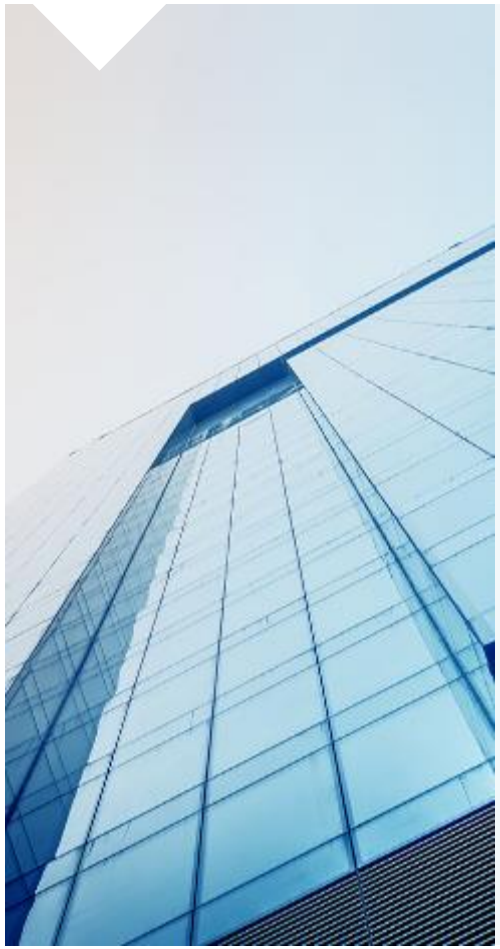
mcmillan

Do’s And Don’ts of Technology Services Contracts

Wednesday October 27, 2021

Agenda



1. Do prepare to negotiate your limitations and caps on liabilities
2. Do understand credits & remedies for service level failures
3. Don’t forget to review your representations and warranties
4. Don’t miss the important issue of data encryption
5. Do carefully consider your audit rights
6. Do plan your contract exit strategy to ensure you can transition out smoothly

1. Do prepare to negotiate your limitations and caps on liabilities

Background

- What is a LOL provision?
  - Restricts the type and scope of liability of the parties
- What types of liability are generally limited?
  - Indirect, incidental, consequential, special and punitive losses, loss of profits, loss of business, loss of goodwill
- Exclusions
  - Gross negligence, willful misconduct, breach of confidentiality, breach of security/privacy
- Caps
  - Dollar limit on liability exposure
  - Often tied to value of the contract
  - Practically, can be more useful than limitations

Key Considerations

- Negotiation issues
  - Scope – liabilities excluded from the application of the limitation of liability
  - Allocation/balance of risk between the parties

- Liability caps
  - Quantum of cap:
    - Value of contract/SOW
    - 12 months' fees
    - greater of $XXX and 12 months' fees
    - Uncapped?
  - Tie liability caps to insurance coverage?

Strategic Takeaways

- Always heavily negotiated
  - Know your rights and obligations
- Business exposure and risk
  - Is the liability risk too great?
  - Proceed or walkaway
- Balance is key
  - Creates legal certainty
  - Strong relationships and trust

2. Do understand your credits & remedies for service level failures

Background

- "Service Levels" are quantitative standards that represent a service provider's obligations for the quality of their services
  - Core service commitment received in exchange for fees paid
  - Measurable, objective and quantitative vs. non-objective and qualitative
  - Examples: Availability (e.g. 99.9%); Response Time (e.g. 90% within 4 hours)

- "Service Level Credits" are pre-determined monetary amounts which vendor provides as an invoice credit for a Service Level failure
  - Typically calculated and credited monthly
  - Liquidated damages not a penalty (genuine pre-estimate of the customer's damages for the stipulated service failure)
  - Customer must claim vs. service provider must measure, report and issue

Key Considerations

- What amount of Service Level Credits is reasonable to expect?
  - A percentage of monthly fees (specific service vs. total monthly invoice)
  - 10 – 15% of total monthly fees for large custom managed/outsourcing services
  - Often a monthly aggregate cap for maximum Service Level credits
  - Can be a sliding scale for cloud services (e.g. credit = 25% of fees for specific service if < 99.9%, but 100% if < 99.5%)

Key Considerations

- Sole and exclusive remedy for the Service Level failure?
  - Service Providers' preferred standard approach
  - Small pre-determined credits vs. large potential unknown damages
  - Generally stated in SLAs of major cloud service providers

- Nature and extent of exclusions (service provider relief)
  - Cause of failure (customer or service provider)
  - Acts and omissions of customer vs. customer's failure to perform its obligations
  - Third party vendors and force majeure

