation of Risk: Use of Data

The enterprise will look for restrictions on how the vendor (and its affiliates and third parties) may use its data, as well as provisions with respect to ownership.

Consider the value of the enterprise's suggestions and feedback, particularly if the data could include sensitive information.

Sample Language:

You consent to our use of Your Content to provide the Services to you and any End Users.

. . .

6.5 Suggestions. If you provide any Suggestions to us or our affiliates, we and our affiliates will be entitled to use the Suggestions without restriction. You hereby irrevocably assign to us all right, title, and interest in and to the Suggestions and agree to provide us any assistance we require to document, perfect, and maintain our rights in the Suggestions.

5.2 Protection of Customer Data. Google will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. . . .

5.3 Customer Feedback. At its option, Customer may provide feedback or suggestions about the Services to Google ("Feedback"). If Customer provides Feedback, then Google and its Affiliates may use that Feedback without restriction and without obligation to Customer.

Allocation of Risk: Data Security

- Our business lawyer will appreciate that the shared responsibility model may place responsibility for the sufficiency of data protection measures on the enterprise.
- The vendor should provide some contractual assurances as to its data security protections, testing, and notice protocols, often found in the master services agreement and/or ancillary agreements, such as the DPA (Data Protection Addendum) or the privacy policy.
- If the enterprise has specific requirements, they need to be addressed early in the procurement process to ensure that the vendor selected has the appropriate capabilities (and that the contract matches the sales pitch). For example, an enterprise may require certain compliance standards, data stored in certain geographies, and certain testing and notices with test results—and not all vendors are able or willing to comply with such requests.

When discussing data, our business lawyer will often have the difficult "what if" conversation: What if data is lost? What if there is a data breach? What if data needs to be moved quickly? What if the enterprise's requirements shift or increase over time?

And a "how" conversation: How dependent is the enterprise on access to the data and use of the services?



Allocation of Risk: Data Security

Sample Language:

[Vendor] Security. Without limiting Section 8 [Disclaimers] or your obligations under Section 2.2 [Your Content], we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

. . .

Your Security and Backup. You are responsible for properly configuring and using the Services and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content.

Allocation of Risk: Data Security

Sample Language across Microsoft agreements:

Microsoft and its Affiliates, and their respective agents and subcontractors, will process Customer Data, Personal Data, and Professional Services Data as provided in this Agreement and the DPA, which is incorporated by reference.

Microsoft DPA [Microsoft Products and Services Data Protection Addendum, found at https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA]:
Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Products and Services meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Microsoft provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application).

Allocation of Risk: Data Security

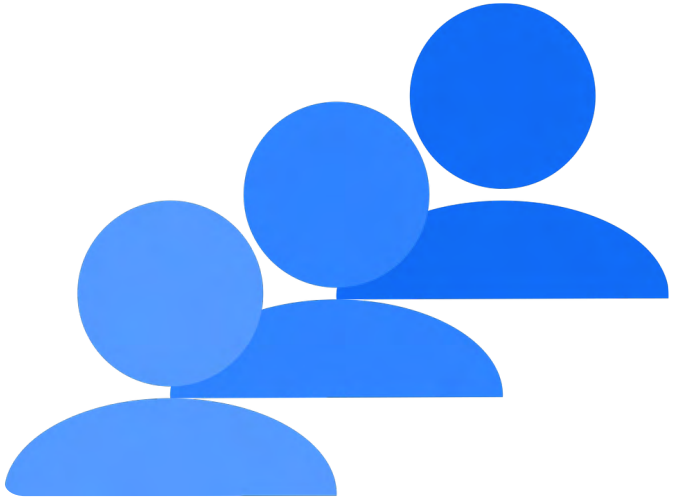
Sample Language across Google agreements:

Protection of Customer Data. [Vendor] will only access, use, and otherwise process Customer Data in accordance with the Cloud Data Processing Addendum and will not access, use, or process Customer Data for any other purpose. [Vendor] has implemented and will maintain technical, organizational, and physical measures to protect Customer Data, as further described in the Cloud Data Processing Addendum.

Google Cloud Data Processing Addendum [Google CDPA, found at https://cloud.google.com/terms/data-processing-addendum]:

Customer's Security Assessment. Customer agrees that the Services, Security Measures implemented and maintained by [Vendor], Additional Security Controls and Google's commitments under this Section 7 (Data Security) provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals).]

