Information Security Forum

Data Privacy in the Cloud

Enabling business agility by managing risk

Organisations can't avoid using the cloud. With surveys reporting that 90% of organisations achieve projected savings and 80% increase their competitive advantage, as a technology writer put it:

> ***"The cloud is coming to your business, like it or not."***

With cloud-based systems come inherent challenges. These are further complicated as data subject to privacy regulation inevitably moves into the cloud.

This combination, putting private information into the cloud, creates risk and must be understood and managed. For example, organisations may have little or no control over the movement of their information, as cloud services can be provided by multiple suppliers moving information between data centres scattered across the globe. If the information being moved is subject to privacy regulations, and the data centres are in different jurisdictions, this can trigger additional regulations or result in a compliance breach.

The decision to use cloud systems should be accompanied by an information risk assessment that's been conducted specifically to deal with the complexities of both cloud systems and privacy regulations; it should also be supported by a procurement process that helps compel necessary safeguards. Otherwise, the persistent pressure to adopt cloud services will increase the risk that an organisation will fail to comply with privacy legislation.

The ISF ***Data Privacy in the Cloud*** report explains why data privacy in the cloud is a business issue. It provides an overview of privacy as a concept, and explains personally identifiable information (PII), along with the demands typically placed on organisations by privacy regulations. It de-mystifies the complexity of cloud-based systems and their inherent risks.

The report further enhances the ISF Privacy Framework to address cloud-based privacy issues, enabling organisations to develop the privacy safeguards and good practice guidelines specific to their organisation – and determine the actions required to achieve privacy compliance when using cloud-based systems. Finally, it contains a structured process for procuring cloud services and managing the privacy risk throughout the term of a cloud contract – a process that supplements and integrates with the ISF Supply Chain Information Risk Assurance Process.

The risks of using cloud services for private data are significant – and easily managed

Cloud complexity made simple

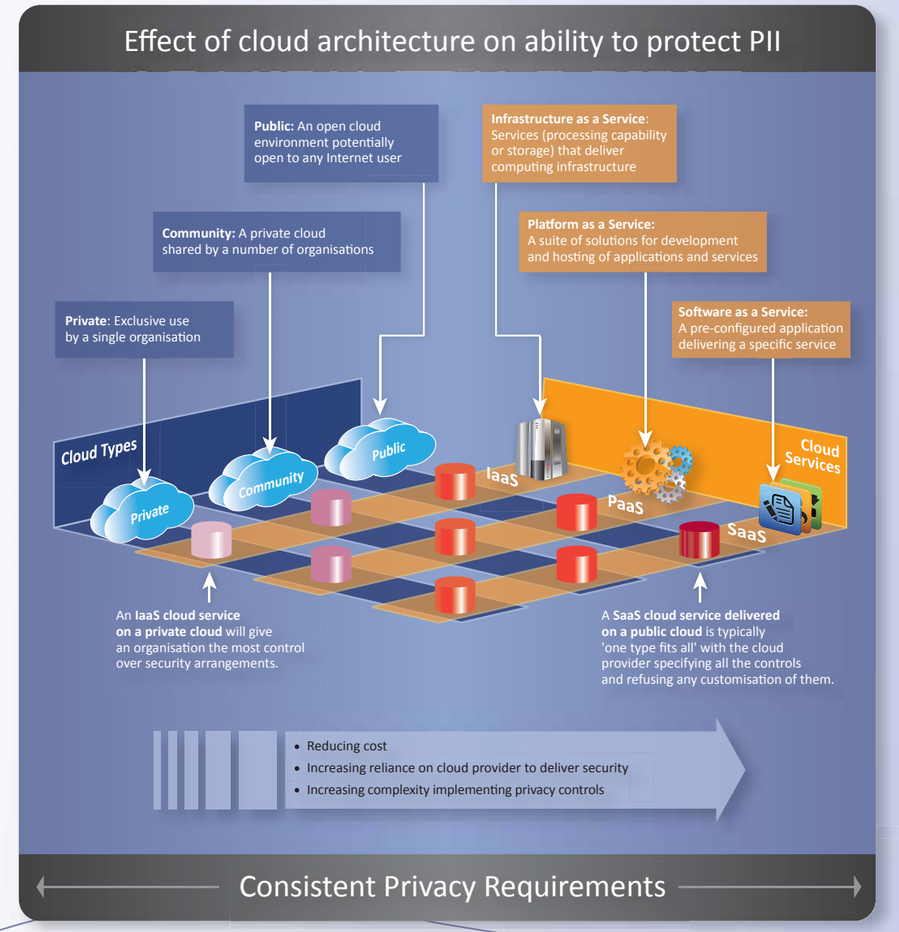
Every cloud-based system is a combination of a particular cloud service deployed on a particular cloud type.

