Risk Associated with Cloud Computing

Overall risk and benefits differ per cloud service and deployment models. Enterprises should consider the risk that accompanies each of them. Click the links below to read more about each type of risk.

Legal Transborder Requirements

Physical Security

Data Disposal

Multitenancy and Isolation Failure

Application Disposal

System Development Life Cycle (SDLC) Process Visibility

Release Management Process

Identity and Access Management (IAM)

Service Orientated Architecture (SOA)

Exit Strategy

Ease to Contract SaaS

Collateral Damage

Hypervisor Attacks

Support for Audit and Forensic Investigations

Legal Transborder Requirements

Description:
Cloud service providers (CSPs) are often transborder, and different countries have different legal requirements, especially concerning personal private information. The enterprise might be committing a violation of regulations in other countries when storing, processing or transmitting data within the CSP's infrastructure without the necessary compliance controls. Furthermore, government entities in the hosting country may require access to the enterprise's information with or without proper notification.

Control:

- Request the CSP's list of infrastructure locations and verify that regulation in those locations is aligned with the enterprise's requirements.
- Include terms in the contract to restrict the moving of enterprise assets to only those areas known to be compliant with the enterprise's own regulation.
- Prevent disclosure, encrypt any asset prior to migration to the CSP and ensure proper key management is in place.

Physical Security

Description:
Physical security is required in any infrastructure. When the enterprise moves assets to a cloud infrastructure, those assets are still subject to the corporate security policy, but they can also be physically accessed by the CSP's staff, which is subject to the CSP's security policy. There could be a gap between the security measures provided by the CSP and the requirements of the enterprise.

Control:

- Request the CSP's physical security policy and ensure that it is aligned with the enterprise's security policy.
- Request that the CSP provide proof of independent security reviews or certification reports that meet the enterprise's compliance requirements (e.g., SOC reports, SOX, PCI DSS, HIPAA, ISO certification).
- Include in the contract language that requires the CSP to be aligned with the enterprise's security policy and to implement necessary controls to ensure it.
- Request the CSP's disaster recovery plans and ensure that they contain the necessary countermeasures to protect physical assets during and after a disaster

Data Disposal

Description:
Proper disposal of data is imperative to prevent unauthorized disclosure. If appropriate measures are not taken by the CSP, information assets could be sent (without approval) to countries where the data can be legally disclosed due to different regulations concerning sensitive data. Disks could be replaced, recycled or upgraded without proper cleaning so that the information still remains within storage and can later be retrieved.

When a contract expires, CSPs should ensure the safe disposal or destruction of any previous backups. Any of the data fed into the CSP's application must be erased immediately using the necessary tools to avoid disclosures and confidentiality breaches (forensic cleaning may be required for sensitive data).

Control:

- Request CSP's technical specifications and controls that ensure that data are properly wiped and backup media are destroyed when requested.
- Include terms in the contract that require, upon contract expiration or any event ending the contract, a mandatory data wipe carried out under the enterprise's supervision

Multitenancy and Isolation Failure

Description:
One of the primary benefits of the cloud is the ability to perform dynamic allocation of physical resources when required. The most common approach is a multitenant environment (public cloud), where different entities share a pool of resources, including storage, hardware and network components.

For example, when allocated storage is no longer needed by a client it can be freely reallocated to another enterprise. In that case, sensitive data could be disclosed if the storage has not been scrubbed thoroughly (e.g., using forensic software).

Furthermore, malicious entities in the cloud could take advantage of shared information—for example, by utilizing shared routing tables to map the internal network topology of an enterprise, preparing the way for an internal attack.

Control:

- Request the CSP's technical details for approval and require additional controls to ensure data privacy, when necessary.
- A contractual agreement is necessary to officially clarify who is allowed to access the enterprise's information, naming specific roles for CSP employees and external partners. All controls protecting the enterprise's information assets must be clearly documented in the contract agreement or service level agreement (SLA).
- Use a private cloud deployment model (no multitenancy)

Application Disposal

Description:
When applications are developed in a PaaS environment, originals and backups should always be available. In the event of a contract termination, the details of the application could be disclosed and used to create more selective attacks on applications or could be copied violating the enterprise's IP.

Control:

- Include terms in the contract that require the proper disposal of applications including objects, source and backups.
- Include non-compete clauses in the contract.

System Development Life Cycle (SDLC) Process Visibility

Description:
Enterprises that use cloud applications have little visibility into the software SDLC. Customers do not know in detail how the applications were developed and what security considerations were taken into account during the SDLC. This could lead to an imbalance between the security provided by the application and the security required by customers/users

Control:

- If possible include a right of audit in the contract.
- Include in the contract language that requires the CSP to be aligned with the enterprise's security policy and to implement necessary controls to ensure it.
- Require SLAs that include a schedule of software changes.