Allocation of Risk: User Risk and Liability



- In many cases, the vendor will expect that the enterprise will be responsible and liable for all users.
- The scope of risk may be determined by the scope of use. Will these services be "used" across the enterprise or by a single, focused business unit? By a few or many users? By users under the enterprise's control?
- For certain services, some liability may be imputed to certain users; in such cases, the individual user, not the enterprise, would be held liable by the vendor for misuse or breach of terms, based on a separate set of terms and conditions agreed to by the user.
- However, in the context of a "master" agreement for services, an enterprise will likely be pushed by the vendor to additionally accept liability obligations with respect to the individual users.
- An enterprise may mitigate this expanded risk with the help of our business lawyer by limiting use, placing internal controls on use and data processed, and/or requiring the users to agree to terms (e.g., employee handbook, student code of conduct, agreement to T&Cs that mirror the vendor's requirements for use). An enterprise may be able to further negotiate for an acceptable use policy to be presented directly to certain users or types of users, as well as priority language ensuring the enterprise agreement and individual AUP work side by side.

Allocation of Risk: User Risk and Liability

Key to the discussion of the allocation of user liability is the identification of who is the user and how much "control" the enterprise has over such user and its actions.

An employee of the enterprise, who may be under the control and direction of the enterprise and subject to an employee handbook or other enterprise guidelines.

Customers and clients of the enterprise, who are generating income for the enterprise but also potentially creating liability.

Users outside of the organization, who may not have visibility with regard to the terms and restrictions on use, but are nonetheless bound by them and can create liability for the enterprise.

Additional issues with regard to the location, age, and role of the end user may affect the risk profile.

Allocation of Risk: User Risk and Liability

Sample Language:

3.1 Compliance. Customer will (a) ensure that Customer and its End Users' use of the Services complies with the Agreement, (b) use commercially reasonable efforts to prevent . . .

. . .

3.3 Restrictions. Customer will not, and will not allow End Users to . . .

2.2 Your Content. You are responsible for Your Content. You will ensure that Your Content and your and End Users' use of Your Content or the Services will not violate any of the Policies or any applicable law.

2.5 End Users. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Services. You are responsible for End Users' use of Your Content and the Services, and for their compliance with your obligations under this Agreement. If you become aware of any violation of your obligations under this Agreement caused by an End User, you will immediately suspend access to Your Content and the Services by such End User. We do not provide any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide such support or services.

Allocation of Risk: Vendor Indemnification

It is common to see indemnification obligations from the vendor to the customer in the limited case of third-party claims for IP infringement, and as the sole and exclusive remedy for infringement claims, subject to exceptions. Vendors typically hold firm and will not accept indemnification obligations outside of third-party IP infringement claims.

With the vendor's greater leverage, our business lawyer may be frustrated by the unbalanced approach to indemnification—even if it appears to be "mutual." However, our business lawyer may be able to achieve additional balance on a case-specific basis by managing other factors discussed in this exercise, as well as negotiating the other risk allocation and limitations on liability provisions, such as disclaimers, caps, and insurance.

Sample Language:

13.1 [Vendor] Indemnification Obligations. [Vendor] will defend Customer and its Affiliates using the Services under Customer's Account and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that any Service or any [Vendor Brand Feature], in each case used in accordance with the Agreement, infringes the third party's Intellectual Property Rights.

Allocation of Risk: Enterprise Indemnification

It is common to see broad indemnification obligations from the customer to the vendor, and such obligations may be uncapped.

Sample Language:

General. You will defend, indemnify, and hold harmless us, our affiliates and licensors, and each of their respective employees, officers, directors, and representatives from and against any Losses arising out of or relating to any third-party claim concerning: . . . [Reciprocal indemnity provided only for infringement claims.]

13.2 Customer Indemnification Obligations. Customer will defend [Vendor] and its Affiliates providing the Services and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from (a) any Customer Application, Project, Customer Data, or Customer Brand Features; or (b) Customer's or an End User's use of the Services in breach of the AUP or Section 3.3 (Restrictions).

Pro Tips:

- ❑ Understanding the enterprise's risk tolerance and the risks associated with proposed and potential use of the services is key to having a true grasp of the business.
- ❑ Our business lawyer should be aware of these specific nuances that affect the enterprise's standing.
- ❑ Negotiating for more favorable risk allocation will be challenging. However, an enterprise's ability to do so may be augmented by its spend; alteration of the scope of use, including user access; industry requirements; and/or other market conditions.
- ❑ Our business lawyer may also mitigate the effect of the contractual risk allocation by educating the business units to understand the risks and assisting in the creation of internal protocols to manage and mitigate such risks.



