G-Cloud

Cloud Spotter's Guide for the UK Public Sector

Contents

Foreword

Back to contents

The UK Public Services Network (PSN) and Government Cloud (G-Cloud) frameworks signaled intent to transition over time to as-a-service consumption models. Since the introduction of these frameworks in 2012, momentum continues to build and there is a growing consensus that the Public Sector can realise significant cost savings through buying IT and digital services in a different way – as metered/managed services (using operational costs) rather than as hardware and software assets (using capital costs).

The impact of the 'cloud' is substantial, and there are great examples of how cloud services are transforming the provision of IT services to the Public Sector. However, the adoption of cloud presents as many challenges for IT departments and cloud service providers as it does opportunities. For example, under the new security classifications there is no mapping with GPMS (and by extension the Impact Levels - IL0, IL2, IL3) and OFFICIAL. Each Public Sector organisation should perform a risk assessment, assess their potential cloud suppliers and ensure that the risks to their information are managed in-line with the risk appetite and the needs of the business. Making an informed decision is of critical importance to make appropriate use of cloud services without compromising the confidentiality, integrity and availability of data.

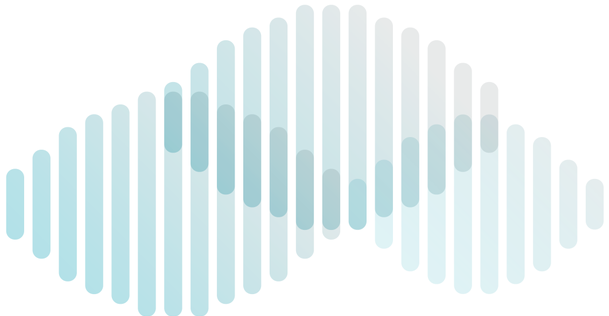
Cisco is increasingly being asked for business and technology advice on how best to plan for, and adopt, cloud services, as one size does not fit all.

This guide offers all Public Sector organisations trusted advice, including the top-ten buying criteria for cloud services. It will help Public Sector buyers develop an appropriate cloud sourcing strategy and confidently select cloud services from approved suppliers on the G-Cloud Framework, which meet both the security needs of end users and the requirements of the business.

So, if you would like to find out more, please contact us. We would be delighted to meet with you, and review the applicability of this guidance for your organisation.

Rod Halstead
Managing Director
Cisco UK Public Sector

What is G-Cloud?



G-Cloud is a UK Government initiative to encourage the adoption of cloud services across the whole of the UK Public Sector. The aim is to simplify how the Public Sector buys and delivers services by creating a marketplace of pay-as-you-go commodity services that can be easily scaled up or down, based on changing needs.

Back to contents

G-Cloud gives Public Sector buyers a framework that allows them to buy cloud-based IT services without having to go through complex tendering and approvals processes.

- It will form the backbone of the 'Cloud First Policy'
- It creates the facility to provide more flexible contractual arrangements for cloud-based services
- The cloud services are innovative and up to date, as the framework is refreshed every 6-9 months
- With the drive to support local businesses, G-Cloud makes it easier for SMEs to sell to the UK Public Sector

The new online catalogue – The Digital Marketplace – presents all the available services in a format that is easy to search.

Opening the Digital Marketplace

Back to contents

The Digital Marketplace is the new home for the whole of the UK Public Sector to buy services from the G-Cloud and Digital Services Frameworks.

The store can be accessed via **digitalmarketplace.service.gov.uk**

The key benefits of the G-Cloud include:

- Everyone in the UK Public Sector can use the service
- Open procurement is already done – there's no need for Official Journal of the European Union (OJEU) or Invitation to Tender, which saves time, resources and money
- There is a vast range of services available, which are continuously updated
- Details of the services, together with terms and pricing, are all listed
- The G-Cloud framework supports the 'Cloud First Policy' so you can access and use cloud-based services in a flexible and agile fashion

How Do You Buy From G-Cloud?