There are three kinds of cloud service – Infrastructure, Platform And Software, all are provided 'as a Service' and are described as IaaS, PaaS and SaaS respectively. There are also three kinds of cloud type – private, community and public. There are therefore nine categories of cloud-based systems, one for every combination of cloud service and cloud type.

Each cloud service and each cloud type provides a different level of control to the purchasing organisation, which in turn creates a different degree of inherent risk. Each of the nine categories of cloud-based systems therefore comes with a different degree of inherent risk.

This diagram shows that the greatest degree of control, and the lowest level of inherent risk, comes from the leftmost combination: an IaaS cloud service on a private cloud type. Risk increases with each combination moving from left to right, with the highest level of inherent risk coming from a SaaS cloud service provided on a public cloud type.

By using this simple diagram, organisations can quickly determine the inherent risk associated with the cloud-based system being put in place and understand the associated risks to information subject to privacy regulation (known as personally identifiable information or PII).



Solving the challenges of putting PII in the cloud

The ISF ***Data Privacy in the Cloud*** report addresses many of the issues that arise when information subject to privacy regulations moves into the cloud, including:

- Cloud risk is seen to be complicated
- BYOC (bring your own cloud) enables people to bypass organisational safeguards; and they are often unaware of the risks associated with putting PII in the cloud
- Locations of information are unclear, potentially triggering additional regulatory requirements or causing a breach of compliance
- PII can mix with other organisations' information
- PII can continue to be held by cloud providers after contract termination
- Cloud providers can use PII for their own purposes
- PII requirements are not always well defined in the contract
- Standard uses and policies for cloud services are not always defined in the organisation's security architecture.

Key findings

1. Cloud systems are here, and organisations are using them.
2. The risk of putting private data in the cloud is not always considered or addressed.
3. The cloud can be suitable for PII.
4. Cloud complexity can be made simple.
5. Privacy obligations are the same for both cloud and non cloud-based systems.
6. The ISF Privacy Framework can be used to manage the risk of placing PII in the cloud.

Recommendations

The movement of PII into the cloud provides an opportunity for the information security function to work closely with business units to enable agility while maintaining compliance.

By following the recommendations below, information security can enable the use of cloud services for PII, ensuring the organisation understands the risks and either puts in adequate safeguards or accepts them.

For any cloud-based system being considered for PII:

1. Use the "Effect of cloud architecture on ability to protect PII" diagram in the ***Data Privacy in the Cloud*** report to quickly classify the cloud-based system being considered and determine its degree of inherent risk.
2. Use the ISF ***Privacy Framework*** and related actions to update existing privacy risk assessments, methodologies, policies and procedures.
3. Use the ISF ***Securing the Supply Chain*** suite to embed the processes for assessing and managing PII risk in the cloud into the procurement and vendor management lifecycle.

Action

Where next?

The ***Data Privacy in the Cloud*** report helps organisations to manage the regulatory and information risk of using cloud services for private data, by:

- demonstrating why data privacy in the cloud is a business issue
- explaining data privacy
- de-mystifying the complexity of cloud-based systems and their inherent risks, enabling privacy safeguards to be put in place
- enhancing the existing ISF Privacy Framework to address cloud-based privacy issues and determine the actions required of an organisation.

Input for the report was gathered from workshops and meetings with ISF Members around the world, interviews with subject matter experts including privacy commissioners from a variety of countries, Member case studies and thought leadership provided by the ISF Global Team.

The report is supported by an implementation space on the ISF Member website, ***ISF Live***, which contains a facilitated forum for Members to discuss related issues and solutions, along with additional resources including a webcast and presentations.

Data Privacy in the Cloud is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members can purchase the report by contacting Steve Durbin at steve.durbin@securityforum.org.

About the ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Contacts

For further information contact:
Steve Durbin, Managing Director
UK Tel: +44 (0)20 7213 1745
US Tel: +1 (347) 767 6772
Fax: +44 (0)20 7213 4813
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

Disclaimer

