Strafford

Presenting a live 90-minute webinar with interactive Q&A

On-Premise Software Licensing vs. Cloud Computing Contracts: Advantages and Disadvantages

Perpetual Licenses vs. Term Subscriptions, Rights in Deliverables, Data Management vs. Access, IP Indemnity, Escrow, Amendments

TUESDAY, OCTOBER 19, 2021

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Benjamin B. Kabak, Attorney, **Loeb & Loeb**, New York

Michael R. Overly, Partner, **Foley & Lardner**, Los Angeles

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1.**

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

Recording our programs is not permitted. However, today's participants can order a recorded version of this event at a special attendee price. Please call Customer Service at 800-926-7926 ext.1 or visit Strafford's website at www.straffordpub.com.

FOLEY

FOLEY & LARDNER LLP

On-Premise Software Licensing vs. Cloud Computing Contracts: Advantages and Disadvantages

Michael R. Overly, Esq., CISA, CISSP, COP, CIPP, ISSMP, CRISC

October 19, 2021

Agenda

- Potential Advantages
- Recent adverse trends
- The Big Four: Trial, Acceptance, Warranty, Support
  - Know how to explain to vendors
- Other Key Concerns

Potential Advantages

- Control of your own destiny
- Maintenance of institutional knowledge
- Better compliance
- BCP/DR

Recent Adverse Trends - General

- "Contract float"
  - Documentation
  - Support
  - Security/privacy
  - Service levels
  - Third party terms – open source/proprietary software

Recent Adverse Trends - General

- "Contract float" – Mitigating risk
  - Don't go negative
  - Lock as exhibit
  - Can't discriminate
  - Termination rights (but what about go-live fees?)

Recent Adverse Trends - General

- Liability and performance
- The dawn of the as-is technology agreement
- Disowning subcontractors
- Contract Balkanization:
  - License Agreement
  - Support Agreement
  - Professional Service Agreement

Risk Mitigation

- Diligence
- Maintaining negotiating leverage
- Use of process tools (e.g., RFP/RFI)
- Post-contract policing

The Big Four

The Big Four

- **Trial**
  - Best way to undermine leverage
  - Test environment/unimplemented
  - Remedy: termination
- **Acceptance**
  - Implemented/Ready for Production
  - Structured approach
  - Remedies: remediate, terminate, refund

The Big Four, cont'd

- **Warranty**
  - Time limited (compare cloud)
  - Cure, termination, potential litigation
- **Support**
  - Kicks-in after warranty period expires
  - Goals, targets
  - Remedies limited
  - SLAs difficult

Other Key Concerns

License Grant

- Key term in any license agreement
- Types of licenses:
  - Enterprise
  - Named user, concurrent user
  - Location
  - Hardware specific (Server ID)
  - What about your own customers?
- In general, the broadest license is preferred

License Grant

- Focus on who is the “licensee”
- Definition of “Licensed Software,” include updates, bug fixes, etc.
- Use of outsourcers and contractors
- Transferability
- Use in backup, disaster recovery, testing environments

Intellectual Property Ownership

- Mixed IP environment
- Types of intellectual property at issue:
  - Vendor pre-existing (background) intellectual property
  - Customer pre-existing intellectual property
  - Intellectual property developed during the engagement
  - Third party intellectual property
    - Commercially licensed intellectual property
    - Open source software
    - Freeware

Audit Rights

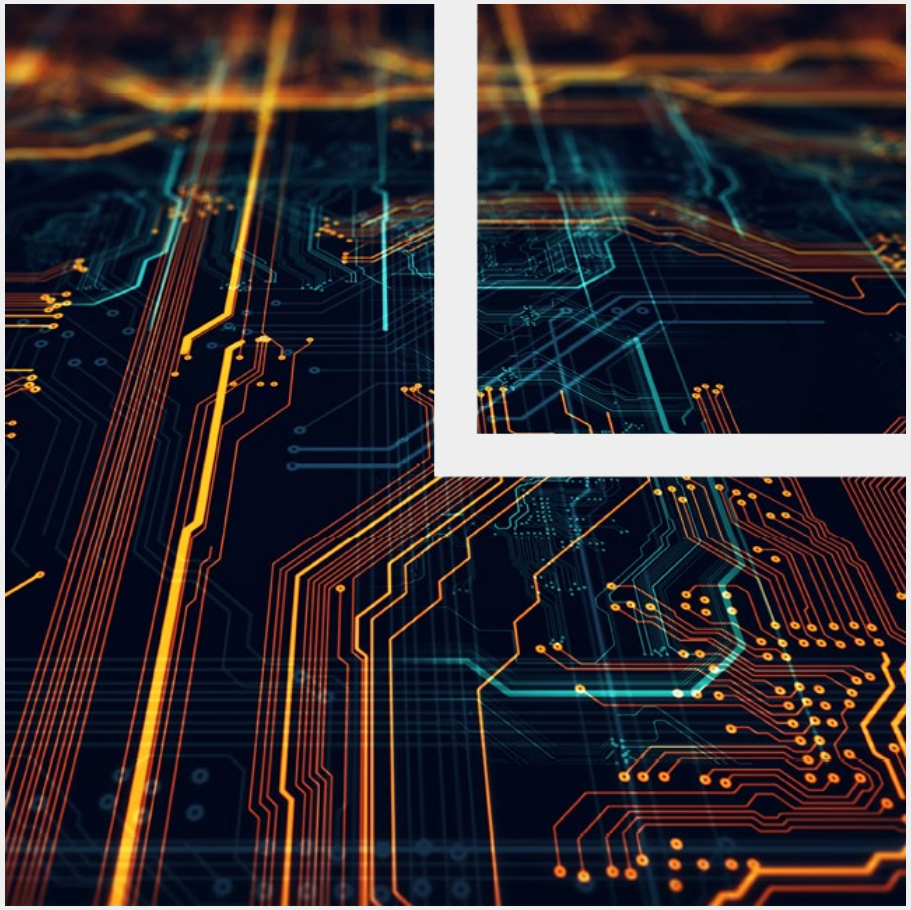
- Customer-Oriented: confirm fees and expenses, compliance with regulatory requirements, information security, etc.
- Vendor-Oriented:
  - Avoid broad, undefined audit rights
  - Preference is to reject on-site and remote access rights in favor of documentation
  - Limit use of third party auditors and their fees
  - Audit rights are not a fishing expedition.