Here's how procurement through the G-Cloud works:

- List the requirements: 'must haves' and 'wants'
- Secure the appropriate internal approval
- Create a longlist of suppliers using a keyword search
- Review service descriptions to determine which services meet your needs
- Choose a shortlist of candidates from the longlist
- Choose a service, award and call-off agreement; call-off duration is limited to no more than 24 months
- Direct award the purchase – no need to go to tender – or review again to ensure best value

The Digital Marketplace will be used for G-Cloud procurements. Remember, purchases are off the peg, so there's no negotiation about what the services include. The terms and conditions and the price are all fixed.

You can find full details of the buying process here:

https://www.gov.uk/government/publications/cloudstore-buyers-guide/cloudstore-buyers-guide--2

Growth of G-Cloud?

All suppliers on the G-Cloud frameworks are required to provide monthly reports of invoiced sales to the Crown Commercial Service (CCS).

These are published on a monthly basis on GOV.UK here:

https://digitalmarketplace.blog.gov.uk/sales-accreditation-information/

Approximately 79% of the total sales to date have been via Lot 4 (Specialist Cloud Service), but there is an increasing trend towards Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) sales across all Public Sector verticals, including Local Government and Healthcare.

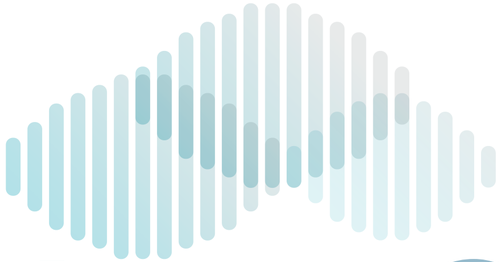
The latest G-Cloud sales figures and statistics are plotted on GOV.UK:

https://www.gov.uk/performance/g-cloud/

Back to contents

UK GOV CLOUD: The Top-Ten Buying Criteria

Here's a simple checklist to use when choosing a supplier of cloud services in the Digital Marketplace:



Understand

the cloud security principles and consult with Public Sector users to determine which of them are the most important, based on how the service will be used

Know

the law on data protection and data sovereignty: where and how will UK Public Sector data be held? Are the G-Cloud providers UK Sovereign, with UK Data Centre facilities and appropriately security-cleared personnel?

Governance

is important to create an initial set of strong ground rules – Service Level Agreements (SLAs). Customers will need full visibility of the services and how they perform for the duration of the contract

Open

standards to ensure that different systems can interoperate with the flexibility to move workloads or switch between suppliers without compatibility problems

Verification

of supplier assertions offers a buyer additional evidence that the service meets a set of cloud security principles. Good examples of independent assurance are ISO27001, CESG PGA, CSA STAR or Cisco's Cloud & Managed Services Programme (CMSP)

Common

multi-tenanted infrastructure can provide significant business convergence and cost benefits. Buyers need to be aware of the security implications of multi-tenancy in order to maintain confidentiality, integrity and availability of information

Location

and supplier independence gives consumers the capability to change any IT services they receive from any particular supplier more easily

On-demand

cloud services can offer elastic resources with reserves of capacity and performance that can flexibly scale up or down to meet changing business demands

Utility

pricing is a key characteristic of cloud services and many can offer pay-per-use terms of engagement; cloud services are delivered as-a-service and there are many different consumption models

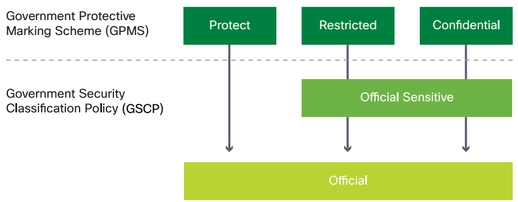
Differentiated

cloud deployment models are offered by suppliers with different levels of assurance to meet the security requirements of consumers - including unassured Public Cloud Services, Hybrid Cloud Services, Assured Community Cloud Services and Accredited Community Cloud Services

Understand the Cloud Security Principles

Security classifications

The UK Government's new OFFICIAL, SECRET and TOP SECRET classifications have made the security assurance process for G-Cloud services simpler. As per the Cabinet Office policy, OFFICIAL-SENSITIVE is not a fourth marking, but is instead intended to be a handling caveat and should not (generally) attract additional technical controls.



