KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

cvent

In-House Counsel's Playbook for
Negotiating Cloud Contracts for SaaS, IaaS, and PaaS

Presented September 28, 2021

Speakers

Sonia Baldia

Partner
Kilpatrick Townsend

Edwin Szeto

VP & Deputy GC
Cvent, Inc.

Jeffrey Connell

Associate
Kilpatrick Townsend

Sonia Baldia brings business and technology savvy to her global practice, which encompasses U.S. and international commercial, transactional, and IP expertise. Sonia advises clients on a wide array of sourcing, technology, and other commercial transactions. She has been recognized by *Chambers USA*, *Legal 500*, and other leading publications for her technology and outsourcing expertise, including deals involving India. She is a frequent speaker and writer on global sourcing, digital transformation, IP, and technology topics.

Ed Szeto has over twenty years of technology contracts experience. As Vice President & Deputy General Counsel for Cvent, Inc., a leading SaaS provider of technology and services to the events and meetings industries, Ed leads the commercial legal team and is responsible for all contractual matters with Cvent customers and vendors. Prior to joining Cvent, Ed spent ten years with MICROS Systems, Inc., a provider of technology products to the hospitality and retail industries, until its acquisition by Oracle.

Jeff Connell focuses his practice on cybersecurity, data privacy, information technology, business outsourcing agreements, systems integration, software as a service (SaaS) transactions, technology licensing, and other technology and commercial transactions. Jeff also maintains an active pro bono practice and provides business legal services through the Pro Bono Partnership of Atlanta. His pro bono service has been recognized by the *Georgia Bar Journal*, which named him a Pro Bono All-Star.

Agenda

- Brief Overview of Saas, Paas, and Iaas
- Informed Tradeoffs
- Key Legal Issues in Cloud Contracts

KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

cvent

Brief Overview of SaaS, PaaS, and IaaS

Who's the expert?

Polling Question #1:

How much experience do you have with SaaS, IaaS, and PaaS?

a. None
b. Minimal
c. Moderate
d. I'm an expert!

Cloud Computing vs. Traditional Software Licensing

In a traditional software licensing engagement, the software is installed **on-premise** in the Customer's environment.

The Customer can have the software configured to meet its particular business needs and retains **control** over its data.

With Cloud, the software and the customer's data are **hosted by the Vendor**, often in a **shared environment** (i.e., many customers per server).

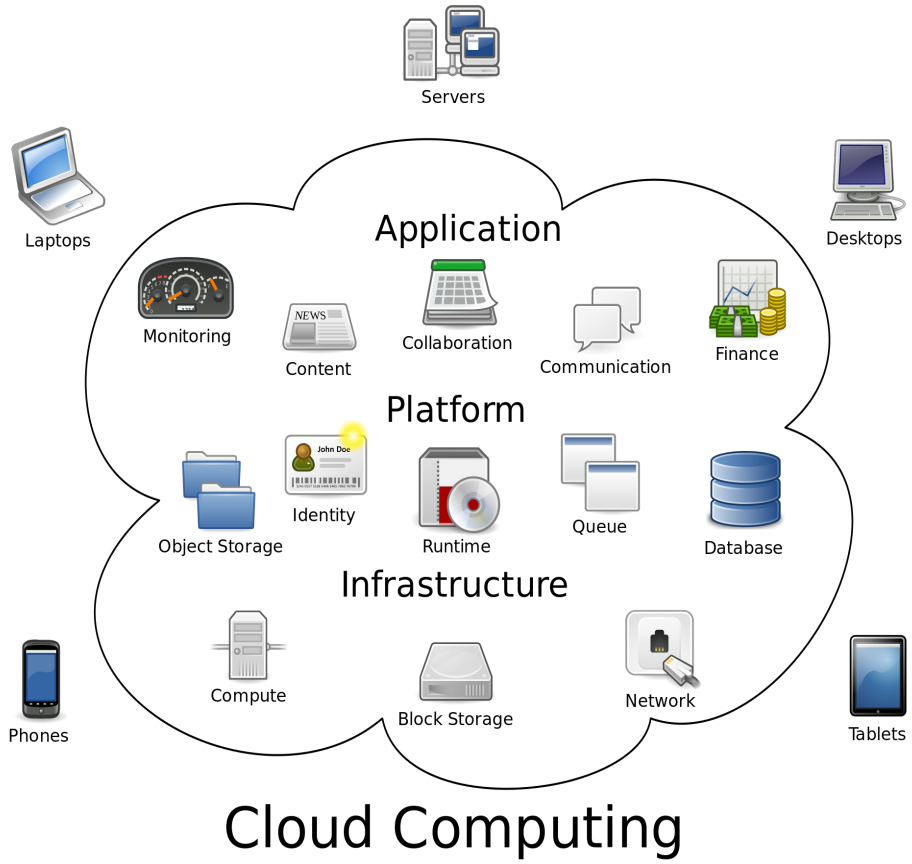
The software configuration is much more homogeneous across all customers in a "one to many" model.

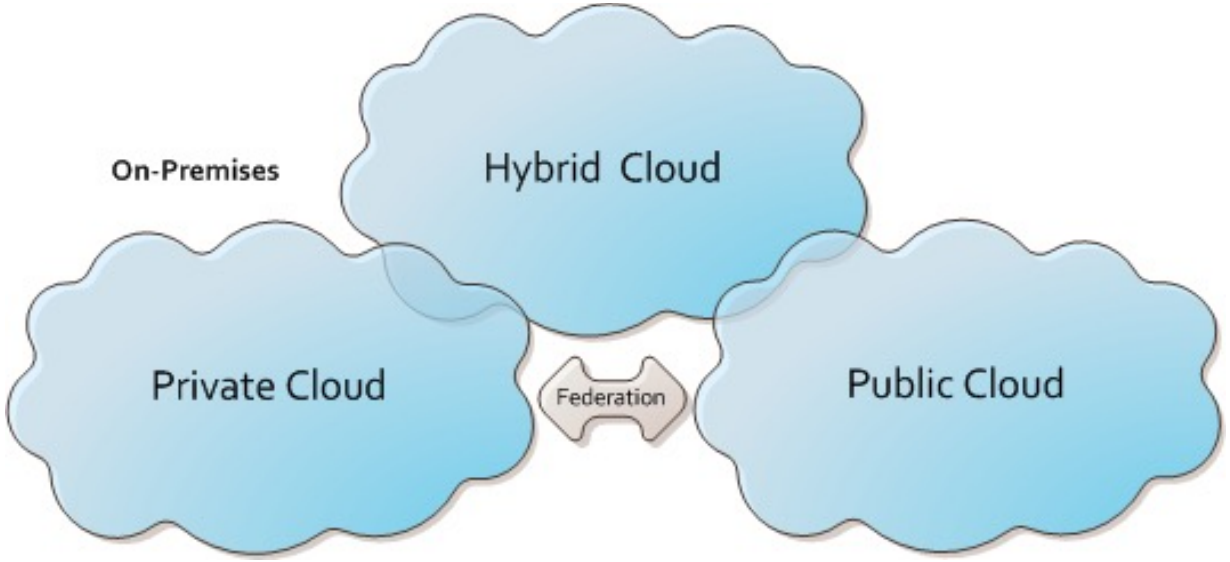
The Customer's top priorities shift from customer specific configuration and acceptance to service availability and data security. However, like a traditional software licensing agreement, provisions such as insurance, indemnity, intellectual property, limitations of liability, and warranties remain important.