Thank You

FOLEY

FOLEY & LARDNER LLP

On-Premise Software Licensing vs. Cloud Computing Contracts: Advantages and Disadvantages



Benjamin Kabak
Associate, Tech & Sourcing
Loeb & Loeb LLP

Oct. 19, 2021

We're all connected.

LOEB & LOEB LLP

LOS ANGELES
NEW YORK
CHICAGO
NASHVILLE
WASHINGTON, DC
SAN FRANCISCO
BEIJING
HONG KONG

loeb.com

The opinions expressed in this document do not necessarily reflect the views of Loeb & Loeb LLP, its clients or the presenters. This document was created for purposes of teaching and commentary, and should not be posted to the Internet, or otherwise used for any commercial purposes, without prior written approval from Loeb & Loeb LLP. The information in this document is not intended to be and should not be taken as legal advice.

Here's a look at the key findings that stood out.

SaaS adoption continues to explode.

In a year like none other, organizations have embraced SaaS faster than ever before. Up from an average of 80 apps last year, this year organizations use **110**, for a **38%** increase. This is nearly a **7x** increase in SaaS app usage since 2017, and almost a **14x** increase since 2015.

2020 **80 APPS** → 2021 **110 APPS**

More SaaS brings more challenges.

More than half (55%) of respondents say the most crucial challenge to solve is

lack of visibility

into user activity and data. The next two biggest challenges? Knowing all SaaS apps in use and consistently managing app configurations.

Levels of SaaSOps automation will nearly double in the next 3 years.

SaaS-Powered Workplaces report that

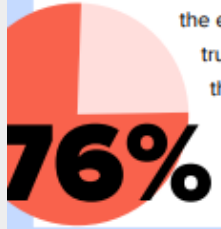
45% **of their SaaS operations is already automated**

and estimate it will rise to nearly

80% **within the next three years.**

In response to the past year, IT's role is becoming more strategic.

This past year, IT's role shifted from functional to strategic. They're solving challenges with SaaS, transforming the employee experience, and becoming trusted business partners—ultimately leading the way to tomorrow's workplace.



76% **of respondents report being more or much more strategic over the last 12 months.**

The well-meaning but negligent employee poses the biggest data loss threat—by far.

72% **of organizations say it's the well-meaning employee**

When it comes to data loss, the biggest threat is not from hackers or saboteurs. Instead, **72%** of organizations say it's the everyday employee who has good intentions and is just trying to do their job, but may inadvertently expose sensitive information along the way.

The SaaSOps role is here to stay.

60% of respondents already use the term "SaaSOps" in their job title/description or plan to include it in the future—**a 100% increase from last year.**