PRO TIPS:

Allocation of Risk: Overview



What risks does the enterprise face when using these services? What is the enterprise's risk tolerance for accepting certain risks?



What type of services (SaaS, PaaS, IaaS) are being provided, and what data will (or could) be input or exported using the services?



What is the scale of (potential) use, who could use or have access to these services, and what could they do with the services?



In the event of an issue, what contractual controls are in place for each party to notify the other? To suspend services or revoke access?



Are operational controls provided for in the contract? Do the parties have the operational capacity to employ internal controls?



Consider termination scenarios and post-termination obligations.

PRO TIPS:

Allocation of Risk: Data, Security, and Privacy

- ✓ Maintain up-to-date versions of the DPA, privacy policy, and any other ancillary agreements.
- ✓ Monitor modifications to the contract.
- ✓ Understand the reach of the vendor's privacy policy. Does it apply to only the enterprise, to all users, or to subsets of content/data?
- ✓ Ensure that the agreement provides for appropriate ownership of the content and use. For example, can the vendor use customer content beyond legitimate business purposes in connection with providing the services? Look for provisions allowing use for improving business practices, new product development, feedback, etc.
- ✓ Confirm the applicability of federal and state laws and regulations, and identify areas of potential disconnect in vendor compliance.
- ✓ Identify where data will be stored and processed by the vendor.
- ✓ Identify users and scale of use; consider how possible scale-ups and scale-downs would affect business operations and potentially trigger contractual obligations.

Potential Internal Controls to Mitigate Risk

PRO TIPS:

- Maintain up-to-date notice information in the event of a security issue or potential breach of the terms; ensure that if notice is through a vendor portal, it is directed internally to the appropriate parties. Consider the timing needed for the enterprise to comply with other obligations (to regulatory authorities, stakeholders, insurance, etc.).
- Monitor user compliance; create a system to allow limited suspension or revocation of access of certain users.
- Ensure that decision-makers understand the scale and scope of use, including what data is being processed (or could be made available) and the range and types of permitted users (and other potential users).
- Ensure that users click through terms and/or are presented with governing terms in connection with their use; provide appropriate training as applicable.
- Review the enterprise's insurance requirements and the vendor's contractual obligation to maintain coverage.

5. Endgame: Term and Termination

End of Relationship: Term

While a mutual termination for convenience provision may seem to be balanced in many commercial contracts, in this context it might be impossible for the enterprise to extract and migrate data and fully transition to a new vendor without interrupting business operations, particularly on short notice that may come without warning.

Consider a typical 30- or 60-day notice for termination without cause, as well as an immediate termination right in the event of a breach. Compare the time and effort necessary for the enterprise to transition from a cloud service to the time and effort necessary for the vendor to turn off the service. The enterprise's need to terminate and the vendor's termination rights can pose material issues to the enterprise's operations.

Sample Language:

Termination without cause. Either party may terminate this Agreement without cause on 60 days' notice. Termination without cause will not affect Customer's perpetual licenses. Licenses granted on a subscription basis and access to Online Services and Microsoft Support Services will continue for the remainder of the then-current subscription period(s) or support term, subject to the terms of this Agreement.

Termination for Convenience. Customer may stop using the Services at any time. Customer may terminate this Agreement for its convenience at any time on prior written notice and, upon termination, must cease use of the applicable Services. Google may terminate this Agreement for its convenience at any time with 30 days' prior written notice to Customer.

…

Effect of Termination. If the Agreement is terminated, then (a) all rights and access to the Services will terminate (including access to Customer Data, if applicable), unless otherwise described in this Agreement, and (b) all Fees owed by Customer to Google are immediately due upon Customer's receipt of the final electronic bill or as stated in the final invoice.

End of Relationship: Role of Third Parties

A potential trigger for termination may be a third party.

A third-party infringement claim may give rise to a vendor's right to terminate or modify the services.

Additionally, the termination of the vendor's relationship with third-party suppliers may also give rise to the vendor's right to terminate or modify the services.

These third-party actions will likely be outside of the enterprise's visibility and control.

Sample Language:

We may also terminate this Agreement immediately upon notice to you . . .
(B) if our relationship with a third-party partner who provides software or other technology we use to provide the Service Offerings expires, terminates or requires us to change the way we provide the software or other technology as part of the Services. . . .

(d) For any claim covered by Section [indemnification for IP infringement], [Vendor] will, at its election, either: (i) procure the rights to use that portion of the Services alleged to be infringing; (ii) replace the alleged infringing portion of the Services with a non-infringing alternative; (iii) modify the alleged infringing portion of the Services to make it non-infringing; or (iv) terminate the allegedly infringing portion of the Services or this Agreement.