On-Prem vs. Cloud – Risk-Benefit Analysis

Factor	On-Prem	Cloud
Ownership	You own the software, hardware, data and are 100% responsible for all upkeep	Vendor accountable for software, hardware, DR, innovation, you own data
Pricing	Upfront cost to license/purchase + annual maintenance fee (% of license fee)	No upfront investment Subscription - “Pay as you go” Maintenance is included
Accounting principle	Capital lease/asset	Operating lease/expense
Security & Control	Customer has greater and direct control over application and data Customer defines access permission and security protocols	Vendor or its third party hosts the application and your data No direct control over handling or control over your data
Customization & Flexibility	Customer has flexibility to customize and configure in house	Limitations to customizations that can be deployed in multi-tenant solution
Upgrades	Customer upgrades software itself on its schedule Customer maintains dedicated IT staff	Dependency on SLAs with vendor to ensure is upgraded
Innovation	12-18 months release cycle	Rapid innovation
Backup and Recovery	Customer bears all responsibility	Vendor manages

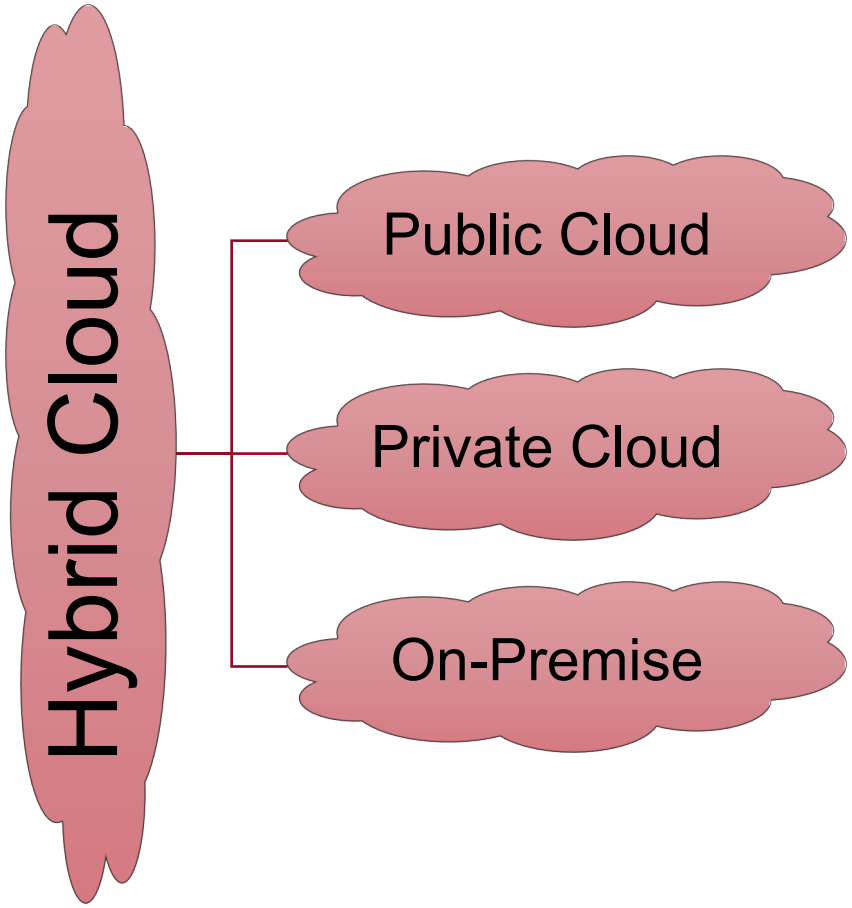
A Brief Overview of the Cloud



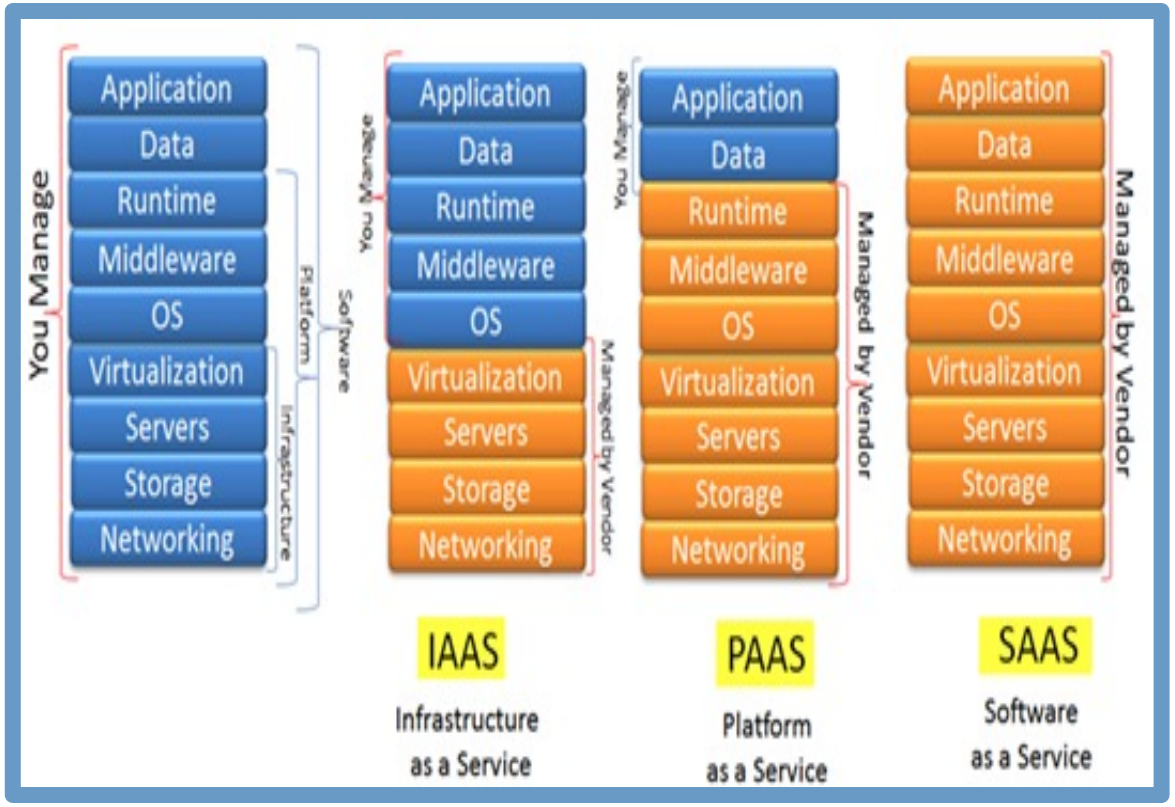


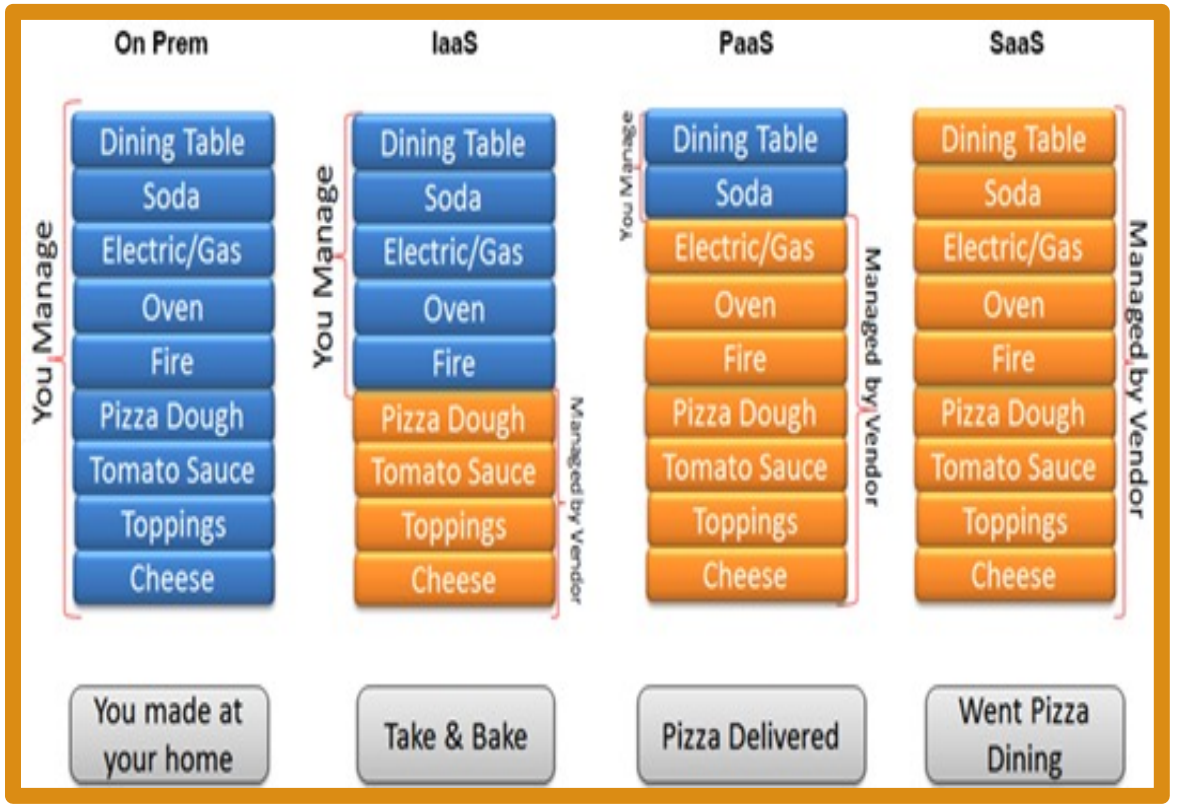
Deployment Models

- Public Cloud
  - Multi-tenant, massive scale, pay for use, multi-datacenter redundancy
- Private Cloud
  - Single tenant, may be hosted internally or externally by a third party; allows a greater degree of control of data and systems
- Hybrid Cloud
  - Use of public cloud, while keeping other IT-resources on-premise or in a private cloud



Cloud Delivery Models





Cloud Delivery Models

SaaS: Software as a Service	PaaS: Platform as a Service	IaaS: Infrastructure as a Service
Consumer uses provider's applications running on provider's cloud infrastructure	Consumer can create custom applications using programming tools supported by the provider and deploy them onto the provider's cloud infrastructure	Consumer can provision computing resources within provider's infrastructure upon which they can deploy and run arbitrary software, including OS and applications. Allows for dynamic scaling.