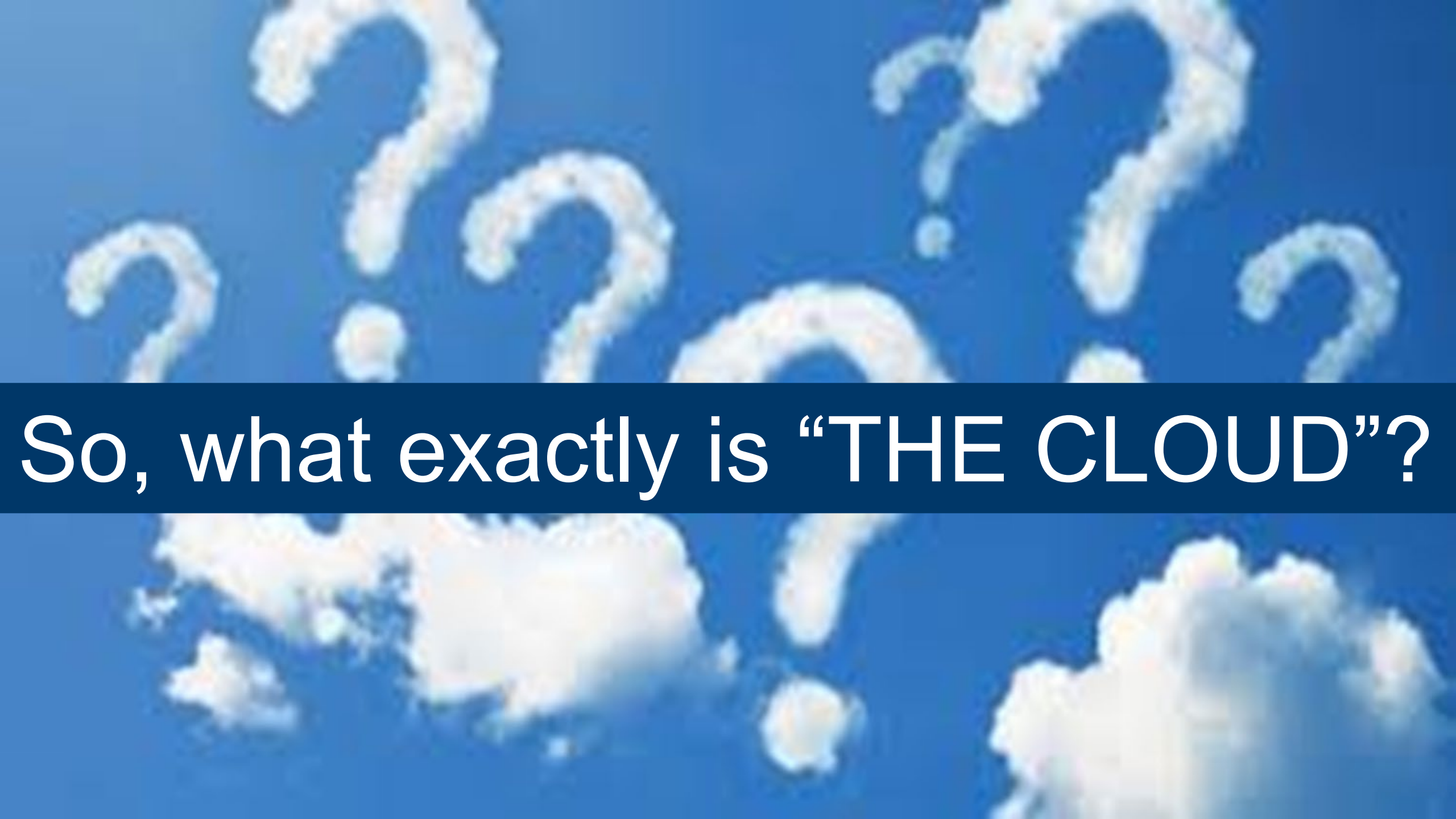
SaaS creates new security concerns for IT.

Lack of visibility is a pervasive challenge: 55% of respondents say their biggest security concern is not knowing where sensitive data exists.

69% of IT professionals are concerned about unsanctioned SaaS apps creating security issues. Additionally, **46%** say they have difficulties securing user activities within SaaS apps. This year SaaS file security violations have spiked **134%**, and the number of files containing PII has grown **1944%** year over year.

The future of SaaSOps is now.

When asked about the future of SaaSOps, more than **40%** of respondents wrote that it's "mission critical" or "essential in IT."


So, what exactly is “THE CLOUD”?

NIST Definition:

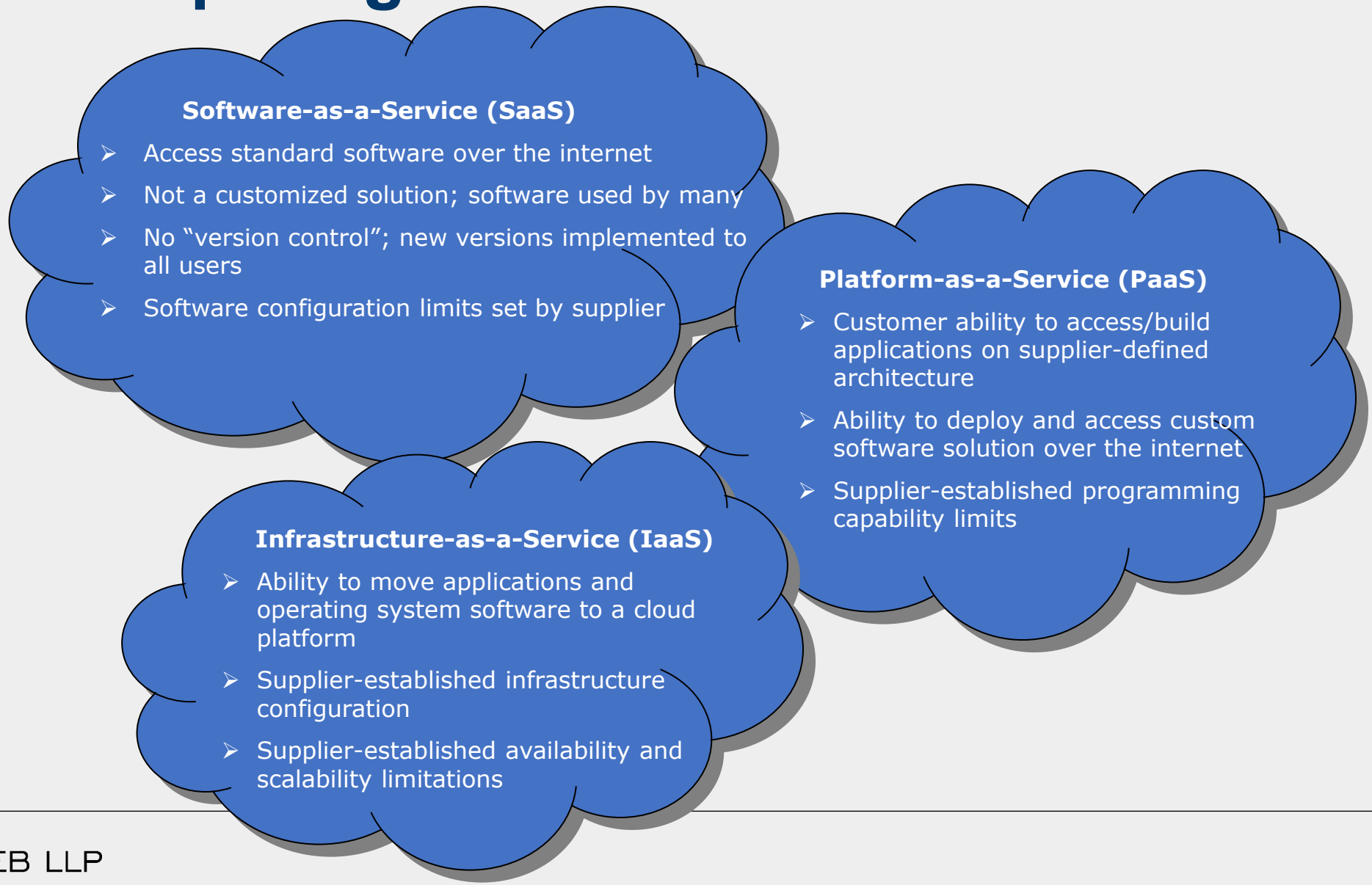
"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