Impact Levels should not be used to describe the security properties and accreditation of different services. Instead, in the OFFICIAL tier, the Public Sector has adopted the 14 Cloud Security Principles.

Buyers should be choosing a service that meets their requirements and decide if a higher level of security is required or not using the principle: Assure, Choose, Reuse.

Assure

Suppliers will complete a number of pre-defined security statements asserting how their services meet the Cloud Security Principles.

Choose

Buyers will have greater awareness of the security detail of the services in the Digital Marketplace.

Reuse

Suppliers can use existing supporting security assurance evidence, such as CESG Pan Government Accreditation (PGA) or Public Services Network (PSN) accreditation. If a service has been assured/accredited once by an appropriate authority then Public Sector buyers don't have to do it themselves.

The new process will make it clearer, simpler and faster to find a service on the Digital Marketplace that meets a buyer's requirements.

Back to contents

Knowledge of Data Protection Legislation and Data Sovereignty

Citizens' data privacy is of paramount importance for any government, and there is a concern that data stored outside the country is not subject to the same data privacy laws – the issue of 'Data Sovereignty.'

No matter what type of solution is being employed, the buyer and supplier (cloud provider) share responsibility for compliance with government regulations and policies, such as the UK Government Security Classifications (April 2014) and local law frameworks and acts (e.g. OSA 1989, DPA 1998, FOIA 2000 and PRA 1967).

Data protection legislation applies if personal data is processed in a cloud service. The ICO has published guidance on compliance with the Data Protection Act (DPA) in relation to using cloud services.

It's available here:

https://ico.org.uk/for_organisations/data_protection/the_guide

To safeguard sensitive business/operational data and protect end users and their reputation, cloud service buyers need complete end-to-end security that spans the network and cloud/hosted service environments. In the past, traditional security solutions such as firewalls could protect the network perimeter and provide strong security. However, with hybrid cloud environments, organisations need protection that extends across the UK Public Sector's physical, virtual, and cloud domains.

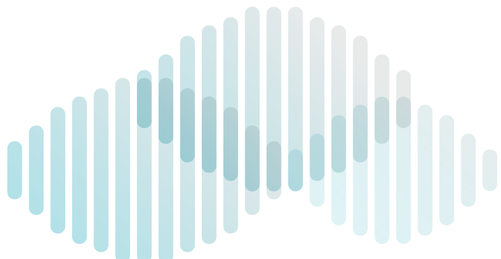
Governance – ‘Expect the Unexpected’

It is important to create an initial set of strong ground rules – Service Level Agreements (SLAs) – with the cloud service provider, which is a process for setting expectations for both parties. It is inevitable that challenges will occur and these exceptions need to be planned for from the start. Good cloud service governance needs to consider the following four requirements:

- **Plan for failures:** SLAs are tools for protecting the stability of a service, outlining the minimum set of service components with corrective actions in the event of a failure, including problem resolution, disaster recovery, change management process and mediation
- **Data ownership:** affirm ownership of data stored within the cloud service and the buyer’s rights to get it back
- **Security assertions:** detail the security controls to be implemented and the buyer’s rights to audit their compliance
- **Portability of the data:** the cost of moving a service and of termination

Open Standards – Vendor Independence

Cloud environments need to interact smoothly across a wide range of network components, applications and services that make up today’s extended enterprise. There’s no reason to be locked into a particular vendor’s solution. That is why Cisco is committed to an open, interoperable, and standards-based approach to the cloud. Cisco’s strategy is to support multiple cloud deployment models, provide choice and flexibility, and meet end user’s business needs.