Google Docs, Google Gmail, Salesforce CRM, Facebook, Groupon, Oracle	AWS, Microsoft Azure, Spring Source, Google Cloud	AWS, Google Cloud, RackSpace, IBM, VMware

The SaaS Market: Facts and Trends

- Gartner Research predicts that the service-based cloud application industry will be worth **$143.7 billion** by 2022.
- Industry experts believe that investment and value in analytics-centric SaaS models will rise by **23.3%** by 2022.
- **Artificial intelligence** is positioned to disrupt the SaaS landscape in a variety of ways, improving the key characteristics of the SaaS model across the board.
- SaaS vendors are now providing greater **integration capabilities** instead of redirecting their customers to third parties.
- **White labeling** of SaaS solutions has become increasingly prominent.
- Enhanced **mobile optimization** is becoming a top priority.

Source: Business Wire

The IaaS Market: Facts and Trends

- The worldwide infrastructure as a service (IaaS) market grew **40.7%** in 2020 to total **$64.3 billion**, up from $45.7 billion in 2019, according to Gartner, Inc.
- The market is projected to reach **$201.83 billion** by 2027.
- In 2020, the top five IaaS providers accounted for **80%** of the market, and nearly 90% of all IaaS providers exhibited growth.
- IaaS **services** include detailed monitoring, log access, load balancing and clustering, security, and storage resiliency features, such as replication, backup, and recovery.
- Asia-Pacific (**China, Singapore, Japan, and Australia**) is an emerging region for vendors in the IaaS market.

Source: Business Wire

The PaaS Market: Facts and Trends

- The global platform as a service (PaaS) market is expected to grow from **$47.29 billion** in 2020 to **$54.09 billion** in 2021.
- The market is expected to reach **$88.11** billion in 2025.
- The rising need for advanced **integration services** and shifting of workload to cloud environments are also driving the demand for PaaS globally.
- The **COVID-19 pandemic** has contributed to the growth of the PaaS sector through a rise in demand for cloud-based business continuity software and services, a strong reliance on public cloud services to achieve near-term business goals, and increased spending on cloud services.

