Four steps to improving cloud security and compliance

Despite the widespread proliferation of cloud computing, IT decision makers still express major concerns about security, compliance, and risk management. Nearly 50% of respondents to the 2014 Future of Cloud Computing Survey cited security as the No. 1 concern that would inhibit deployments. The next two greatest inhibitors were privacy and compliance, each cited by more than 30% of the 1,358 respondents.¹

There are a number of ways that organisations can improve their level of comfort in working with a cloud services provider, whether for hybrid cloud, Infrastructure as a Service, Platform as a Service, or other types of deployments. Companies can be far more circumspect in examining the security capabilities of their cloud services providers, and they can insist on the highest levels of certification, such as ISO 27001.

But just focusing on your cloud supplier and its certifications won’t be enough to ensure your comfort and protection. There are many examples of companies doing the utmost in due diligence and certification compliance, yet they still suffer from attacks and data breaches with serious consequences.

The reality is that each company is ultimately responsible for protecting its own data and brand, so it must assume a good portion of the responsibility and control of security and compliance in dealing with cloud providers. Simply put: You should not fully outsource your cloud security.

At the very least, you should consider security and compliance to be a shared responsibility with cloud providers, and you should ensure that your organisation is accountable and actively engaged in defining policy and processes, with proper reporting to provide the oversight to reduce risk.

A good way forward is to ensure that the cloud provider understands your strategic requirements for applications and workloads, and how you plan to govern policy and process to reduce risk. The best approach to ensuring security and compliance with regulatory requirements is a collaborative partnership.

What does it take to ensure a collaborative and strategic approach to security governance, risk management, and compliance in the cloud? The following are four of the most important steps your organisation can take:

**Step No. 1: Conduct an internal assessment**
Loss of control and lack of visibility are two of the primary concerns that organisations express most often in moving to a cloud-based platform. But the challenges typically start internally, without clearly defined controls and visibility within the organisation.

Dimension Data has worked with a wide range of companies deploying the full gamut of cloud models. One of the lessons we’ve learned is that there is a wide gap between mature organisations with well-defined policies and processes related to acceptable risk, versus companies that are less mature in their approach.

Companies without processes and policies have more work to do before they can confidently address challenges of securing data and applications in the cloud.

As an organisation, you can begin to address these challenges by assessing what you are doing, why you are doing it, what kinds of challenges you anticipate, and what outcomes you expect. You must understand not only what you are doing, but also the context of why you are doing it. In using cloud services, key questions to ask of your organisation are:

- What is the business rationale for selecting cloud as a delivery model for specific applications and workloads?
- Which services will be placed in the cloud, and what are the expected outcomes? Has the organisation done a thorough cost analysis, does it know which areas of the business will be positively affected, and does it have clearly defined business goals?
- What data is the organisation potentially exposing in the applications moving to the cloud? Assuming the reward outweighs the risk, what can be done to mitigate risk?
- As the organisation adopts new technologies, such as the Internet of things, big data analytics, or mobility, how much risk is the business willing to assume to derive the associated benefits?

**Step No. 2: Determine your security maturity and risk appetite**
After the internal assessment phase, organisations have a better idea of their security maturity. The next step is to understand the risks and how much risk the organisation is willing to take. Then you are ready to work with your
cloud provider to eliminate or mitigate associated risks.

The discovery and follow-on discussion with your cloud provider will give you a good idea of what you can expect. Here are some areas that should be explored:

- **Compliance requirements:** There are compliance requirements that apply to all businesses, ranging from financial reporting to security aspects of the specific data centres you are using. There are also industry-specific compliance requirements that address issues around data protection, such as HIPAA in healthcare or Dodd-Frank in finance. Which of these apply to the applications you are planning to move to the cloud?

- **Business demands:** Core systems and applications moving to the cloud will dictate service levels. Can you address your risk tolerance and achieve service levels required by the business? How will the cloud provider enable your organisation to meet obligations such as audits, contracts, standards, and certifications?

- **The impact of data loss:** With a thorough understanding of which data you need to protect and where you need to protect it, you can work with your cloud provider on a collaborative strategy to ensure protection at all points—at rest and in transit between the data centre and the cloud, for example. The financial impact of data loss is significant: One study puts it at $145 for every lost or stolen record containing sensitive and confidential information. But you also have to factor in the damage to brand reputation and customer goodwill, which can be devastating. There’s strong incentive for you and the cloud provider to have an acceptable plan.