Strategic Takeaways

- Understand what's negotiable (measures? amount of credits? nothing?)
- Consider the sole/exclusive remedy language and exclusions
  - Reasonable compromise allow claims for damages but deduct any credits paid
- Work closely with your technical team
- Advanced considerations:
  - Escalations for repeated Service Level failures
  - Multiple Service Level credits and double jeopardy

3. Don’t forget to review your representations and warranties

Background

- Purpose of reps and warranties
- Typically imposed more on the service provider
- What do reps and warranties generally address?
  - Corporate organization
  - Ability to enter into contracts
  - Performance in accordance with industry standards

Key Considerations

- Common reps and warranties in tech contracts
  - Malicious Code
  - IP infringement
  - Privacy/Data Security
  - Personnel

- Warranty Disclaimers

Strategic Takeaways

- Ensure you understand:
  - Scope of reps and warranties
  - Cost implications
- Can be a tool to foster trust
- Warranty disclaimers – understand impact

mcmillan

4. Don’t miss the important issue of data encryption

Background

- "Encryption" is a type of technological security control applied to protect data
  - Encryption converts data from an openly accessible state into a concealed state to obscure its original content and make it unreadable except to a person or system with the applicable decryption key

- Do common security standards or obligations require encryption?
  - *Personal Information Protection and Electronic Documents Act* (Canada) – businesses obliged to use "appropriate security safeguards", such as "up-to-date technological tools (e.g., … encryption)"
  - OSFI Cyber Security Self-Assessment (2021) – encourages applicable regulated entities to assess and improve cyber security with reference to best practices, including certain uses of encryption

Background

- ISO/IEC 27001
  - Independent international standard for information security management systems outlining non-industry specific best practices and potential security controls
  - Annex A requires policies on the use of encryption and encryption key management

- National Institute of Standards and Technology (US) Cybersecurity Framework
  - Voluntary risk management framework designed to improve cybersecurity
  - Framework does not expressly call for encryption, but data protection is a core component and companion guidance deals directly with encryption as a best practice

Key Considerations

- What types of data should be encrypted?
  - All data? All personal information? Sensitive personal information? Client confidential information?
- Data in transit vs. data at rest
  - "Data in transit" is data moving between networks or locations within a network
  - "Data at rest" is data stored in a given location within a system and not being accessed by a user (e.g. data stored on laptop hard drive)
  - Data in transit often encrypted; for data at rest, it will depend
- Blanket "encrypt all data" approach is impractical for service providers
  - Higher standard than most organizations meet themselves
  - Need to consider hardware/software limitations and potential costs

Strategic Takeaways

- Understand which standards are most common in your industry
  - Standards and certification can be helpful but don't guarantee encryption
  - Service providers generally consider customers responsible for determining specific practices for their different categories of data
- Contract representations to use "security measures used by top tier technology service providers" vs. "reasonable security measures"
- Work with your technical/security leads to understand the risks, types and location of data and what should/can be encrypted

5. Do carefully consider your audit rights

Background

- What are audit rights?
  - Contractual right that promotes the concept of trust but verify
- What can be audited?
  - Security
  - Charges
  - Legal/Contractual compliance
    - Consents to process personal information
    - Number of license seats

Key Considerations

- Do I need audit rights? / Do I need to be audited?
  - Risk management tool
  - Encourages compliance
  - Identifies strengths/weaknesses in systems and processes
  - Can foster trust

- Scope – how broad/narrow should the audit be?
  - Are there security issues related to granting access?
  - Who must be made available to the auditors?