In other words … the benefits of the Cloud

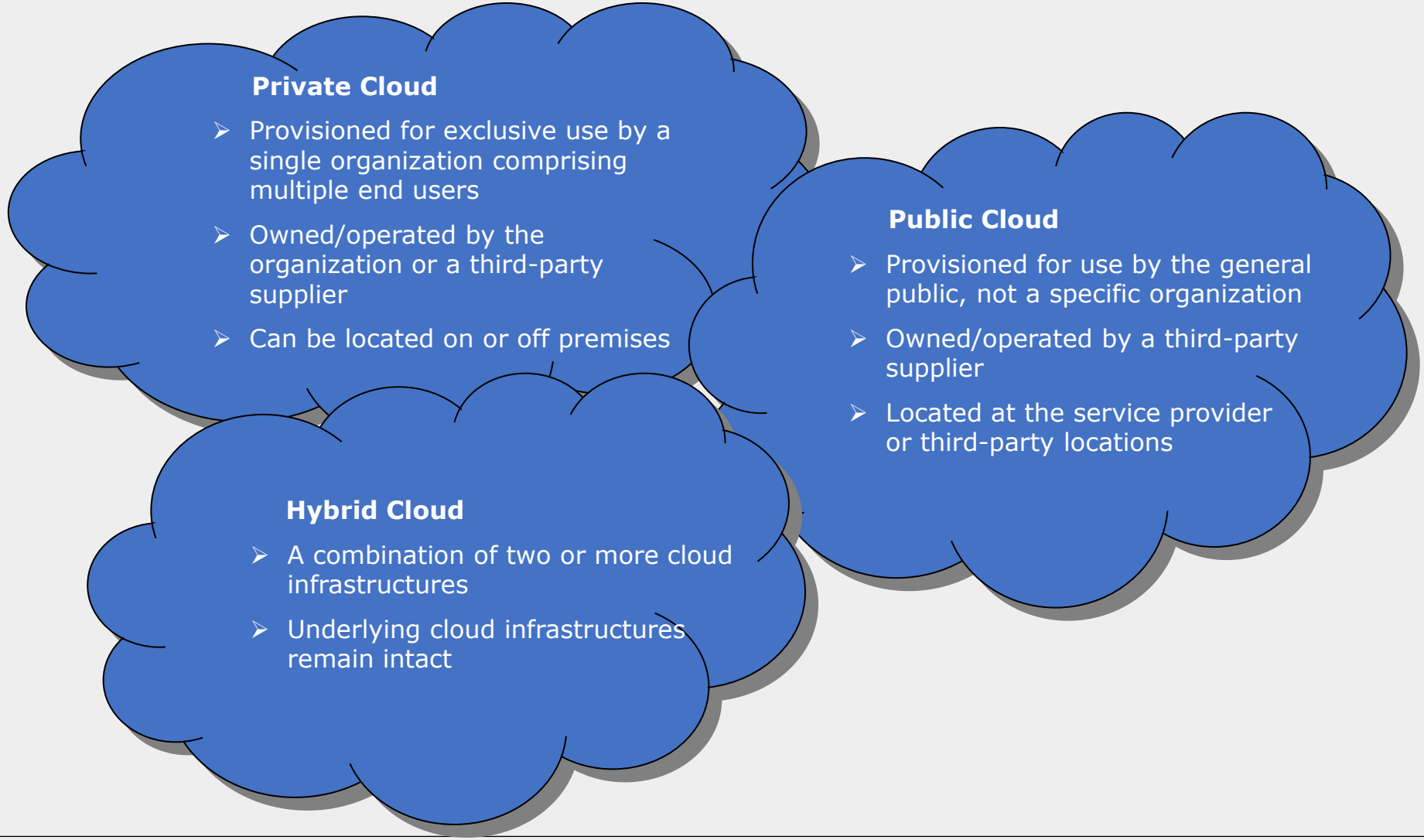
Cloud

- ✓Enables ability to work remotely
- ✓Offers utility billing (pay as you use)
- ✓Has vast capacity
- ✓Reduces cost
- ✓Has the elasticity to scale up or down
- ✓Speeds innovation

Cloud Computing Models



Key Cloud Terminology



Why does this Cloudspeak matter?

The particular cloud model drives key issues that both parties need to address

- Data ownership, privacy and security
- Business continuity and disaster recovery
- Risk profile/liability
- Other key cloud contract terms

How Are Cloud Contracts Structured?

- Order forms
- Subscription Agreements
- Service-level agreements (SLAs)
- Specify uptime and the credits given for downtime
- Data processing agreements (DPAs)
- Clickwraps
- Linked terms
- Pass-through terms

The Cloud Contracting Quandary: Enterprise Risk v. Commodity Transaction

The "enterprise" customer:

- ✓ Negotiates the transaction to address its own risk profile
- ✓ Uses the transaction to maintain a competitive advantage
- ✓ Maintains "control" over the services

The cloud computing supplier:

- ✓ Standardizes its own risk profile/contract terms
- ✓ Standardizes the services across its customer base
- ✓ Needs to distinguish cloud from Application Service Provider (ASP) and IT Outsourcing Services

All business and legal issues are implicated

Key Risk Issues:
Software Deployment and Control

Acceptance Testing, Updates and Version Control

- Benefit of the Cloud: Someone else is in charge of updating the software
- Customer wants rights to:
  - Acceptance-test new versions
  - Determine cadence of updates
  - Retain support on older versions
- Suppliers wants one unified solution for all its clients
- Contractual assurances
  - Retain features and functionality
  - Maintain backwards compatability

