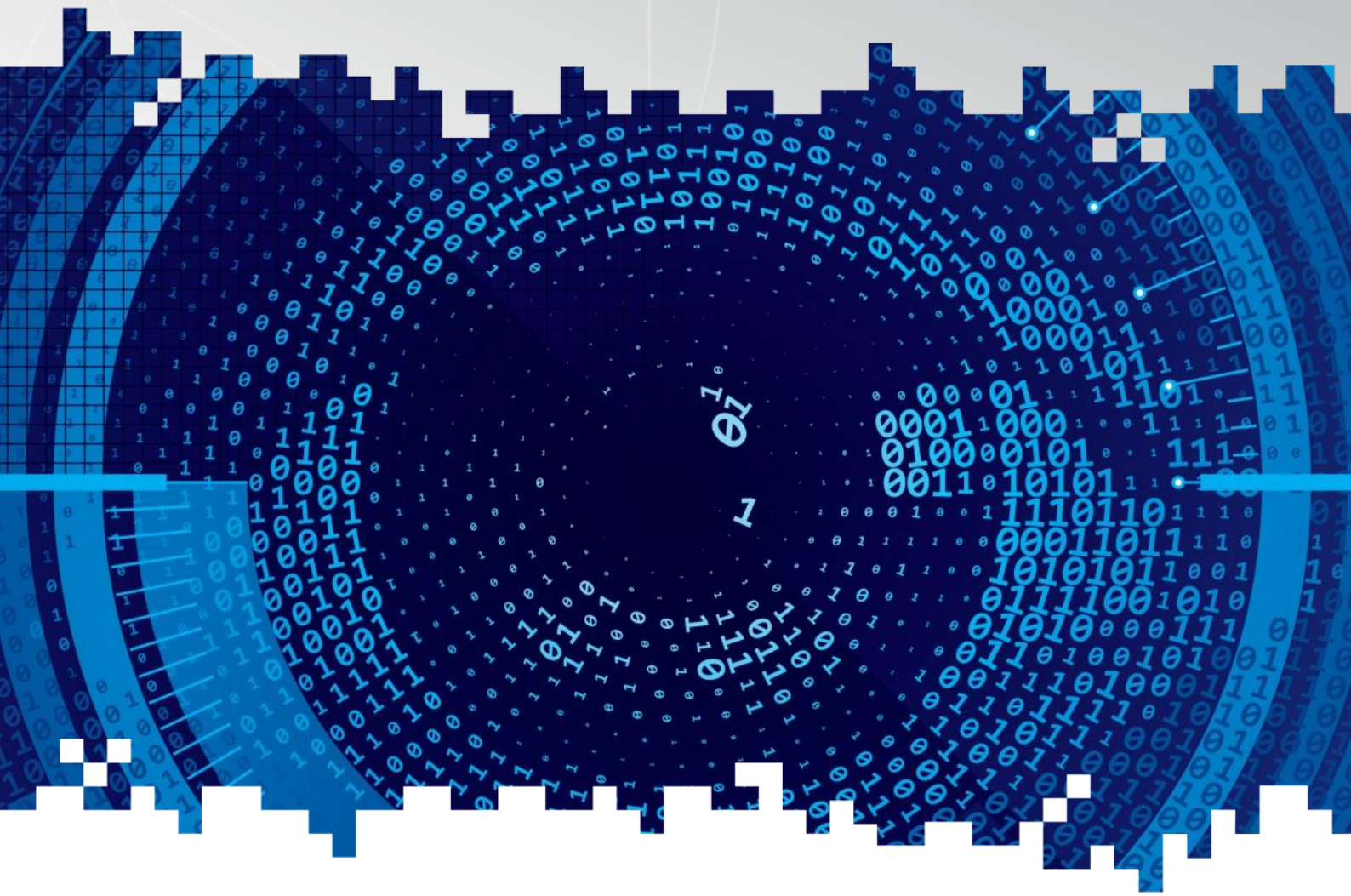
Achieving the **Benefits of Cloud Services Above OFFICIAL**