Verification of Supplier Assertions

On the 30th July 2014, G-Cloud stopped accepting submissions for Pan Government Accreditation (PGA), and a new security approach was introduced. Instead of PGA, suppliers must now deliver assertion statements against the Cloud Security Principles by selecting predefined answers to a range of questions that test if they meet the Cloud Security Principles.

Independent validation offers a buyer additional evidence that the service meets a set of cloud security principles. Suppliers can use existing security-assurance evidence, such as ISO27001, CSA STAR, CESG PGA Accreditation (PGA IL2 and IL3). In addition, Cisco Managed Service Programme (CMSP) is a rigorous certification with third-party audits of cloud services, which ensures that providers align well with ISO27001:2013 and ITIL and thus some of the Cloud Security Principles.

They can also use additional or different supporting approaches, like IT Health Checks, as and when new evidence is available. Accreditation submissions for cloud services connected to the Public Services Network (PSN) will continue to require PGA.

Location and Supplier Independence

What happens when you move from supplier to supplier?

Some departments have a captive relationship with their suppliers and find it difficult to switch providers, because their services are fully outsourced with bespoke and/or legacy components.

Cisco Intercloud Fabric enables application portability between different hypervisors (e.g. VMware, Microsoft, Linux) and between different cloud deployment models (e.g. private and public). Therefore, it gives consumers the capability to change any IT services they receive from any particular supplier more easily. Please refer to Cisco's Cloud Strategy Intercloud section

On Demand

Cloud services can offer elastic resources with reserves of capacity and performance that can flexibly scale up or down to meet changing business demand needs. These flexible service models can cater for short periods of peak demand, allowing for the efficient use of IT resources to lower operating costs and energy use to aid the 'Greening Government' IT agenda.

Utility

Cloud service models are delivered and consumed as-a-service with commercial flexibility and, in most cases, pay-per-use terms of engagement.

Public sector IT departments are moving from being **pure providers to IT brokers** of cloud and managed services that meet the needs of the business.

The optimum type of cloud solution for the buyer may depend on the applications being used; total cost of ownership (TCO), security needs, and Service Level Agreement (SLA) requirements.

The Public Sector buyer may choose to build their own private cloud, build a regional community cloud and offer it 'as-a-service' to other agencies, buy specific Line-of-Business applications (SaaS), select Cisco Powered services from cloud providers, or take a hybrid IT approach and fuse on-premise and cloud resources.

Common (Multi-Tenant and Shared)

Efficiency is another key design principle of cloud services. Cloud providers adopt secure, multi-tenant architectures and share physical infrastructure across several consumers, employing virtualisation technologies to implement robust logical separation.

Buyers need to be aware of security and performance considerations with multi-tenant environments in order to maintain confidentiality, integrity and availability of information. The cloud security **'Principle 3: Separation between consumers'** offers a set of deployment principles that should be observed by end-user organisations. These principles, however, are not rigid and their application will depend on the cloud service model (e.g. IaaS/SaaS), deployment model (e.g. public), an organisation's tolerance of risk, and the level of threat they face.

The following advice may help inform the separation requirements of consumers:

- **Private cloud services:** applies to a single organisation and thus only limited assurance in the separation of the service is likely to be necessary
- **Community cloud services:** if the community is trusted and its members are known to practice a good level of hygiene, it is envisaged that a well-scoped penetration test is likely to offer sufficient assurance
- **Public cloud services:** need to understand the types of consumers sharing the platform, as they may be actively hostile; if a higher level of confidence is needed beyond a penetration test, it may be desirable to gain assurance in the service design, or to choose public cloud services which make use of assured components (e.g. Foundation Grade assured products)

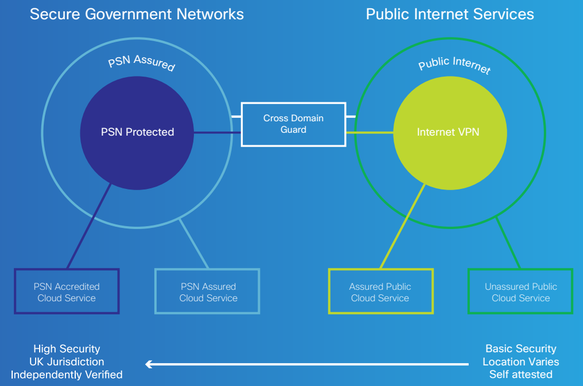
Differentiated Cloud Deployment Models – One Size Does Not Fit All...

