Information Assurance
Consulting Services

Practical guide to secure cloud adoption

Keeping applications and data safe when migrating them to the cloud can be challenging, but it's not impossible. You need to know your exact requirements, why you're migrating, and a clear idea of how the solution should be designed and delivered to reduce risk and maximise ROI.

Plenty of organisations now benefit from applications delivered via the cloud. Yet the majority of these are relatively simple software as a service (SaaS) applications where the Cloud Service Provider (CSP) manages the infrastructure and application stack.

When it comes to migrating core applications and data to the cloud, the consumer assumes much more responsibility for configuring and securing those applications and data – unless of course, they are taking it as a managed service. Even under the latter, the consumer is still responsible for defining the requirement and ensuring their suppliers design and deliver the platform properly.

The benefits of migrating to the cloud are well documented. Moving bigger, more expensive application environments can mean massive savings in terms of air con, power, cabling, rack and data centre space. Unfortunately, there's also been a lot of focus on the associated complexity, cost and risk, which has meant organisations have remained reticent.

Nevertheless, there are technology products, services and processes available in the market today to address the vast majority of cloud concerns. Migrating core applications is not that risky if you know what you are doing, engage the right people to support you and specify the right solution set.

Getting started

The first step for any organisation looking to benefit from cloud computing is to gain a true understanding of its requirement. Rather than just earmarking an application or system, you need to know exactly what that application environment is comprised of at an estate level, the business functions it serves and anticipated benefits in migrating it (or part of it) to the cloud. You also need to know the level of information security required. This includes how many servers and devices there are, and the LAN-based security applications and appliances needed – such as anti virus (AV) and anti malware, firewalls, intrusion prevention systems (IPS), load balancers, patching, protocols, and security information and event management (SIEM).

Information Assurance Consulting Services

Practical guide to secure cloud adoption

Approaching suppliers with a generic list of requirements and saying 'I don't know what I need, help me…' will almost certainly result in a large quotation with a complex technology solution, lengthy project timeline and a huge bill for consultancy. To avoid this, it's vital to be clear on the project scope by defining no more than five objectives or reasons why.

For example, the application or system identified is not mission-critical, so issues encountered during a migration could be tolerated. Or perhaps the current operating system (OS) running the application or system is coming out of support, providing a good opportunity to install a newer version and virtualise it.

Once you've identified your key objectives or reasons why the planned migration makes sense, list no more than five key security concerns or reasons as to why not. Taking the time to understand the arguments for and against enables you to address issues and overcome stakeholder concerns.

It is also vital to review your reasons objectively and be absolutely certain that they are directly related to the project scope, as practical experience shows that 80% of risk is actually related to generic information security and IT, with only 20% related directly to cloud issues or industry-specific threats.

Keeping it simple

To understand your risk, you need to assess the criticality of the data held on your assets and undertake a threat modelling exercise. Both of these processes can entail a great deal of complexity in terms of threat modelling, information security frameworks, and cost versus risk formulas that lead to a solution design of such technical granularity that cloud migration projects slow to a crawl.

Fortunately, these processes don't have to be complex if you keep it simple. For threat modelling, there are a number of systems and sources available that allow you to understand the specific threats to your industry. The Cloud Security Alliance (CSA) for example, publishes 'The Notorious Nine' report on cloud computing top threats, while PwC's annual Global State of Information Security Survey splits findings by threat type, source of incident and reported losses.

Harnessing these freely available sources of information enables you to not only assess the threats that your organisation is exposed to and better understand where your risks come from, but also to understand the threat posed to the application environment you are looking to migrate.

There are also several information security frameworks that you may need to follow. ISO 21007 is the high-level framework addressing information security managements systems. There's also much more detailed frameworks for ensuring compliance with regulation such as the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS isn't directly related to cloud, but it is relevant if the applications you are migrating will be processing cardholder details or financial transactions. Likewise, the CSA's Cloud Controls Matrix (CCM) provides a controls framework that gives a detailed understanding of security concepts and principles aligned to guidance in 13 domains.

CCM is a comprehensive and robust framework with 400 or so controls. But as with the others, it's quite complex and all of them will take you a long time to follow when in actual fact, information security in the cloud doesn't have to be this complicated – there is a much simpler way.

Information Assurance Consulting Services

Practical guide to secure cloud adoption

Applying the 80 / 20 principle

In the context of cloud security, the 80 / 20 principle means grouping similar assets and applying the same level of security instead of spending time and money on varying levels of security hardening guidelines, software, policies and processes that invariably ends up increasing complexity (and thus cost and risk).

The importance of applying the 80 / 20 principle becomes apparent when performing threat modelling because, as stated previously, you will find that 80% of the risk you are exposed to within a cloud environment is the same as that in conventional physical IT environments. The remaining 20% of the risk will be specific to your application and can be drawn out by using threat modelling and the aforementioned sources to look at what has happened previously in your industry.