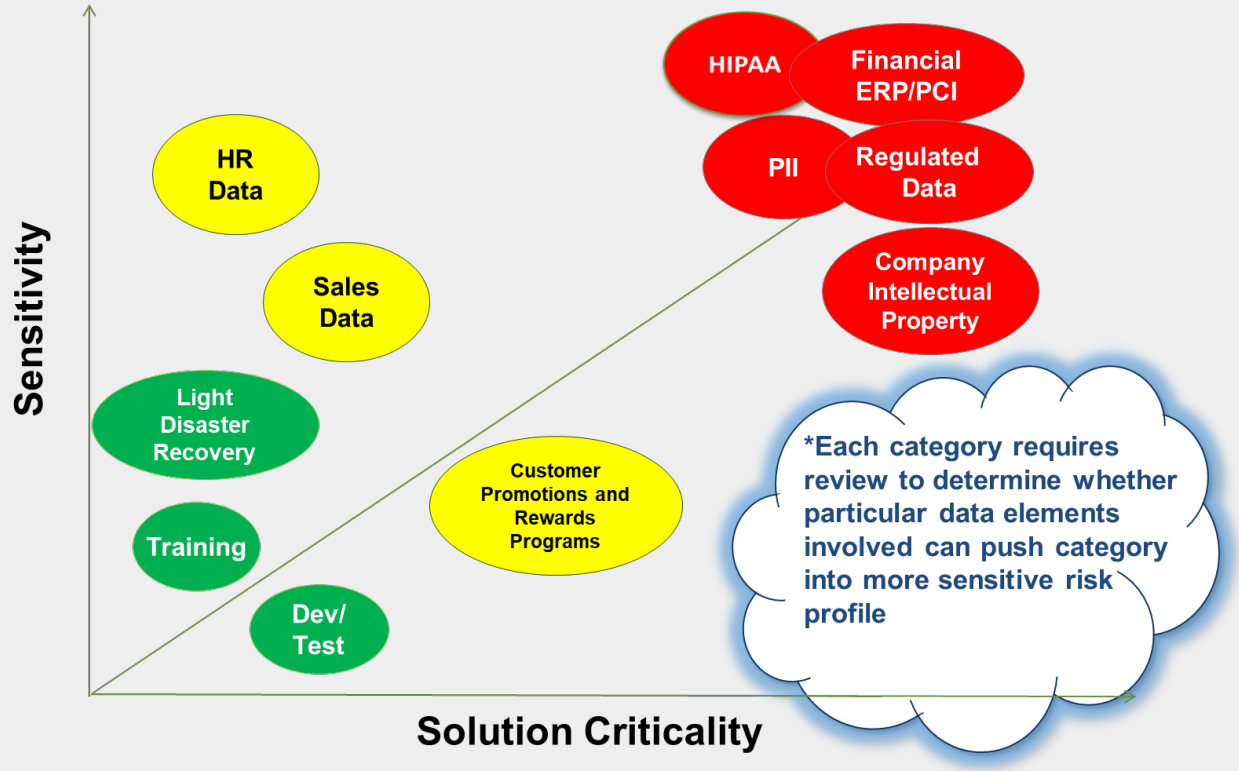
Key Risk Issues:
Data Ownership, Privacy and Security

Different Types of Data and Implications

- Differing Data Types
- Transactions data
- Regulated data (PII, PHI, PCI, etc.)
- Corporate proprietary data

Key is understanding the data and solution-specific concerns

- **PRO TIP:** The risk profile is very different between a product that has access to personal data vs. a product that does not



Data Ownership and Use

- Data ownership (who owns what, what can they do with it)
- Customer wants ownership of:
  - Data input by customer -- and by its end users
  - Data processed and stored in the cloud
  - Derivative data
- Right to use supplier data
- Data processed and stored by third-party providers
  - Many cloud suppliers utilize third party cloud infrastructure

Data-Related Concerns

- Supplier right to use de-identified/ aggregated/anonymized data – for what use?
  - Optimize the solution
    - Suppliers usually want the ability to use anonymized data for usage statistics and product improvement
  - The risk is whether it is really anonymized
    - Cannot identify the customer
    - Cannot identify an individual
    - Hard to comply with standard under EU and other laws
  - Broader use
    - Great value in the data – driving AI and other solutions

Data-Related Concerns – Data Security

- More focus required based on expanded cloud adoption
  - Has this received sufficient attention in the rush to get solutions implemented?
  - Understanding of differing security for varying aspects of solution?
    - Multiple IT infrastructures as part of solution
- Data security requirements
  - Physical and technical security
  - Encryption
  - Handling security incidents/data breaches
  - Audits and reporting
  - Network security
  - Flow downs to subcontractors

Data-Related Concerns – Data Security

- Customer expectations v. supplier offering
- Practical approach
  - Data security teams from customer and supplier need to be involved
  - If customer has specific requirements, they should be vetted early
    - Consider including in RFI/RFP requirements
  - Use of security questionnaire to understand supplier data security policies
  - Contract considerations
    - Include reference to supplier data security/security questionnaire results
    - Describe as “minimum” data security to address future modifications

Data-Related Concerns

- Location, processing and storage of data
  - Restrictions on geography
  - Specific locations/data center
- eDiscovery and data preservation
- Data retention and destruction
- Audit rights and audit obligations
  - Vendor wants:
    - Make information that proves compliance available to customer
    - Provide copies of third-party audits or certifications
      - (e.g., SSAE 18 SOC 1/SOC 2 Report)
  - Customers wants: on-premise audit

Data-Related Concerns – Privacy

- Privacy Concerns
  - Does the solution meet all laws/regulatory requirements?
  - Does the solution meet customer's (and its end users') privacy expectations?
    - Customer internal solution or consumer end users
  - Will the solution be consistent with customer's privacy policy (and TOS)?