End of Relationship: Process Planning, Generally

Part of our business lawyer's task will be to focus attention on the end of the relationship with the vendor, which may be challenging, particularly if the business units are excited and optimistic about the services and the vendor. Considerations may include the following:

- Understanding the **base term** while acknowledging the enterprise's investment in this relationship. If there are financial and temporal investments, the enterprise may look for a longer initial term to allow it to recoup its costs.
- Awareness around the **vendor's termination rights and suspension rights** in the event of breach (or alleged breach) or other events. Understanding the enterprise's termination rights and the minimum time needed to exercise such rights.
- Identifying **force majeure events** and the scope of the force majeure provision.
- Availability and **accessibility of backup data**, without vendor assistance (or other technical assistance).
- Potential **overlap between payment and other obligations** and the vendor's obligation to turn over data.
- Post-termination **confidentiality** obligations and **data security and privacy** obligations. Possible state law **restrictions on vendors holding data "hostage."**

End of Relationship: Data Management

Review of the contract provisions highlights the need for process planning that includes recovering customer data at the end of the relationship, whether it be a friendly or unfriendly breakup. These are opportunities for the business lawyer to remind the enterprise about business processes and contingency planning for disruptions and end of service.

Sample Language:

8.6 Effect of Termination. If the Agreement is terminated, then (a) all rights and access to the Services will terminate (including access to Customer Data, if applicable), unless otherwise described in this Agreement, and (b) all Fees owed by Customer to Vendor are immediately due upon Customer's receipt of the final electronic bill or as stated in the final invoice.

Post-Termination. Unless we terminate your use of the Services pursuant to Section 5.2(b) [for cause], during the 30 days following the Termination Date:

(i) we will not take action to remove from the [Vendor] systems any of Your Content as a result of the termination; and

(ii) we will allow you to retrieve Your Content from the Services only if you have paid all amounts due under this Agreement.

End of Relationship: Data Management

Additionally, the relevant terms may also be found in ancillary agreements, such as the Data Processing Addendum or Data Protection Addendum.

Consider the treatment of Data Retention in the Microsoft DPA.

[Microsoft Products and Services Data Protection Addendum, found at https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.]

Sample Language:

Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA to retain such data.

End of Relationship: Data Management

The contract review and process planning should consider contractual provisions and operational controls that would address data management specific to the following:

- Recovering data from vendors (and third parties) in a usable and transferable format upon termination of the service for any reason
- Temporary storage of data and potential continued access to the vendor's portal as needed
- Engaging/procuring a new vendor
- Data-migration tools
- Ensuring the purge of data and return of confidential information distributions (as requested of materials) from the terminated service and vendor



End of or Changes in Relationship: Force Majeure Triggers

Our business lawyer should also engage in discussions with the business teams to ensure that—as with the difficult conversations around termination—in the unfortunate event of an early termination or suspension of services due to a force majeure, the enterprise has a transition plan ready.

Many vendors provide a force majeure provision that may seem mutual but is more likely (as with other provisions) to lean in favor of the vendor.

The enterprise should appreciate that there is no guarantee of uninterrupted service; and, in fact, the vendor may have carved out interruptions caused by factors outside of the vendor's reasonable control in a force majeure.

Our business lawyer should ask:

- Is the vendor contractually obligated to mitigate force majeure events? If the vendor's negligence or poor business practices contributed to a force majeure event, would the application of and relief offered by a force majeure provision be voided?
- Is the force majeure provision truly mutual? Would it apply to the enterprise's ability to satisfy payment obligations? Ability to deliver reports or other items required by the vendor? Ability to ensure compliance (and user compliance) with T&Cs?

Force Majeure Exceptions

Negligence

Avoid overly broad force majeure ("FM") provisions that would except performance even if the FM event was due to the vendor's own negligence (e.g., the vendor fails to properly maintain its technology, which is subsequently damaged).

Payment Obligations

Would the enterprise's payment obligations continue through an FM event that allows the vendor to stop providing the services?

Can the failure of the payment technology/system act as an FM event to excuse the enterprise's payment obligations (during such failure)?

Changes in Laws

In a highly regulated industry, does a change in law or legal requirements constitute an FM if it materially affects the vendor's ability to provide the services at the contractual pricing?

With new data privacy and security laws at the state, federal, and international levels on the horizon, could a new (stricter) law that makes business more expensive constitute an FM event?