Approaching information security in the cloud using the 80 / 20 principle allows you to make decisions that avoid complexity, such as how you assess your levels of criticality. One of the key challenges with this process is that traditional security models have proved too complex to be practical.

Data classification is a prime example. The concept is that you classify the various data on a server as low, medium or high and then apply the appropriate level of controls – such as how that data can be run, how it is secured when at rest and how it is transmitted securely.

The trouble with data classification is that it's far too complex, so nobody does it. Typically, there will be multiple levels of classification on one server, thus the corresponding multiple levels of controls results in increased complexity, increased cost, greater management overhead and a much higher probability that someone at some point will make a mistake.

Taking a uniform approach

Although it can be important to classify data, it should be implemented at asset level at an absolute minimum. To make information security even simpler, why not take data classification up a level again, to the application estate? Because at the asset level, you might have 15 applications you migrate to the cloud with different levels of criticality and controls and still end up with different levels of controls for each.

Take patching as an example, which is typically applied according to criticality. Patches are applied immediately to highly critical assets, monthly for medium criticality assets, and every six months for low criticality assets. If you just had one rule for patching and apply it across the estate at the right time, you free up resources to focus on ensuring patches are tested properly first.

After tests are completed successfully, patching can then be applied automatically. Windows Server has this capability once a patch is approved. This way, patching becomes a one size fits all model and there's no complexity and potential for mistakes.

The same applies to your application environment. If you have 15 servers or devices, five of which you put in the cloud and ten you keep on physical infrastructure, some of the challenges encountered will be in running a mixed mode environment. With cloud you have virtual switches and firewalls, a guest network within the cloud platform and virtual machines (VMs). The way this software and technology works will impact how your traditional infrastructure functions.

For example, OS templates for hardening VMs cannot be deployed automatically on physical servers. This additional complexity overhead increases your risk of a mistake or something not working properly. This is not to say you can't run a mixed environment, but if you are going to do it, you have to think about the added complexity it entails. However, it could be argued that it's better to run each application estate as a unified environment (cloud or physical), or migrate each application one at a time rather than attempting a mixed mode deployment.

Information Assurance Consulting Services

Practical guide to secure cloud adoption

Moving faster

With information security and IT there are many inter-related aspects. Whilst it is important to consider all of them, by making the right decisions it's possible to positively impact the indirect aspects. This is the case with criticality. Often you will find stakeholders arguing that the complexity and the cost are too high. But in practice, by keeping things simple and classifying assets at an estate level, there will only be several technology items to acquire. Costs can be justified by focusing on delivering the business benefits, ensuring rapid time to market, and maximising return on investment (ROI).

Covering 80% of your traditional risk at the outset of a cloud migration project and focusing your time and money on mitigating the 20% of risk directly associated with cloud ensures a faster migration and time to market. The only area to address is the delta between what you have done and what is specific to your application (the risks identified with threat modelling).

Consider a market analysis application estate that includes 15 individual assets. If that application is feeding important data to another application to make trades, then the confidentiality, integrity and availability (CIA) of that data are much higher. The requirements you identify here are critical – i.e. the information has to be 100% guaranteed integrity when it reaches the destination, and it has to be available within a certain timeframe (milliseconds).

Specify, engage, and demand

Having applied the 80 / 20 principle to arrive at a solid scope identifying the application estate to migrate, criticality and risk, specifying the right architecture and solution set in the cloud stack is relatively easy. There is an element of associated cost, but it relates to ensuring you have the right compute and storage capacity. Here, the 'Chaos Monkey' model can help, whereby you spin up VMs for an hour, transfer the application or system you are running onto that VM, hypervisor or stack, and then shut down the original host to expose your cloud environment to any sort of attack or risk.

At this point, you are also ready to commence informal conversations with suppliers. Visit the CSA register to identify approved or certified providers of technologies by category and rating. Some will have been assessed by advanced auditors (such as IACS) and achieved Platinum or Gold status. This resource enables you to select a small number that you want to engage with based on their experience and maturity level.

The premise of the methodology discussed in this guide is to get you to the point where you are ready to start talking about technology or engaging an external advisor. Crucially, you are now equipped with the right level of knowledge to ensure a rapid implementation. Armed with this approach, you can now be assertive in the articulation of your requirement, and confident in the fact you will have a robust cloud-enabled environment supporting your strategic goals.

If you would like to find out more about keeping cloud migrations simple I will be presenting at **CSA Congress EMEA 2015 in Berlin.** Join me on **16 November** to learn how to develop a pragmatic game plan for secure cloud adoption.

If you can't make it, enter your email address *here* for a copy of my presentation.