Under the new security classifications there is no mapping with GPMS (and by extension the Impact Levels - IL0, IL2, IL3) and OFFICIAL. Each Public Sector organisation should perform a risk assessment, assess their potential cloud suppliers and ensure that the risks to their information are managed in line with the risk appetite and the needs of the business. Making an informed decision is of critical importance to make appropriate use of cloud services without compromising the confidentiality, integrity and availability of UK citizen data.

To help address this, suppliers offer a range of Cloud Deployment Models with different levels of assurance to meet the security requirements of consumers. Some cloud services will provide evidence to satisfy all of the Cloud Security Principles, while others may only be a subset. However, a large number of cloud services will be self-attested with no independent validation or auditing of controls.

Cloud Deployment Models are of critical importance to the Public Sector and link together the Public Services Network (PSN) and G-Cloud programmes in a very direct way. Each deployment model is associated with particular security characteristics that dictate which applications and services may run over them:

Cloud Deployment Models within the UK Public Sector



Back to contents

Accredited Cloud Services

These are Community Cloud Services that have a direct, resilient connection to Government Secure Networks protected by cryptographic overlays like the 'PSN Protected Tier'. Some cloud service providers have achieved CESG PGA IL3 accreditation already and they are listed here.

Assured Cloud Services

These are Community Cloud Services that have a direct, resilient connection to Government Networks like the PSN 'Assured Tier'. Some cloud service providers have achieved CESG PGA accreditation already.

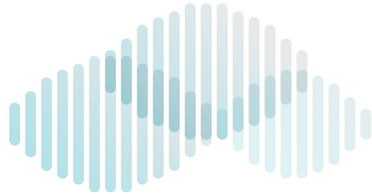
Assured Public Cloud Services

These are Public Cloud Services that are directly connected to the Internet and have self-asserted their compliance with the Cloud Security Principles. However, some providers may have achieved CESG PGA accreditation already.

Unassured Public Cloud Services

These are Public Cloud Services that are directly connected to the Internet and have not been assured or independently validated by a recognised authority.

The Public Sector is already procuring various types of cloud platforms, but the selection is based on the customer's use cases. Each case helps to define which of the Cloud Security Principles are important, and what controls will be necessary to protect data assets.



Typical Characteristics of UK Public Sector Cloud Deployment Models

NIST Cloud Deployment Model	Independent Verification	Network Connection	Evidence of Assertions	Vetting of Staff	UK Jurisdiction	Protective Monitoring	Aligns with Cloud Security Principles
Public	Unassured	Direct Internet	Self Asserted	Varies	Varies	No	SOME
Public	Assured	Direct Internet	UKAS ISO27001	Varies	Varies	Commercial Best Practice	SOME
Private	Unassured	Private circuit	Self Asserted	Varies	Likely UK	No	SOME
Private	Assured	Private circuit (CAS-T)	UKAS ISO27001	BPSS	Likely UK	Commercial Best Practice	MOST
Community	Assured (ex PGA IL2)	PSN Assured Tier	PSN Accreditation	BPSS	Operate within UK	CESG GPG13	MOST
Community	Accredited (ex PGA IL3)	PSN Protected Tier	PSN Accreditation	SC Cleared	Operate within UK	CESG GPG13	ALL

BPSS Baseline Personnel Security Standard
SC Hosted Collaboration Solution
CAS-T CESG Assured Service (Telecoms)

GPG13 Good Practice Guide No. 13 – Protective Monitoring for HMG ICT Systems
UKAS United Kingdom Accreditation Service

Back to contents

Hybrid Cloud

The term Hybrid Cloud describes a scenario where two or more Cloud Deployments Models are combined. They remain unique entities, but are bound together by technology that enables data and application portability between them.