Application of Laws and Regulatory Schemes

- Understanding U.S., international and industry regulatory considerations when contracting for cloud computing
- Compliance with law
  - Which laws/regulations apply?
    - Contract will have choice of law, but privacy laws such as GDPR will apply via DPA
  - Impact of regulatory “guidance” and commentary
  - Cloud services may be provided from multiple unknown jurisdictions
    - Sub-processors will likely be based in multiple geographies

Application of Laws and Regulatory Schemes

- Changes in laws/regulations
- Particular concerns of a regulated entity
  - Definition of “laws”
  - Regulatory consents/approvals
  - Governmental authority audits
  - Mandatory regulatory “flow downs”
  - Interaction with related documents (e.g., BAA)

Data-Related Concerns – Key Laws

- California Consumer Privacy Act (CCPA)
  - Key tenet: Consumer can opt-out from the sale of personal information
    - “Sale” is a very broad term
- HIPAA and HITECH: Federal laws that protect PHI and provide for electronic and physical security of PHI
  - Is a BAA required?
- General Data Protection Regulation (GDPR)
  - EU data protection laws with steep penalties for non-compliance
  - No more Privacy Shield
  - New Standard Contractual Clauses

Data Processing Agreements

- Which form – vendor vs. client
- Who are the parties?
  - Controller vs. processor vs. subprocessor
- Standard contractual clauses
  - No Privacy Shield after *Schrems II*
- Audit rights
  - Client performing the audit vs. vendor performing self-audit
  - Acceptable limitations
    - Information available upon written request and with adequate notice
    - Right to object to unqualified auditors
    - Require auditor to sign NDA

Data Processing Agreements

- Data breach
  - Actual vs. suspected breach
    - Vendor can only accept actual, but customer will want suspected
  - What is a reasonable deadline?
- Subprocessors
  - How much notice is sufficient in the event of an addition or replacement?
    - Varies from actual to suspected - 72 hours under GDPR if controller knows
    - What happens if the client objects?
  - General consent vs. individual consent
  - Online list vs. static list
  - Impact of dollars spent/collected

Key Risk Issues: Business Continuity and Disaster Recovery

Disaster Recovery and Business Continuity

- Disaster Recovery and Business Continuity are more significant in the COVID-19 environment
  - Majority remote workforce means loss of a cloud service has a greater impact
  - Customers and suppliers need to actively engage in discussions about how service delivery would continue as the pandemic significantly impacts solution/supplier ability to perform
- Disaster Recovery v. Business Continuity
  - Often lumped together, but may require separate consideration

Service Continuity

- Disaster Recovery
  - Will the solution support the customer's disaster recovery requirements?
  - Solution as "commodity" v. customized offering
  - Understand supplier's DR plan
    - RPOs and RTOs
    - Backup and redundancy
    - Provider or third-party contractor
- Contract approach
  - Address supplier's DR plan
  - Interaction with SLAs and penalties

Service Continuity

- Business Continuity
  - Understand supplier's business continuity plans
    - Red flags if supplier does not have a plan
  - More comprehensive than DR plan
    - Addresses business processes, IT, facilities, other assets, and HR
  - How will the supplier perform if workforce/IT/assets are unavailable
    - e.g., pandemic "second wave"
- Force Majeure provision continues to evolve to reflect broader reality of "disaster"
  - Now a hotly negotiated provision, including remedies

Key Risk Issues:
Liability And Indemnity

Which Party Is Responsible for What? Liability Issues

- Liability and remedies are limited
  - Commodity solutions
  - But can negotiate some key issues
- Need to understand solution and data involved to address key risks
- Reality of use of third party infrastructure may limit remedies available
- Necessarily ties to understanding/agreement on key risk issues
  - Privacy and Data Security
  - Disaster Recovery and Business Continuity
  - SLAs and remedies

Negotiation Key Contract Terms – Limitation of Liability

- Industry standard liability cap based on a multiple of fees
- Carve-outs
  - Indemnification obligations
  - Confidentiality breaches
  - Data security failures (including breach notification costs)
  - Gross negligence/willful misconduct
- Unlimited liability v. Supercap
  - Increased fixed number/multiple of fees, particularly for data security breaches
- Attention to “sole remedies”

Negotiation Key Contract Terms – Indemnification

- Indemnifications – what the customer wants
  - Confidentiality violation
  - IP infringement
  - Gross negligence and willful misconduct
  - Data breach; breach of security requirements; breach of DPA
  - Violation of law
- Indemnifications – what the vendor may agree to and how it can limit the effects
- Understanding of “inter-party” claims liability and “third-party” claims indemnification

Key Risk Issues: Termination Assistance

Breaking Up Is Hard To Do

- What happens at the end?
  - Customers: Services continuity, transfer of data, help with migration
  - Vendors: Hard-cut off dates, make data available, assistance for a fee

- Contractual Considerations
  - Negotiate a term extension and termination assistance at the start
  - Customers want assurances of services continuity
  - Vendors will seek more fees

Key Risk Issues:
Other Key Contract Terms

Service Levels/Key Performance Indicators

- Subscription Fees = Ongoing obligation to maintain the solution and its availability
- Limited SLAs, limited remedies
  - Commodity solutions
- Differing SLAs by supplier
- SLAs and remedies will differ by solution
- Limited negotiability

Subcontracted IT-Hosting Environment

Concern is consistency across solution for all major risk issues:

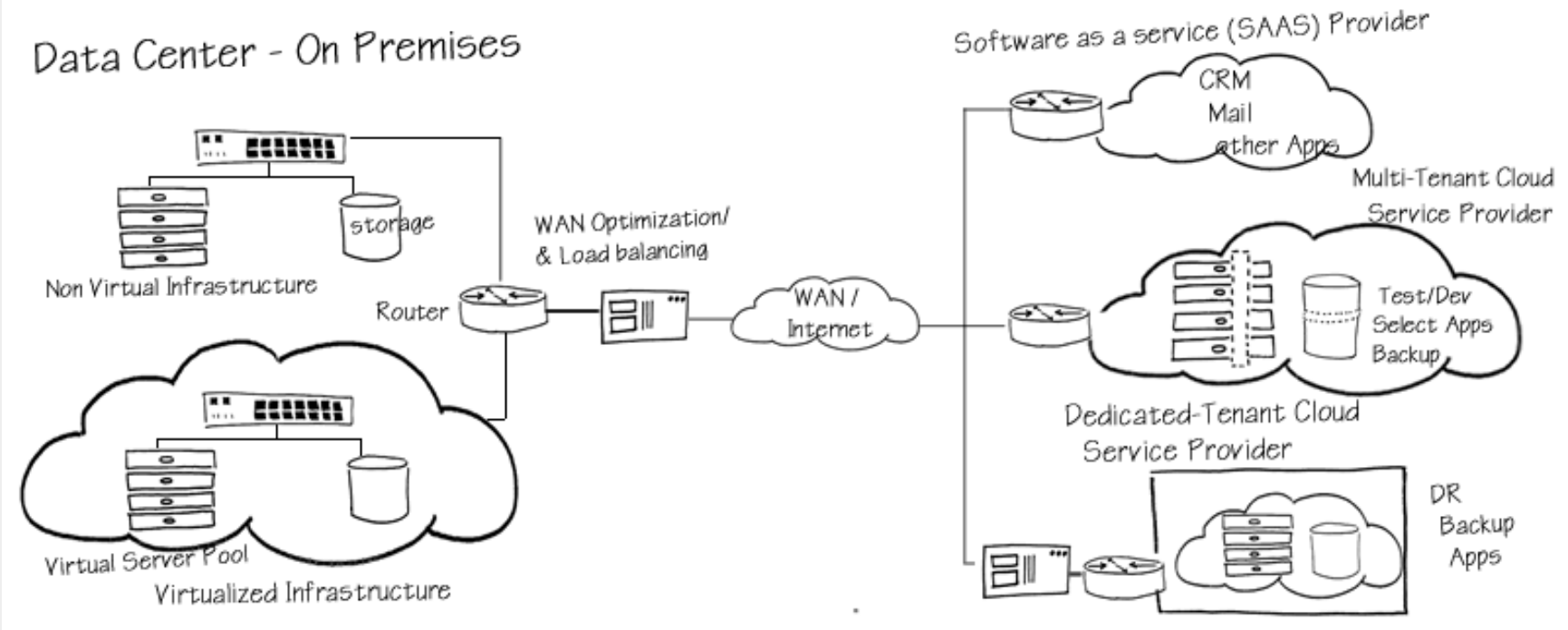
- Data security standards and obligations
- Self-Audit and Audit Rights
- Service Levels/Remedies
- Liabilities
- Disengagement

Key Take-Aways and Best Practices

Tactical Review Pre-Contract (solution, suppliers, subcontractors)

- ✓ Determine which stakeholders should participate (the department buying the solution + finance + legal + IT security)
  - ➢ **PRO TIP:** Involve IT security and legal teams **early**
    - Many data security contracting concerns can be quickly resolved by the security experts having a conversation
    - Security reviews can be time consuming because service providers may need to complete a controls questionnaire
    - Legal often needs time to review and redline agreements
  - ➢ **PRO TIP**: Get a demo of the solution; many negotiation points will be more easily resolved if both parties understand what the product does and how it works

Whiteboard the Deal



** Layer on top:

- Data flows
- Geographies

Tactical Review Pre-Contract (solution, suppliers, subcontractors)

- ✓ Determine whether the solution complies with:
  - Legal and regulatory requirements for privacy and data security
  - Privacy policies
  - Information security policies
  - Transactional standards
- ➢ **PRO TIP:** Ask service providers whether they use subcontractors and for what purpose. This information may not be given unless requested, and the use of subcontractors has data privacy, data security and liability implications
- ➢ **PRO TIP:** Be reasonable. For any mature/tested product, a deal should not die because of the lawyers. We are there to protect our companies while enabling them to do business

Challenging Negotiations

- Vendors view their offerings as commodities and will not negotiate or take on risk
  - View: Customers would carry this risk if they self-hosted
- Customers want protection from risk and may have legal obligations to protect data
  - If cloud vendors will not negotiate, summarize risks and secure internal approval
    - Cost vs. Liabilities/Risk

- Negotiation pressure points

✓ Consider timing – end of quarter/year as part of the negotiation strategy

✓ Consider value of contract: More money = more leverage