Version1-0

August 2018



Leonardo
Sigma House, Christopher Martin Road, Basildon, Essex, SS14 3EL, United Kingdom
Telephone: +44 (0)1268 823400 Fax: +44 (0)1268 823490 www.leonardocompany.com

Registered in England No. 2426132
Registered Office: As above

1 INTRODUCTION

Organisations are transitioning to Cloud Services (defined below) in order to take advantage of the wide range of benefits that they offer. Historically this transition has been for information at lower sensitivity, and within HMG environments this has been at the OFFICIAL Tier. Her Majesty's' Government (HMG) conducts significant business above OFFICIAL and whilst Cloud offerings exist which claim to be "accreditable" at above OFFICIAL, the transition to Cloud Services at higher classifications has been slow and is hampered by concerns over security.

Fundamentally, the risks associated with Cloud Architectures are different to those for on-premise solutions and a different approach to the implementation of security controls and risk management is required[1]. There is no reason why transition to cloud services at above OFFICIAL necessarily requires an increase in organisational risk appetite. By understanding how to address the specific challenges that Cloud Services at above OFFICIAL present, and implementing an appropriate set of controls allowing Security Accreditation to be achieved, organisations can take advantage of the cost and functionality benefits provided by cloud computing at higher classifications.

1.1 What do we mean by Cloud Services?

There are a range of cloud service options available[1] but the focus of this paper is on Infrastructure as a Service (IaaS). Although the concept of 'cloud' has been muddied in recent times, this paper looks at true cloud as defined by National Institute of Standards and Technology (NIST) using the essential characteristics of the cloud computing model[2]:

a. **On-demand self-service.** Ability to provision resources automatically.

b. **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms.

c. **Resource pooling.** Computing resources serve multiple consumers.

d. **Rapid elasticity.** Capabilities can be provisioned and released to meet demand.

e. **Measured service.** Automatic control and optimisation of resource use.

The assumption is that at higher classifications, a Community Cloud model will be adopted, whereby a Cloud Service is only offered to government departments or other equivalent organisations working at the classification of interest.

1.2 Opportunities offered by Cloud Services above OFFICIAL

The business benefits of Cloud Services at OFFICIAL and at unclassified have driven their widespread adoption in both Government and Industry, and the same benefits can be realised at higher Classifications. These include:

[1] https://www.ncsc.gov.uk/blog-post/my-cloud-isnt-castle

[2] NIST Special Publication 800-145

a. **Scalability and Flexibility**. The ability to provision or reduce capacity based on demands and meet operational requirements; and the ability to "port" services to new providers rapidly if requirements are not being met or other providers offer significant benefits.

b. **Evergreen**. Take advantage of the latest technologies, both in terms of security and business functionality.

c. **Agility and Speed of Adoption**. The ability to rapidly stand up and tear down services in an Agile manner to meet the needs of projects.

d. **Collaboration**. Increased ability to work collaboratively compared to standalone, stove-piped solutions.

e. **Cost**. Move away from high cost, bespoke, legacy hosting contracts.

2 CHALLENGES OF DELIVERING CLOUD SERVICES ABOVE OFFICIAL

SECRET services are exposed to a very different threat landscape compared to OFFICIAL services. Some of the characteristics of Cloud Services which would allow the associated business benefits to be delivered result in a set of security challenges which themselves caused the adoption of Cloud Services at higher classifications to be overly limited. This then reduces the benefits realisation. These challenges include:

a. **Threat Level and Capability.** At SECRET, the threat model includes threat actors with the ability to bypass many commercial grade static security controls, in a way that potentially negates controls used in traditional cloud environments. In addition, when sharing infrastructure and services, customers inherit threats from other organisations. This could mean that organisations which wouldn't ordinarily be associated to the same threat groups, will share a threat landscape.