Source: Business Wire

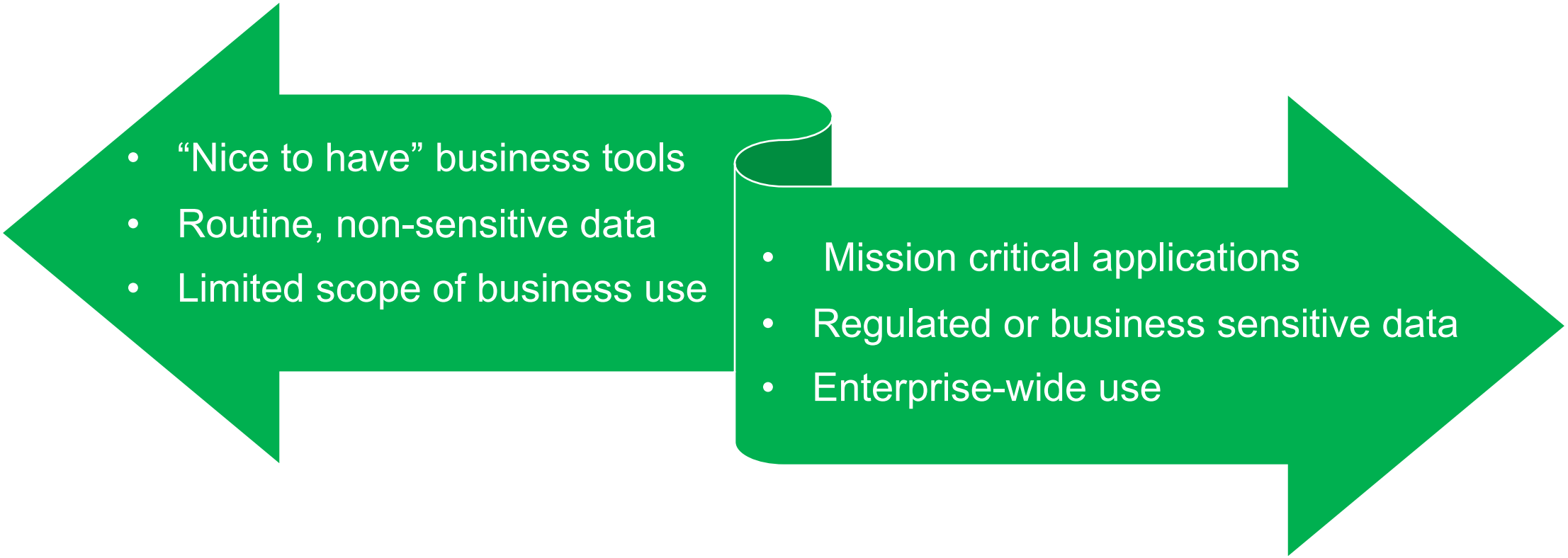
KILPATRICK TOWNSEND

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

cvent

Getting Started

Breadth of Cloud-Based Offerings



Each end of the spectrum presents different legal and contractual challenges, options, and trade-offs

Vendor vs. Customer Paper

- All cloud services agreements have a shared basic structure with key terms and provisions in common, which we will discuss today.
- However, each individual SaaS, PaaS, or IaaS agreement will have special requirements that depend on the particular product, services, and industry.
- SaaS Agreements are focused on the software and data that are hosted by the Vendor and accessed by Customer over the internet.
- PaaS Agreements enable the Customer to create its own SaaS applications that are then hosted, so the agreement is more technical to cover development, testing, and deployment environments.
- IaaS Agreements must also cover the physical equipment that a Customer outsources to the Vendor, which makes it more of an outsourcing arrangement.

Customers Must Make Informed Tradeoffs

- How critical is the cloud service?
- How confidential is the data?
- What service levels are being offered?
- Can the provider meet your company's expectations?
- What are the economics of the transaction?
- What is the relative bargaining position of the parties?
- Are other alternatives available?

Are There Any Legal Issues?

Polling Question #2:

In your opinion, what are the biggest issues relating to cloud contracts?

a. Service Levels
b. Warranties
c. Data Ownership
d. Data Security and Privacy
e. Indemnities and Liability
f. All of the above

KILPATRICK TOWNSEND

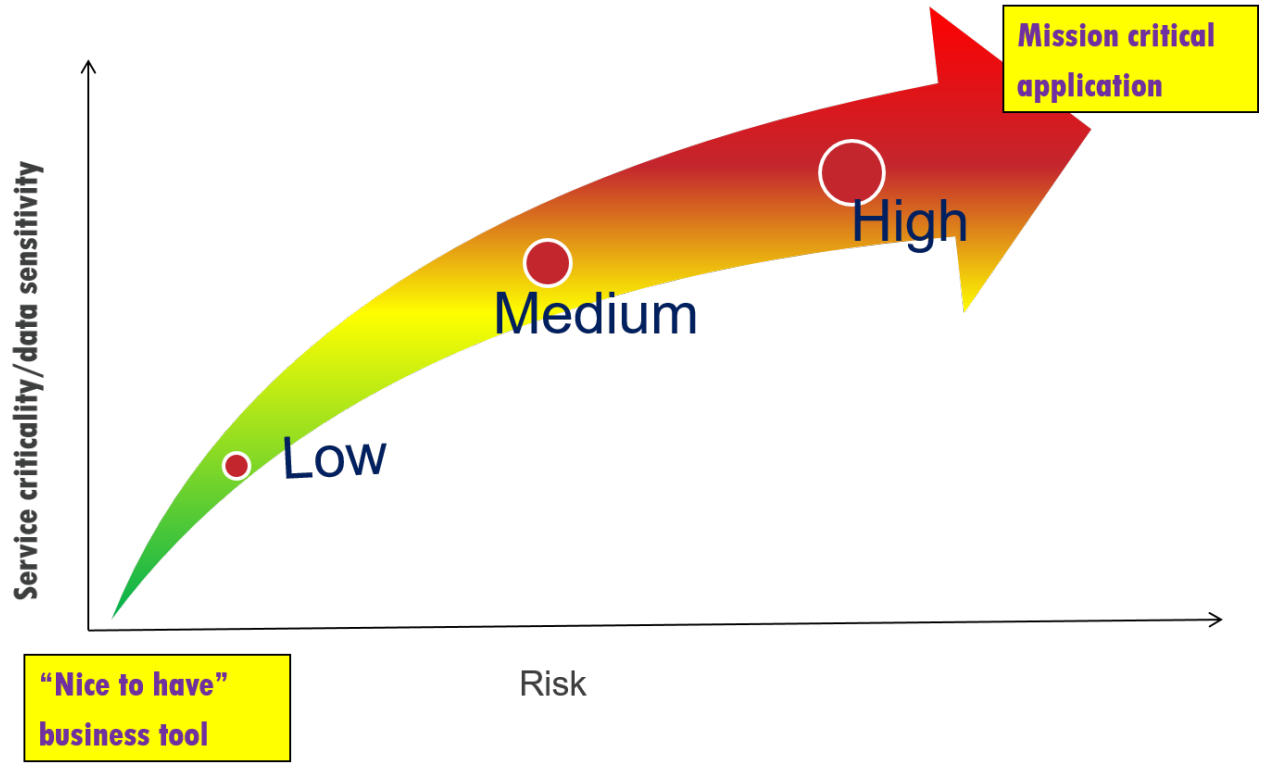
Key Areas

Key Areas:

1. **SLAs**
2. Warranties
3. Data Ownership
4. Data Access, Security, and Privacy
5. Indemnities
6. Limitation of Liability
7. Termination for Convenience

Service Levels

- Why have SLAs?
- What to measure?
- When to measure?
- Who will measure/report?