According to a Cisco study, in partnership with Intel, 76% of respondents believe that IT will act as a broker, or intermediary, of cloud services, orchestrating the planning and procurement process for Public Sector client agencies across private and public clouds. Effectively, they will be creating a Hybrid Cloud.

Cisco is building the platform that connects multiple types of clouds to form the Intercloud. The Intercloud enables end customers, partners, and service providers to build secure, hybrid-ready cloud services.

Cisco's Cloud Vision: The Intercloud

The Internet of Everything (IoE) is bringing together people, processes, data, and things to make networked connections more relevant and valuable than ever before. These days, Public Sector organisations need computing models that are able to cope with dramatic exponential growth.

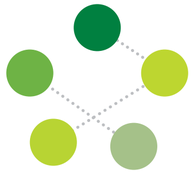
Thirty years ago, Cisco pioneered a strategy to connect previously isolated, heterogeneous networks, which led to the rise of the Internet as we know it. Now, Cisco is embarking on a journey just as ambitious: the connection of multiple, isolated clouds, leading to the creation of the Intercloud – an interconnected cloud of clouds.

Back to contents

The Intercloud

Internet

World of isolated networks



Using a multitude of protocols

The Internet

IP based

Open standards

Intercloud

World of isolated clouds

Built using customised cloud infrastructure and services

Each cloud is custom built with no consistent APIs

The Intercloud

- Web-scale architecture
- API driven automation
- Open, secure, hybrid

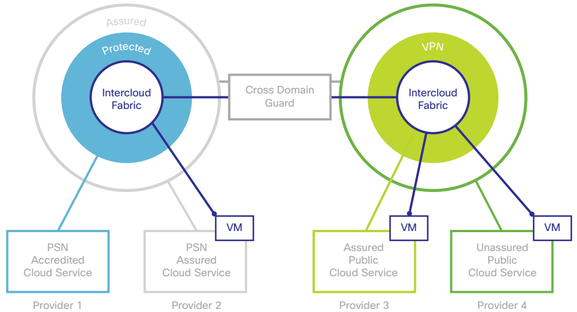
Cisco does this by enabling businesses and cloud providers to build hybrid-ready private clouds, by providing ready-to-consume public cloud services, and by enabling secure workload migration across public and private clouds, through the Cisco Intercloud suite of connective products.

This strategy enables organisations to increase ROI, reduce TCO, lower risk, and enable business agility by using the increased efficiency, automation and management capabilities, enhanced security, transformative potential, and innovation edge that the Cisco cloud solutions, services, and partner ecosystem can provide.

As the line separating the different cloud environments continues to fade, it is becoming clear that:

- Hybrid Cloud, and more broadly hybrid IT (inclusive of traditional on-premises IT applications), are the new normal
- The ability to move cloud workloads across heterogeneous environments, with consistent network and security policies, is a key foundation for long-term, industrialised consumption of cloud services

Hybrid Cloud Environment



The brokerage of IT services and cloud services becomes a core IT capability. Increased brokerage activity will lead to a 'marketplace' for cloud offerings.

Intercloud is very much about creating an open marketplace for cloud services, giving customers the choice to initiate and move their workloads easily between providers. Therefore, the Intercloud construct will support initiatives like the G-Cloud and the Digital Marketplace.

Back to contents

The Cloud Standard: Cisco Powered Cloud Services

Partners participating in Cisco's Cloud and Managed Services Programme (CMSP) must meet various Cisco requirements to prove the ability to develop, deliver, manage, and support Cisco-based cloud and managed service solutions. CMSP partners have demonstrated IT Infrastructure Library (ITIL) Foundation processes, practices, and tools to support Cisco technologies at all lifecycle phases.