b. **Segregation between Customers.** Shared services offer a range of benefits however there are associated risks due to the capability of threat actors to execute highly complex attacks which breach segregation controls. Whilst it is likely that only certain customers will be permitted to use Cloud services, and that the level of security around co-located services will be regulated by robust risk management procedures, the risks associated with the use of shared infrastructure and services need to be understood, mitigated and managed.

c. **Administration and Solution Support.** Cloud services have a shared responsibility model outlining the division of responsibility between each service provider and the customer. Some aspects of the infrastructure will be managed and maintained by cloud service providers and this leads to service providers presenting a potential risk to customer services.

d. **Security Assurance Levels.** Much of the assurance around high classification systems revolves around the use of assured products at the appropriate level. In many cases, these products will not be available in a virtualised cloud environment and therefore security controls must compensate for this lack of external assurance.

3 DELIVERING SECURE CLOUD SERVICES ABOVE OFFICIAL

The challenges outlined above can be addressed through the application of good security practise in the following areas:

a. **Risk and Information Management,**

b. **Security Architecture,**

c. **Security Engineering,**

d. **Security Monitoring.**

Through application of a layered approach of the key principles governing the above areas, the challenges identified above can be addressed, allowing risks to be reduced to acceptable levels. Leonardo believes that, done properly, Cloud Services can deliver higher levels of security and lower residual risk than traditional on-premise solutions in many cases. Each case requires distinct and specific investigation to make the case for transition to Cloud Services or remaining and improving the On-Premise provision.

1.3 Risk and Information Management

Risk Management in Cloud Environments is different to traditional on-premise systems and the approach must reflect this. The use of cloud services to host information and services above OFFICIAL does not present more risks; rather it presents a set of different risks than those associated with traditional IT infrastructure, and those risks are managed in different ways.

To address the capability of the threat actors, there is a need for a more robust risk management regime at the Cloud Service Provider level to provide assurance that risks associated with shared infrastructure are managed. This requires a higher level of transparency relating to risk appetite and risk acceptance than would be necessary in lower classification environments, and in particular around the application of the required security standards by co-hosted customers.

It is also necessary to understand what information services hold and how is it processed, at a more granular level than for on-premise solutions. This can help inform whether an entire system should be migrated to the cloud or only certain elements, the approach to security monitoring, and targeting of security architecture controls.

1.4 Security Architecture

The security architecture of cloud-based solutions is not simply a replica of on-premise solutions transferred to the Cloud. Security Architectures need to be developed which take into account the characteristics of Cloud Services, and in particular architectures must meet the specific challenges at higher classifications. Examples include:

a. **Data separation.** Robust architectures must be in place to ensure separation between customers and data, both between and within environments. Due to the level of threat and the ability to use High Grade products, these architectures should make use of layers of controls with multiple products, and should implement robust security engineering. This will, combined with targeted security monitoring, provide assurance that segregation controls are effective.

b. **Security Monitoring and Audit solutions.** A robust audit and monitoring architecture needs to be implemented, backed up by robust Security Monitoring. Crucially, the audit solution should be segregated appropriately and privilege management must be implemented so that access to the audit solution is limited.

c. **Privileged Access Management.** Privileged accounts have the capability to bypass security controls. Privileged capabilities must be segregated such that a single compromise does not allow all controls to be bypassed.

d. **Encryption Management.** Use of encryption can provide assurance that Cloud Service Providers cannot access customer information, and that a compromise of multiple systems would be required to access sensitive information. The architecture of key management must be tailored to the specific service, for example holding keys on separate systems.

1.5 Security Engineering

Combined with robust security architecture and rigorous monitoring, implementing good security engineering provides assurance that exploits are not available to an adversary. This has been given less importance in on-premise solutions where the assurance provided by an air-gap is often relied upon. In Cloud solutions at higher classifications, there needs to be assurance that each security control is implemented in as robust a fashion as possible, and that each layer of controls complements the next in terms of the way in which the control is engineered to deliver the specific security enforcing functionality required.