Customer Perspective

Service Levels

As a Customer, the definitions of "availability" and "outage" are critical. For example, availability should be tied to functionality, rather than access.

A Customer will want to make sure that there are not too many exclusions (such as emergency maintenance) from the definition of an outage.

Availability

Tendency for customers to want to customize availability metrics

Credits and Remedies

No sole and exclusive remedies, which effectively create a sub-cap on liability

Availability %	Downtime per year	Downtime per month	Downtime per day
90% ("one nine")	36.5 days	72 hours	2.4 hours
95%	18.25 days	36 hours	1.2 hours
97%	10.96 days	21.6 hours	43.2 minutes
99% ("two nines")	3.65 days	7.20 hours	14.4 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	1.44 minutes
99.99% ("four nines")	52.56 minutes	4.38 minutes	8.66 seconds
99.999% ("five nines")	5.26 minutes	25.9 seconds	864.3 milliseconds
99.9999999% ("nine nines")	31.5569 milliseconds	2.6297 milliseconds	0.0864 milliseconds

Vendor Perspective

Service Levels

As a Vendor, define “availability” as having access to the solution. Excluding *de minimus* outages from the calculation is also a way to minimize the impact. A long measurement period, for example, may hide some outages that a Customer would otherwise consider significant.

Availability

Stick to the set standard offered to all customers

Credits and Remedies

Streamline remedies and avoid dispute

Availability %	Downtime per year	Downtime per month	Downtime per day
90% ("one nine")	36.5 days	72 hours	2.4 hours
95%	18.25 days	36 hours	1.2 hours
97%	10.96 days	21.6 hours	43.2 minutes
99% ("two nines")	3.65 days	7.20 hours	14.4 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	1.44 minutes
99.99% ("four nines")	52.56 minutes	4.38 minutes	8.66 seconds
99.999% ("five nines")	5.26 minutes	25.9 seconds	864.3 milliseconds
99.9999999% ("nine nines")	31.5569 milliseconds	2.6297 milliseconds	0.0864 milliseconds

Service Levels

Common Landing Spot

- Compromise on increased credit amounts
- Set high standards for the Vendor through SL Termination Events

Practice Pointers

- Study the definitions and test formulas for unintended consequences
- Create the opportunity to either pursue credits or, instead, a damages claim

Key Areas:

1. SLAs
2. **Warranties**
3. Data Ownership
4. Data Access, Security, and Privacy
5. Indemnities
6. Limitation of Liability
7. Termination for Convenience

Show me the money.

Polling Question #3:

Have you had surprise charges when your technology provider did not deliver as expected?

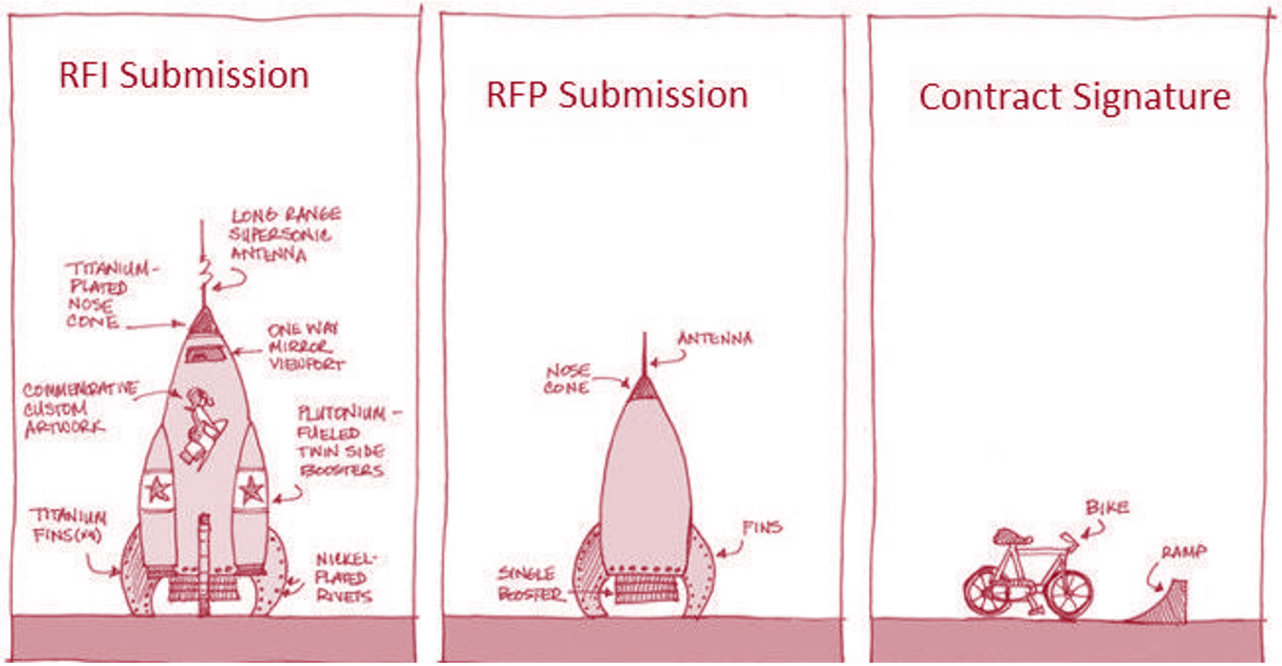
a. Yes

b. No

c. No, but they tried.

Performance Warranty

- Warranty that the Solution will perform in accordance with certain specifications
- Typically tied to Vendors standard service documentation
- Typical remedies for a Vendor's breach of this warranty are repair, replace, or refund for non-conforming item



Customer Perspective

Warranties

A Customer is looking for a strong performance warranty that requires the Solution to perform in accordance with certain specifications (material or not), that are usually tied to the Vendor's service documentation. These agreed specifications should not change over time. Finally, the warranty should set forth clear remedies in the event of a breach of warranty.

Compliance

The Vendor must strictly meet all requirements

Specifications

The Vendor cannot change without consent. Consider whether to attach the documentation to the agreement so that it is frozen in time.

Remedy

Repair! Replace! Refund! Avoid sole and exclusive remedies (a performance warranty remedy should not be used as limitation on breaches of other contractual provisions)

Vendor Perspective

Warranties

A Vendor wants the ability to make changes across its customer base, so a Vendor will seek flexibility to make unilateral changes.