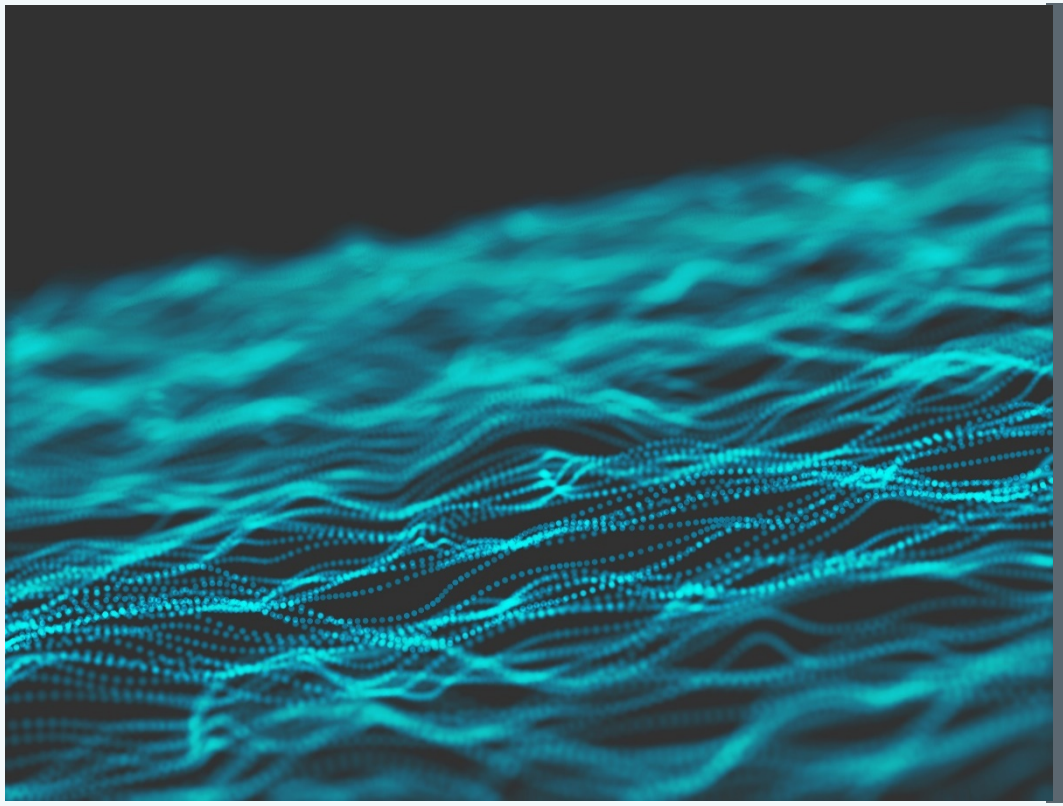
Key Considerations

- Auditor vs. Audited
  - Risks/benefits of doing an audit
  - Issues to consider
    - Confidentiality/NDAs
    - Who is the auditor?
    - Frequency and notifications
    - Who is responsible for the costs of the audit?

Strategic Takeaways

- Carefully review the language of the audit clause
- Does the language reflect the agreement and your expectations
- Incorporate sufficient detail to avoid disputes, disruption to business, costs and damage to relationships. Consider:
  - Who will be the auditor
  - NDAs for third party auditors
  - Frequency/timing of audits
  - Notice requirements
  - Cost allocation

mcmillan



6. Do plan your contract exit strategy to ensure you can transition out smoothly

Background

- What is an exit strategy?
  - Having the resources, staff, processes and planning in place for a smooth transition on contract termination or expiry
  - Maintain service quality and service levels with minimal disruption
  - May apply mid-term for termination for convenience or to termination of partial services/functions

- When is it appropriate to have one?
  - Longer term managed service/outsourcing contracts
  - As-a-Service contracts involving a cloud platform and customer data
  - Less important for short term and consulting or advisory services contracts

Key Considerations

- What are the resources/assets a customer needs to be able to access at contract termination/expiry?
  - Staff with relevant expertise – availability; option to hire
  - Software – commercially available from 3rd parties vs. custom/proprietary
  - Hardware – shared vs. dedicated; option to purchase
  - Transition Planning – which party leads vs. assists

- Be sure to think through access to data
  - Customer or service provider responsibility to retrieve/return data
  - Format acceptable to customer, industry standard, or "as is"
  - Access to separately available, up-to-date back-up copies of data

Key Considerations

- Does customer require a ramp-down or transition-out period?
  - 30-60 days in standard Cloud/SaaS contracts
  - 6–12 months typical for more complex managed/outsourced services
  - Customer option to extend
- What fees are payable during ramp down period?
  - Fees for steady state services (equitable adjustment)
  - Pre-define rates for transition assistance from Service Provider
- What is the vendor responsibility for service levels during ramp-down?
  - Good transition plan is important
  - May be difficult to meet Service Levels if Vendor has only partial responsibility

Strategic Takeaways

- Understand the extent of your exposure (customer reliance on service provider vs. service provider risk of stranded resources/assets)
- As a customer, drill deep on categories and availability of data
- Important for both parties; shouldn’t be contentious
- Service provider reputation can depend on how well they assist/cooperate during contract termination

Thank You

Q&A

Robert C. Piasentin

Partner, Technology

Vancouver

604.893.7636

robert.piasentin@mcmillan.ca

Greg Johns

Counsel, Technology

Toronto

416.305.7187

greg.johns@mcmillan.ca

Graham Bevans

Associate, Business Law

Toronto

416.865.5514

graham.bevans@mcmillan.ca

Gurp Dhaliwal

Associate, Business Law

Vancouver

236.826.3060

gurp.dhaliwal@mcmillan.ca

mcmillan

Get in Touch

EMAIL
info@mcmillan.ca

LINKEDIN
@mcmillanllp

INSTAGRAM
@mcmillanllp

TWITTER
@mcmillanllp

If you have any questions about McMillan, or how we may help you with your legal needs, please get in touch with us.