1.6 Proactive and Effective Security Monitoring

Security monitoring takes on increased importance in Cloud Services at higher Classifications. Robust security monitoring at both the Cloud Service Provider level and the Customer tenant will provide assurance that the specific threats to SECRET cloud services are managed appropriately.

The Cloud Service Provider needs to be able to actively demonstrate there is no unusual activity on the Cloud Platform, which would be indicative of complex attacks. Careful monitoring including heuristic analysis will also provide early indication of compromise of a tenant prior to any breakout to the underlying Cloud Platform. Passive and reactive security monitoring is not sufficient; monitoring must be proactive and change as the threat and environment evolve. Analysts should be actively hunting for threats and targeting specific attack paths and compromise methods, to actively provide assurance that exploits are not occurring and have not occurred.

A similar level of security monitoring is needed for each customer; it is critical that no customer presents a weak link. Assurance that this is the case is part of the robust risk management approach at both the Cloud Service provider and customer level.

4 UKCLOUDX SECRET CLOUD SOLUTION

UKCloudX is exclusively focused on addressing the needs of UK government agencies, by providing an infrastructure that meets the rigorous security requirements required for data at higher security classifications, and that does so at substantially less cost than the current arrangements for this level of sensitivity. It is a result of a significant investment of over £25

million in people, enhanced physical security and a new technology platform which uses higher grade assurance to create a trusted and neutral platform for better collaboration and faster innovation.

At the recent launch of UKCloudX *Simon Hansford, UKCloud's CEO* commented:

> "Capitalising on the same cloud-first approach that has been so successful in accelerating digital transformation and reducing cost across central government, UKCloudX will bring the benefits of cloud computing to bear for secure communications. By harnessing the potential of the cloud to overcome the long lead times, inflexibility and considerable fixed costs that have traditionally hampered secure communications; UKCloudX will enable far greater innovation and collaboration on sensitive projects."

Bernard Brown, vice chairman at KPMG UK, added:

> "Cyber security is a real and growing issue for the UK. As the pace and complexity of cyber-attacks and the threats from nation states are increasing, it is necessary to find new and better ways of working so that we're best able to both respond and pre-empt threats to our sovereign interests. UKCloudX enables government agencies and their UK industry partners to focus on the mission, collaborate more effectively and innovate faster to keep ahead of the threats as they emerge."

Nik Beecher, VP Cyber Security & ICT Solutions at Leonardo Security & Information Systems added:

> "Leonardo has safely handled the most secret data of our UK national and international customers for years. The UKCloudX initiative will provide a highly secure new platform, allowing our clients to benefit from new opportunities offered by the latest, most innovative and secure cloud-based services."

5 CONCLUSION

Delivery of Cloud Services at SECRET presents a challenge when combined with traditional views of security architecture and assurance that is limiting uptake and the realisation of the associated benefits; however there is no reason why organisations cannot make use of cloud services at this level within the current risk appetite, and achieve the associated business benefits.

A combination of good risk and information management, good security architecture, security engineering and security monitoring when combined in a layered approach, can meet the challenges associated with the use of cloud services at SECRET.

Crucially, each of the security controls in place must be backed up by pro-active security monitoring which is based on a thorough assessment of the risks to the service, the attack paths through which those risks can be realised and the attack framework which an adversary would use to potentially deliver an exploit.

The UKCloudX solution delivers the advantages of Cloud Services with the assurance needed to support accreditation above OFFICIAL:

a. **Elasticity.** A genuine public cloud platform can scale to support the most complex UK public sector workloads and enables dynamic auto-scaling

b. **Self-service.** Complete autonomy to provision, change and manage your virtual data centre via the UKCloudX Portal or using our fully documented API

c. **Measured Usage.** True consumption-based pricing

d. **Broad Networking.** Connect via existing government secure networks, such as SLI or HybridConnect, using your own dedicated circuits

e. **Resource Pooling.** Shared with a trusted community of Defence and national security users