End of Relationship: Force Majeure

Sample Language:

Force Majeure. Neither party will be liable for failure or delay in performance to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, terrorism, riots, or war.

Force Majeure. We and our affiliates will not be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, electrical or power outages, utilities or other telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

End of Relationship: Force Majeure

As our business lawyer has found before, relevant terms may also be found in ancillary agreements, such as the Service Level Agreement (SLA).

Consider the exception allowing nonconformance with the SLA and the various service level standards contained in the Service Level Agreement for Microsoft Online Services, found at https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services.

Sample Language:

This SLA and any applicable [service standards] do not apply to any performance or availability issues:

1. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center) . . .

Pro Tips:

- This is an area where our business lawyer can add value by understanding the business use and advising the clients on best practices.
- Our business lawyer can also encourage appropriate planning, particularly for uncomfortable outcomes such as a sudden or unfriendly termination of services and access to the data and/or the unfortunate event of a data breach.
  - An enterprise that is prepared with a contingency plan will be in a better position to withstand such an event.



PRO TIPS:

End of Relationship Considerations

- ✓ Understand the contractual notification obligations of both parties.
  - ✓ What notice must the vendor give for a termination with or without cause?
  - ✓ What termination triggers could cause disruption to the enterprise's operations?
- ✓ Counsel business units on strategy.
  - ✓ With respect to vendor actions: What if the vendor breaches this agreement? What if the vendor does not or cannot comply with applicable law? What if services are discontinued?
  - ✓ With respect to third-party actions: What if there are third-party supplier issues? What if there are third-party claims of IP infringement? What is there are force majeure events?
  - ✓ With respect to enterprise goals: What if the enterprise breaches this agreement? What if the enterprise's goals shift and it wants to exit the contract? What if pricing or terms are modified in a way that makes the services no longer viable for the enterprise?
- ✓ Engage in discussion early on for transition planning, and account for potential business disruptions; look for data backup and recovery plans.

Additional Pro Tips



8/24/2023

Key Questions During Contract Review

Identify Gaps	• Are there gaps in expectations? Is the enterprise able to do what it plans to do with these services? Do all stakeholders agree on the scope of use?
Identify Risks	• Are there specific risks given the industry of the enterprise? Given the proposed use? Given the types of users with access? Do the parties understand the contractual risk allocation?
Controls	• Can the enterprise negotiate for certain controls on the use of the data or for data protections? If not, can the enterprise employ internal controls?
Term	• Have the parties planned for a friendly, or unfriendly, breakup? A data breach? A force majeure event? How will data migration be handled? Refunds and payments?
Communication	• How often and using what methods will the parties communicate? Are there open lines between key stakeholders? Are there third parties, such as resellers or third-party providers, involved in the relationship?

Key Tips for Internal Controls



Identify what internal bridges and/ or additional services will be needed or desired to ensure the full scope of necessary services.



Develop a plan for educating the business units on what is and is not allowed under the contract.



Monitor and assess accuracy and quality of vendor's work product; train employees to identify and escalate issues with vendor, third-party, enterprise, and user compliance.



Review vendor attestations and certifications; monitor insurance coverages.



Do business units have up to date contact information or a means to connect with vendor? Is there an endgame plan in place?

Managing the Vendor Relationship

- ✓There is an internal and external component to managing the relationship.
- ✓The business lawyer adds value working with (and devising a strategy to work with) its internal clients and the vendor, as well as any other external stakeholders.
- ✓Prepare a unified voice among various units, e.g., internal accounting, IT, legal, and operations.
- ✓Prepare a road map to communicate with and handle any potential issues with the vendor; note that relationships with cloud vendors may need to be handled differently than relationships with other vendors.

Conclusion

The concepts and terms highlighted in this presentation illustrate that our business lawyer has an important role beyond negotiating and editing contract language. Cloud service agreements are complex in part because readers must jump from one document to another to get the full picture. Cloud services also anticipate an ongoing relationship with shared responsibilities.

Effective administration of cloud services is a multifaceted endeavor.

Feedback

This presentation was created as a project of the ABA Cloud & Enterprise Technology Subcommittee of the Cyberspace Law Committee.

The Subcommittee welcomes feedback on this presentation and other tools in the Cloud Computing and Cloud Marketplace Toolkit Project.

The Subcommittee also invites members of the Business Law Section to participate in this project (and other Cyberspace Law Committee activities). If there is a topic covered or mentioned in this toolkit that you would like to expand on, please reach out.