### Step No. 3: Choose the right cloud provider

Understanding your goals, level of security maturity and appetite for risk will help you determine what to look for in a cloud provider. There are certainly enough commodity-type suppliers in the market if you are willing to take the risk—and if your organisation doesn’t need any help at all with your approach to governance, compliance, and risk management.

However, as more production workloads move to the cloud and the applications are more complex, most organisations find that they need a cloud provider that is a partner in protection. Today, companies have to recognise that cloud security and compliance are shared responsibilities, and should be looking for partners that can provide:

- **Thought leadership:** You want a partner that can work closely with your organisation to understand your challenges, identify your gaps, and put in place a cloud solution that will ensure that each workload is going to be secure.

- **People on the ground:** Most organisations can benefit from having a trusted security advisor. Not all cloud providers have a team of experts to architect the right environment for mission-critical applications. Select a provider that can surround your cloud applications with custom network, storage, and security solutions. Many providers partner with hundreds of service providers, leading you to integrate and manage the different aspects of your cloud, which introduces risk into the process.

- **Integration and security technologies/expertise:** Security is an ongoing and evolving challenge. Working with a cloud partner gives you an edge in developing a long-term approach to governance, compliance, and risk management. Projects should include hardening your...
systems, ongoing vulnerability management, and quality assurance.

One other important consideration in evaluating a cloud provider: Don’t be afraid to ask questions about its levels of security and infrastructure, including the security technologies it deploys, its network architectures, and its certifications for security and data centre compliance. If you don’t get clear and specific answers, be suspicious. Your suppliers should be open about their own capabilities.

**Step No. 4: Work with your cloud provider to develop a shared responsibility matrix**

Once you’ve selected your security partner, you can move forward together with a shared responsibility matrix. Matrices will vary depending on factors such as the cloud model (public or private); the organisation’s risk profile and maturity level; and the type of applications and workloads moving to the cloud. That’s why it’s important to work with a partner that can deliver on the characteristics cited above: Thought leadership, broad and deep security experience, and integration experience. A shared responsibility matrix could look like this:

### Cloud Security – Shared Responsibility

<table>
<thead>
<tr>
<th><strong>IaaS</strong></th>
<th></th>
<th><strong>PaaS</strong></th>
<th></th>
<th><strong>SaaS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td></td>
<td>Applications</td>
<td></td>
<td>Applications</td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td>Data</td>
<td></td>
<td>Data</td>
</tr>
<tr>
<td>Runtime</td>
<td></td>
<td>Runtime</td>
<td></td>
<td>Runtime</td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
<td>Middleware</td>
<td></td>
<td>Middleware</td>
</tr>
<tr>
<td>O/S</td>
<td></td>
<td>O/S</td>
<td></td>
<td>O/S</td>
</tr>
<tr>
<td>Virtualisation</td>
<td></td>
<td>Virtualisation</td>
<td></td>
<td>Virtualisation</td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td>Servers</td>
<td></td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td>Storage</td>
<td></td>
<td>Storage</td>
</tr>
<tr>
<td>Networking</td>
<td></td>
<td>Networking</td>
<td></td>
<td>Networking</td>
</tr>
</tbody>
</table>
Recognising that success in the cloud requires a shared responsibility model, and putting together a framework and matrix to outline how that works, is a key step in forging a long-term partnership. Other key elements include:

- **Continued evolution**, by working together to adopt a strategy for governance, risk management and compliance, and conducting the necessary due diligence along the cloud journey.
- **Increased visibility of controls** to support and address your unique business requirements.
- **Thought leadership**, providing guidance based on best practices.
- **On-site support** with a physical presence and bespoke solutions.

### Taking the next step

Cloud computing presents a great opportunity for organisations to be more competitive, grow at a lower cost and innovate to benefit customers, employees, partners, and shareholders. More production workloads are destined for the cloud, including critical applications and core systems. Security and compliance are concerns that organisations must address if they are to feel confident in expanding their use of public, private, and hybrid cloud environments.

Understanding your organisation’s tolerance for risk and its vulnerabilities is key to choosing applications for the cloud. Choose cloud providers that can operate in a true shared-responsibility model as a rule, not an exception, combined with thought leadership, on-site support, and a team of professionals to help you every step of the way.

Dimension Data is one of a few cloud providers with a managed security practice, used to advising risk-conscious companies. Dimension Data is where you are, in more than 50 countries around the world. For companies moving mission-critical applications to the cloud, Dimension Data is a full service provider and the Dimension Data Cloud Surround™ provides storage, network, and security solutions for consistent successful outcomes. With more than 6,000 clients across all industry segments, we are hands-on experts so you can be hands-free users of cloud.