A Vendor may not even initially offer a warranty. If a warranty is offered, a Vendor will limit the warranty as much as possible. A Vendor will often include multiple disclaimers to further disclaim express and implied warranties.

Compliance

Addition of a “materiality qualifier” to meet requirements (and include broad disclaimers)

Specifications

The Vendor may change specifications in its sole discretion and at any time

Remedy

The warranty is the Customer’s sole and exclusive remedy

Warranties

Common Landing Spot

- Specifications may change – but only so long as the change does not materially affect the solution and the Customer receives prior notification

  "The Service descriptions are available at www.example.com. Vendor may change or otherwise update the descriptions at its discretion; provided that no change will materially degrade the Service."

- A termination right for objectionable changes may provide additional options if a change will have an adverse effect on functionality

Practice Pointers

- Consider whether the termination right comes with a refund and consider whether additional amounts (such as migration costs) should be included

Other Warranties

- No virus or malicious code; No open source; Required third party consents; Compliance with laws; Non-infringement; Etc.

Key Areas:

1. SLAs
2. Warranties
3. **Data Ownership**
4. Data Access, Security, and Privacy
5. Indemnities
6. Limitation of Liability
7. Termination for Convenience

Data Ownership

- What is Customer Data and how should it be defined?
- Who retains ownership of the data that is stored, transmitted, and/or created with the solution?
- Does the Vendor want to reserve the right to use the Customer's data for the purposes of operating and improving the services?

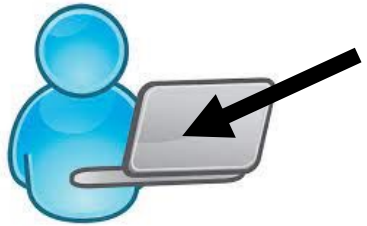
Data Ownership – Types of Data

Customer Input

- Data of customer and its users submitted or made available to the vendor

Derived Data Identifiable to Customer

- Original data that has been subject to a modification, enhancement, or other derivation, but from which the original data may be traced.
- E.g., certain analytics, insights, and reports

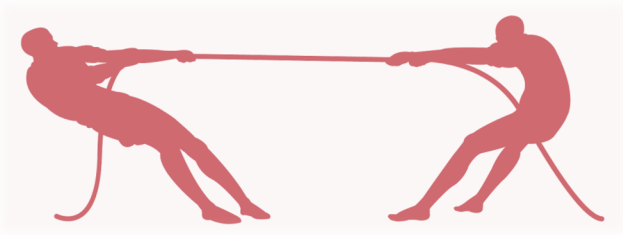


Derived Data Not Identifiable to Customer

- Aggregated or anonymized data sets where the original data is not identifiable
- Data regarding the vendor's network or performance of the solution

Customer Perspective

Data Ownership



From the Customer's perspective, a definition of Customer Data that is too narrow may not capture other data that is derived from the use of the solution but that contains sensitive and critical information.

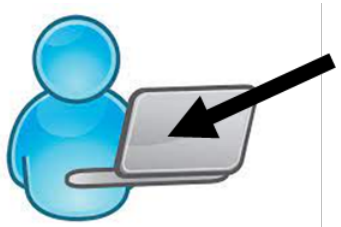
Customer Data

Own more than just input; own any data generated by use and output

Customer Data Definition

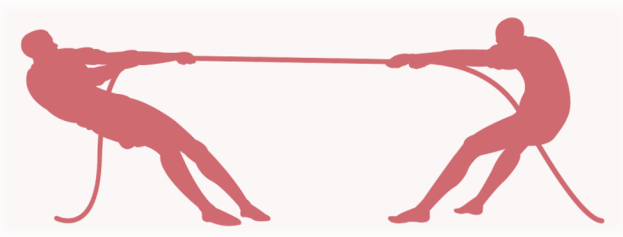
"means any data that Customer or its Authorized Users enter into the Service"

"means all data and/or information provided or submitted by or on behalf of Customer, all data and/or information stored, recorded, processed, created, derived or generated by the Vendor as a result of and/or as part of the Service, regardless of whether considered Confidential Information"



Vendor Perspective

Data Ownership



A Vendor, however, may find it operationally difficult to provide a broad definition of Customer Data. Moreover, a Vendor often relies on data generated within the Solution for its own internal business purposes.

Customer Data

Whatever the Customer puts in, the Customer owns

Aggregated Data

Include aggregated data provisions giving ownership/broad license rights to the Vendor with respect to aggregated/anonymized data

✓ "Baked into the cost"

Data Ownership

Common Landing Spot

- Create a definition that picks up data submitted to vendor and customer specific data that is generated using the solution (e.g., reports, analytics run by the tool)
- Inclusion of an aggregated data provision, but with limitations (e.g., responsibility for compliance with Privacy Law and an indemnity to Customer for use of the aggregated data maybe included)

Practice Pointers

- Clearly define the types of data
- Consider whether the data identifies the Customer, can be used to identify the Customer, or if it is capable of being re-identified
- Include contractual controls that outline permitted use and prohibited use
- Provide for the return or destruction of data

Key Areas:

1. SLAs
2. Warranties
3. Data Ownership
4. **Data Access, Security, and Privacy**
5. Indemnities
6. Limitation of Liability
7. Termination for Convenience

Data Issues

- Data transfer issues (EU and similar jurisdictions)
- Data location issues
- Location of users accessing data
- Movement and storage of data
- Use of subcontractors
- Use of multiple platforms
- Lack of transparency and control
- Data breach issues
- Data destruction issues
- Ability to impose security and privacy requirements
- Compliance with privacy laws

Customer Perspective

Data Security

A Customer wants to ensure the Provider safeguards the security and confidentiality of customer data are critical in any technology agreement. The Provider should deliver details regarding, and agree to reasonable provisions addressing, its competency and its policies and procedures related to protection against security vulnerabilities, data backups, the use of customer data, and data conversion.

Data Breaches

A Provider should have strict liability for data breaches

Vendor Perspective

Data Security

A Provider should be responsible solely for their actions. In other words, it is important to limit liability for any third party actions over which the vendor has no control, such as a malicious hacker. A Provider will agree to reasonable controls commensurate with the data it agrees to handle. Moreover, it is necessary to cap liability at an amount that reflects a Provider's risk to reward.

Data Breaches

A Provider shouldn't be an insurance policy

Data Security

Market Landing Spot

- Robust security programs are the first line of defense
- To the extent an employee absconds with data, that's covered. But a Provider's responsibilities are primarily contained within maintaining its security program.

Practice Pointers

- Be aware of Customer specific obligations that may be used to limit/reduce Vendor liability (i.e., encryption)
- Have a breach response in place
- Consider data locations (U.S. vs. foreign)

It’s my right!

Polling Question #4:

Does your company exercise its audit rights?

a. Never

b. Only if there is a problem

c. Regularly

d. I have no clue!

