Legal Risk and Uncertainty in Managing Services, Vendors, and Contracts

Discussion Activity: Parameters of Risk Inquiry

We ask about many types of legal risk in cloud contracts, but sometimes the answers we receive are not ideal. Where do you choose to continue to negotiate, where do you walk away from a contract? Rank the following items by your greatest concern, least concern, and greatest concern where you are willing to accept an unsatisfactory answer.

1. Auditing and forensics: Verify that the vendor has a process in place to audit the services and provide those audit logs to the institution as needed for performance, incident handling, and forensics needs
2. Business Continuity and Disaster Recovery: Verify that the vendor has appropriate safeguards to ensure continued operations in the event of an outage or disaster
3. Data Backups: Verify that data backups are regularly made and verified to be accurate and usable
4. Data Segregation: Verify that your institutional data is kept separate from another entity's data
5. Encryption of Data at Rest: Verify that institutional data is encrypted
6. Institutional Data Availability: Verify the processes to ensure that critical institutional business and academic data (e.g., admissions, business operations, research, etc.) are available when needed
7. Institutional Service Availability: Verify the processes to ensure no institutional loss of access to IT systems and services for an unacceptable period of time
8. Operational Security: Verify that the vendor has enacted logical security safeguards to protect institutional data/services (such as single sign-on support, configurable security groups)
9. Physical security: Verify that the vendor has appropriate co-location, redundancy, security zones, two factor authentication presence, camera surveillance, least privilege.
10. Security Compliance and Certifications: Verify that the vendor/service meets a security standard such as ISO, NIST, or institutional developed standard
11. Service management: Verify that the vendor has a process for measuring and managing service performance, and for managing service problems to ensure they are adequately resolved or for investigating causes to prevent recurrence

<table>
<thead>
<tr>
<th>Items of greatest concern</th>
<th>Items of least concern</th>
<th>Greatest concern/usually unsatisfied</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. _____________________</td>
<td>1. _____________________</td>
<td>1. _____________________</td>
</tr>
<tr>
<td>2. _____________________</td>
<td>2. _____________________</td>
<td>2. _____________________</td>
</tr>
<tr>
<td>3. _____________________</td>
<td>3. _____________________</td>
<td>3. _____________________</td>
</tr>
</tbody>
</table>