Compliance Checklist for Prospective Cloud Customers

Disclaimer: This checklist is designed to assist a potential cloud user in thinking through some general issues surrounding cloud computing. It is not intended, nor should it be regarded, as legal advice. Companies or individuals contemplating entry into a cloud computing contract or having particular questions should seek the advice of counsel.

General Questions to Consider

- What are the characteristics of the information that will be stored on the cloud?
  - How sensitive is the information/what is the risk profile?
    - Consider what laws and regulations of general applicability apply to the information (e.g., Massachusetts data security regulations).
    - Is the data subject to sector-specific regulations (e.g., health and medical personal information (HIPAA); non-public personal financial information (Gramm Bliley Act); phone records (Communications Act and CPNI rules)
  - Is it imperative that the cloud provider keep the information confidential?
  - Would it be permissible for the cloud provider to aggregate data and use such data for its own purposes or to sell reports to others?
  - Is it possible to go without the information for any period of time? How long?

- Does the cloud provider's product and contract adequately address the issues identified during due diligence review?
  - How, and by whom, will the provider handle, control, and process your organization's information?
    - Where information is stored implicates what data protection legal regime may apply. Is data stored in the EU? Asia-Pacific Economic Co-operation countries? Canada? U.S. (state and federal laws potentially apply)?
    - Depending on the jurisdiction, the customer must also consider:
      - Trade secret protections
      - Data security requirements
      - Breach notification obligations
  - Are there geographic boundaries to the service offering?
  - Does the cloud provider's product and contract adequately address the information's risk profile?
    - What are the cloud provider's standard security guidelines, policies, and procedures?
    - Does the cloud provider use exclusively its own computing environment (including back-up and storage capacity)?
    - Are the representations and warranties about data protection and regulatory compliance adequate?
    - Are the remedies adequate, including for data breaches, indemnification obligations, and service availability failure?
    - Does the cloud provider's protections mirror protections the customer uses when it hosts its own data?
  - Does the cloud provider seek to access or use the customer's data in aggregate form or otherwise?
  - What are the schedules and procedures for updating and maintaining the service? Is it manageable?
  - For form contracts, especially a click-wrap agreement, when and under what conditions can the terms be updated by the cloud provider (i.e., "at any time," etc.)?

- Are you comfortable with relying on the provider's computing environment and its ability to make its computing environment available (and to restore interrupted access)?

Key Contract Sections and Issues

- Data Security
  - Who is responsible for the handling, processing, storing, and using of personal and sensitive information?
    - Is the provider responsible for subcontractors?
  - What are the representations as to security measures?
    - Physical protections
    - Encryption
    - Data backup and off-site storage schedules
  - Who is liable for security breaches and how will the cloud provider respond to a breach?
    - Must the cloud provider notify the customer and under what time frame?
  - What data security due diligence is being done?
  - How will the disposal of personal and sensitive information be handled?

- Regulatory Compliance
  - What representations do the parties make about who is responsible for regulatory compliance?

- Asset Availability
  - What availability warranty does the cloud provider offer?
  - How is available uptime calculated?
  - What's the definition of "scheduled down time?"
  - Is there a remedy for a warranty breach?
  - Is there a disaster recovery/business continuity plan?

- Asset Maintenance
  - When are the customer support hours?
  - Are the routine maintenance windows manageable?
  - Can the provider provide meaningful problem response and resolution commitments?
  - Does the provider give notice of material reductions in functionality?

- Data Control
  - May the provider use the customer's data? What if the data is aggregated and de-identified?
  - Does the customer have the right to insist on a complete copy of all of its data? Under what terms?

- Termination/Transition
  - Does the customer have the right to terminate if the provider introduces material modifications to service terms?
  - Is there a right of termination for material breach of applicable privacy and security obligations (cure period)?
  - If the contract is terminated, may the customer seek transition assistance to installed assets or to a replacement cloud service provider? Does the provider have any obligation to return the data?
  - Can the provider continue to use data in aggregate form after a contract is terminated?

- Pricing
  - What are the pricing terms: Pay as you go? Upfront payments?
  - When can the provider increase rates?
  - Is there a cap on liability?

www.hoganlovells.com