Security Audits

	SOC 1	SOC 2	SOC 3
Standards	SSAE 16	AT 101, AICPA Guide "Reporting on Controls at Service Organizations"	AT 101, AICPA Trust Service Principles, Criteria, and Illustrations
Subject Matter	Controls over financial reporting	Controls relevant to security, availability, processing integrity confidentiality, or privacy	Controls relevant to security, availability, processing integrity confidentiality, or privacy
Report's Intended Recipients	Management, auditors of financial statements, and customers	Parties knowledgeable about nature of the services, system interactions, and internal controls	Anyone

Data Access, Security, and Privacy – Checklist

When reviewing or negotiating provisions regarding the access, security and confidentiality of your data consider the following:

- ❑ Does the system prevent unauthorized access, use, alteration, or destruction of your data?
- ❑ Is your data secure during procedures of transfer into and out of the system?
- ❑ Does the Provider have a confidentiality policy in regards to its employees, partners, and subcontractors?
- ❑ Does the Provider use the services of a subcontractor?
- ❑ Does the Provider offer information about the identity of the subcontractor and its tasks?
- ❑ Are subcontractors held to the same level of legal obligations as the Provider of the cloud service?
- ❑ Is the Provider responsible for data retention and backup?
- ❑ Are Provider systems and practices compliant with applicable privacy laws?

Key Areas:

1. SLAs
2. Warranties
3. Data Ownership
4. Data Access, Security, and Privacy
5. **Indemnities**
6. Limitation of Liability
7. Termination for Convenience

Indemnities

- Enabling Clause

"Defend and pay"	The duty to defend and pay only requires the indemnitor to pay for defense costs and any resulting judgments awarded to a third party or settlements
Full indemnity (i.e., "defend, indemnify, and hold harmless")	Generally speaking, a full indemnity is intended to broadly make the indemnitee whole; covers more damages than payment of judgments or settlements

- Trigger: Third party claims vs. direct claims

Customer Perspective

Indemnities

A Customer seeks an enabling clause that includes a **full indemnity** (i.e., “defend, indemnify, and hold harmless”).

Moreover, a Customer will want to ensure that it is able to recover for **first party damages** in addition to third party damages.

Finally, a Customer will include a series of indemnity events, including for confidentiality, privacy, non-infringement, personal injury and property damage, violation of law, and gross negligence.

Scope

Broad indemnity to cover any and all damages, losses and liabilities

Scope

Triggered by a direct indemnity claim

At a minimum, covers both first party and third party damages

Vendor Perspective

Indemnities

A Vendor seeks to limit indemnity obligations to "**defend and pay**" so that the Vendor is only responsible for amounts finally awarded by a court or an approved settlement with the obligation only triggered by third party claims.

A Vendor seeks to limit its indemnity obligations to a **narrow list of occurrences**, such non-infringement and will include exclusions.

Scope

Limited indemnity to defend and pay

Practical Exercise

Indemnities

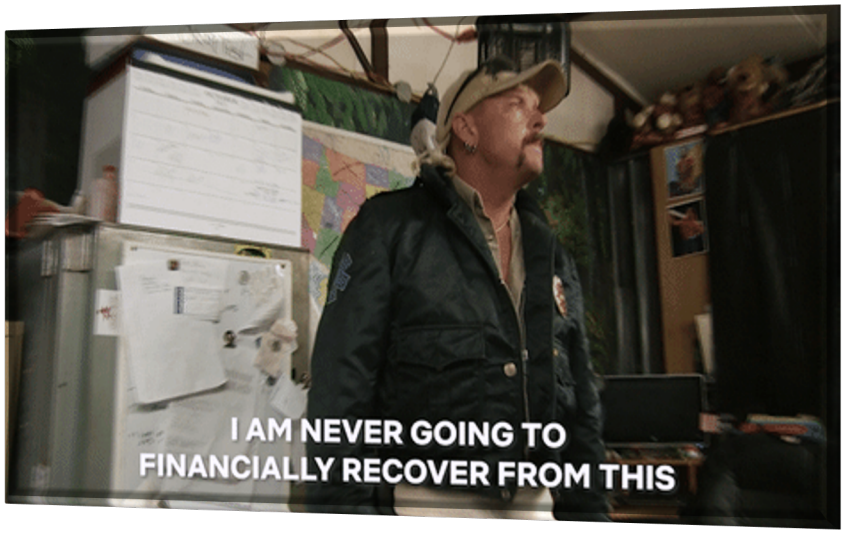
Duty to indemnify vs. duty to defend and pay

Is a “defend and pay” sufficient to cover all damages associated with:

1. Breach of confidentiality or security issue?
   No – Notice related costs

2. Data privacy violation?
   Probably not – Fines and penalties

3. IP Infringement?
   Maybe – if additional infringement indemnity provides for refund



Indemnities

Common Landing Spot

- Indemnities are typically limited to a **3rd party claims trigger**, although full indemnity vs. defend and pay is still somewhat of a toss-up
- Depending on the Vendor's risk tolerance, Vendors offer **IP-infringement** at a minimum, but others may include:
  - personal injury if its damage to *tangible* property or bodily damage (would not be strictly acts, likely tied to negligence or higher standard)
  - breach of confidentiality and data security, if tied to a SuperCap (*more on this later*)
  - breach of legal compliance (may be tied to a SuperCap)

Practice Pointers

- Even though an indemnity may be triggered by 3rd party claims, a broad definition of "Losses" can include first party damages
- Watch out for exclusions to IP infringement indemnity that could undo protection (such as integration with 3rd party systems)

IP Indemnity
- Should it be capped?
- Only third party claims?

Key Areas:

1. SLAs
2. Warranties
3. Data Ownership
4. Data Access, Security, and Privacy
5. Indemnities
6. **Limitation of Liability**
7. Termination for Convenience

Consequential or Direct?

Polling Question #5:

Would you consider costs to perform a workaround in the event of a failure to perform, costs to correct damaged data, and notice related costs direct damages? Are you willing to exclude these liabilities?

a. Yes, and they should be excluded.