Release Management Process

Description:
CSPs are able to introduce patches in their applications quickly. These deployments are often done without the approval (or even the knowledge) of the application users for practical reasons: If an application is used by hundreds of different enterprises, it would take an extremely long time for a CSP to look for the formal approval of every customer. In this case, the enterprise could have no control (or no view) of the release management process and could be subject to unexpected side effects.

Control:

- If possible, include a right of audit in the contract.
- Include in the contract language that requires the CSP to be aligned with the enterprise's security policy and to implement necessary controls to ensure it.
- Require SLAs that include a schedule of patches and software releases.

Identity and Access Management (IAM)

Description:
Information assets could be accessed by unauthorized entities due to faulty or vulnerable access management measures or processes. This could result from a forgery/theft of legitimate credentials or a common technical practice (e.g., administrator permissions override).

Control:

- If possible, include a right of audit in the contract.
- Include in the contract language that requires the CSP to be aligned with the enterprise's security policy and to implement necessary controls to ensure it.
- Request that the CSP provide proof of independent security reviews or certification reports that meet the enterprise's compliance requirements (e.g., SOC reports, SOX, PCI DSS, HIPAA, ISO certification).

Service Oriented Architecture (SOA)

Description:
Security for SOA presents new challenges because vulnerabilities arise not only from the individual elements, but also from their mutual interaction. Because the SOA libraries are under the responsibility of the CSP and are not completely visible to the enterprise, there may be unnoticed application vulnerabilities.

Control:

- If possible include a right of audit in the contract.
- Include in the contract language that requires the CSP to be aligned with the enterprise's security policy and to implement necessary controls to ensure it.
- Request that the CSP provide proof of independent security reviews or certification reports that meet the enterprise's compliance requirements (e.g., SOC reports, SOX, PCI, DSS, HIPAA, ISO certification).

Exit Strategy

Description:
CSP tools facilitate bring data to the cloud or CSP but rarely the other way around. This can make it very difficult for the enterprise to migrate from one CSP to another or to bring services back in-house. It can also result in serious business disruption or failure should the CSP go bankrupt, face legal action or be the potential target for an acquisition (with the likelihood of sudden changes in CSP policies and any agreements in place).

If the organization decides to bring the data back in- house, the question of how to securely render the data becomes critical because the in-house applications may have been decommissioned (i.e., sunset) and there is no application available to render the data. Another possibility is the run-on-the-banks scenario, in which there is a crisis of confidence in the CSP financial position, resulting in a mass exit and withdrawal on a first-come, first-served basis.

If there are limits to the amount of content that can be withdrawn in a given time frame, then the enterprise might not be able to retrieve all its data in the time specified.

Control:

- Ensure by contract or SLA with the CSP an exit strategy that specifies the terms that should trigger the retrieval of the enterprise's assets in the time frame required by the enterprise.
- Implement a disaster recovery plan, taking into account the possibility of complete CSP disruption.

Ease to Contract (SaaS)

Description:

Business organizations may contract cloud applications without proper procurement and approval oversight, thus bypassing compliance with internal enterprise policies.

Control:

- Require that the purchase of cloud services follow the established procedures.
- Ensure executive management support for this strategy.

Collateral Damage

Description:
If one tenant of a public cloud is attacked, there could be an impact to the other tenants of the same CSP, even if they are not the intended target (e.g., DDoS). Another possible scenario of collateral damage could be a public cloud IaaS that is affected by an attack exploiting vulnerabilities of software installed by one of the tenants.

Control:

- Ask the CSP to include the enterprise in its incident management process that deals with notification of collateral events.
- Include contract clauses and controls to ensure that the enterprise contracted capacity is always available and cannot be directed to other tenants without approval.
- Use a private cloud deployment model (no multi-tenancy).

Hypervisor Attacks

Description:
Hypervisors are vital for server virtualization. They provide the link between virtual machines and the underlying physical resources required to run the machines by using hypercalls (similar to system calls, but for virtualized systems). An attacker using a virtual machine in the same cloud could fake hypercalls to inject malicious code or trigger bugs in the hypervisor. This could potentially be used to violate confidentiality or integrity of other virtual machines or crash the hypervisor (similar to a DDoS attack).

Control:

- If possible, include a right of audit in the contract.
- Include in the contract language that requires the CSP to be aligned with the enterprise security policy and to implement necessary controls to ensure it.

Support for Audit and Forensic Investigations

Description:
Security audits and forensic investigations are vital to the enterprise to evaluate the security measures of the CSP (preventive and corrective), and in some cases the CSP itself (for example, to authenticate the CSP). This raises several issues because performing these actions requires extensive access to the CSP infrastructure and monitoring capabilities, which are often shared with other CSP customers.

Control:

- Request the CSP the right to audit as part of the contract or SLA. If this is not possible, request security audit reports by trusted third parties.
- Request that the CSP provide appropriate and timely support (logs, traces, hard disk images, etc.) for forensic analysis as part of the contract or SLA. If this is not possible, request to authorize trusted third parties to perform forensic analysis when necessary.