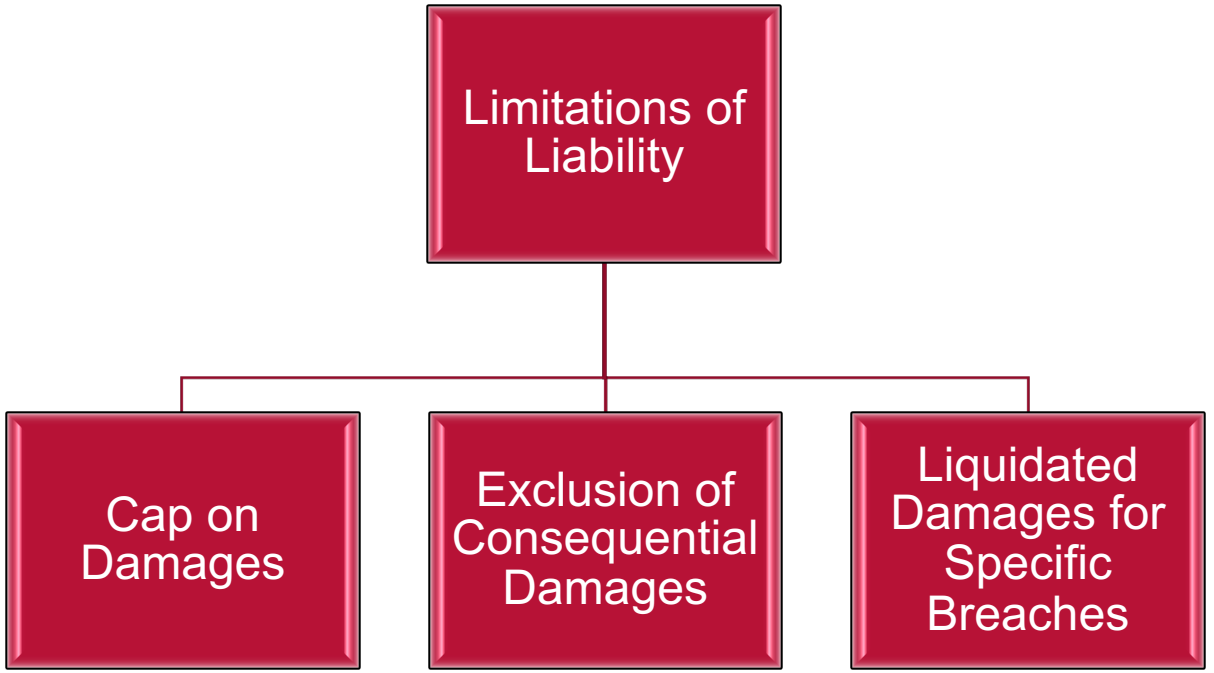
b. Yes, and they should not be excluded.

c. No, and they should be excluded.

d. No, and they should not be excluded.

Limitation of Liability

- Damages Cap
  - Aggregate Cap vs. Per Order/SOW vs. Fees for Deficient Services
- Consequential Damages Waiver
  - Are potential damages more likely direct or consequential?
  - Does prohibiting consequentials effectively exclude ability to recover meaningful damages?
- Exclusions from Limitations
  - Full exclusions from the damages cap (i.e., unlimited liability) vs. Super-caps



Customer Perspective

Limitation of Liability

A Customer wants to maximize potential for recovery of damages and, therefore, include **all amounts paid or payable** into the calculation – whether or not under the same order/SOW – **and a dollar amount floor**

Exclusions should be applied to **both** the **damages cap** and the **consequential damages waiver**.

Exclusions

Include exclusions that capture the losses that may happen from an economic perspective

- Such as: breach of confidentiality, data security, indemnification, violations of applicable law, personal injury, property damage, intellectual property infringement, fraud, gross negligence, willful misconduct

Damages Cap

Aggregate fees paid or payable

Dollar amount floor

Vendor Perspective

Limitation of Liability

A Vendor will attempt to limit the overall damages cap as much as possible, often times through **services-specific caps**.

Vendors want to limit exclusions from the limitations of liability – the “not an insurance provider” argument exclusions.

Vendors may start with limited exclusions, such as for IP infringement indemnity and bad acts (fraud/gross negligence), but will attempt to only carve out from the damages cap.

Exclusions

Consequential damages should be excluded

Damages Cap

Limited to amount of fees paid for the services under a particular order OR fees for the deficient services

No dollar amount floor

Limitation of Liability

Common Landing Spot

- Damages caps are often set at 12 prior months fees
- Full exclusions from limitations of liability are negotiable and vary by vendor tolerance
- Super Caps for certain breaches such as data security are now market and vary drastically in amounts (i.e., a set amount, or 2x or 3x the general cap)

Practice Pointers

- Do carve-outs apply to both the damages cap and the consequential waiver?
- What are “direct damages”? Consider including a definition for acknowledged direct damages.
- Is it clear that amounts paid under a carve-out or super-cap do not erode the general damages cap?

Key Areas:

1. SLAs
2. Warranties
3. Data Ownership
4. Data Access, Security, and Privacy
5. Indemnities
6. Limitation of Liability
7. **Termination for Convenience**

I'll be back.

Polling Question #6:

Have you been stuck in a contract when you did not have the termination rights you needed?

a. Yes. It was terrible.

b. No. I am the Terminator

Termination for Convenience

- Allows one or both parties to terminate the contract at any time for any or no reason
- Relative negotiating power
- Pricing and Termination Fees
- Other Termination Rights

Customer Perspective

Termination

A Customer prefers a **unilateral** right to terminate for convenience at any time. At the same time, a Customer does not want the Vendor to have this ability, which could leave the Customer stranded without services.

The Customer does not want to pay any termination fees and wants to receive a **refund of any prepaid fees** for services not received.

Termination

Any time, for any reason by only Customer (no termination right for the Vendor)

Fees

Refunds and no additional fees

Vendor Perspective

Termination

A Vendor does not want the Customer to have the ability to walk away for convenience other than **for cause** in the event the Vendor breaches the agreement.

The Vendor has made **pricing assumptions** based on the term of the contract.

Any termination for convenience will be subject to termination fees equal to remaining contract value.

Termination

For cause only

Fees

No refunds, termination fees

Termination for Convenience

Common Landing Spot

- If the agreement includes the right to terminate for convenience, there will likely be some sort of termination fee and **no right of refund**
- A termination for convenience will often come with a price increase or **loss of discounts**

Practice Pointers

- Rather than a termination for convenience, parties can negotiate shorter terms (i.e., one year renewals)
- However, the amount of termination fees can sometimes be negotiated (i.e., decreased percentage of fees in out years)

Questions?

Sonia Baldia

Partner
Kilpatrick Townsend

+1 202.508.5840

sbaldia@kilpatricktownsend.com

Edwin Y. Szeto

Vice President & Deputy General Counsel
Cvent, Inc.

+1 571.765.5699

ESzeto@cvent.com

Jeffrey Connell

Associate
Kilpatrick Townsend

+1 404.541.6822

Jeff.Connell@kilpatricktownsend.com

Locations

Counsel to innovative companies and brands around the world

We help leaders create, expand, and protect the value of their companies and most prized assets by bringing an equal balance of business acumen, technical skill, and creative thinking to the opportunities and challenges they face.

Anchorage
Atlanta
Augusta
Beijing
Charlotte
Dallas
Denver
Houston
Los Angeles
New York
Raleigh
San Diego
San Francisco
Seattle
Shanghai
Silicon Valley
Stockholm
Tokyo
Walnut Creek
Washington DC
Winston-Salem