Cisco Powered cloud services give our customers more choice in the way they buy and use Cisco infrastructure and solutions in a cloud format. Cisco's cloud services offer a host of attributes that include global availability, reliability, sustainability and scalability.

Cisco Powered cloud services are based on validated design architectures and partner and service certifications that deliver faster time-to-value, assured performance and continuous innovation. This validated end-to-end architecture allows for the effective delivery of customer Service Level Agreements (SLAs), which are important when making the transition to cloud.

cisco Powered

The benefits of Cisco Powered cloud services

The Cisco Powered portfolio brings together everything needed for a successful cloud strategy:

- The assured performance of Cisco Powered services enables organisations to connect with confidence; Cisco partners undergo rigorous certification and a third-party audit of their solutions to assure superior levels of service, security, and 24/7 support
- 'Connect with confidence' and experience faster time-to-value, assured performance and continuous innovations with Cisco Powered services
- The faster time-to-value of Cisco Powered services is achieved by minimising complexity during the entire technology lifecycle, so organisations can focus on their core competencies while lowering costs and reducing risk

Cisco and its partners are leaders in the industry, so end customers benefit from extensive, ongoing R&D investment, based on the highest percentages of R&D investment-to-revenue.

In addition:

- Validated architectures help assure proven reliability
- Rigorous partner certifications help build confidence and trust in the cloud
- Third-party audits help verify delivery of services as promised
- SLAs help to achieve 99.99% to 99.999% uptime
- Integrated end-to-end security and redundancy lowers costs
- 24-hour, year-round Day 2 support helps assure day-to-day operations
- Independently-validated scalability matches buyer's dynamic business needs
- Open standards commitment gives buyers long-term flexibility
- Industry's highest R&D investment-to-revenue ratio delivers ongoing innovation

Back to contents

Cisco Powered Cloud Providers Available on G-Cloud

Cisco Cloud & Managed Services Programme (CMSP)
Partners available on G-Cloud

Please refer to Cisco Cloud & Managed Services Partner Locator tool for the latest information on Cisco Powered Partner Cloud Services

G-Cloud Providers	Verification		Cisco Powered Cloud Services					
	CMSP	PGA	IaaS	DRaaS	DaaS	HCS	HCS CC	TPaaS
Accenture			Click here					
Adapt			Click here	Click here	Click here			
ANS Group			Click here	Click here	Click here			
BT Global Services			Click here			Click here	Click here	
Capita ITS	Pending		Click here					
Centurylink			Click here					
Colt Technology Services			Click here	Click here	Click here			
Computacenter			Click here					
Daisy Group			Click here					
Damovo UK						Click here		
Dimension Data			Click here			Click here		
Fujitsu Services						Click here		
Kcom Group			Click here			Click here	Click here	
Logicalis			Click here					
Skyscape Cloud Services			Click here					
Steria			Click here					
Sungard AS			Click here					
Virgin Media Business						Click here		
Vodafone			Click here			Click here		
Xerox			Click here					

*Information current at time of publishing

Confirmed | Cisco powered | Cisco solution | Pending

IaaS Infrastructure as a Service
HCS Hosted Collaboration Solution
HCS CC Hosted Collaboration Solution for Contact Centre
TPaaS TelePresence as a Service
DRaaS Disaster Recovery as a Service
DaaS Desktop as a Service

Customer Cloud Service Success Stories

Here are some examples of how Cisco Powered partners are transforming the provision of IT services to the Public Sector through cloud services.

Case Study	Challenge	Solution	Result
Government Digital Services (GDS) **Skyscape Cloud Services** **IaaS**	Implement a single domain for government to replace Directgov and Business Link sites, 24 government departments websites and all agencies/non-departmental public bodies in less than two years.	· Hosting on a secure, accredited cloud platform which offers PSN connectivity · Cisco powered using Nexus, UCS and Vblock · Solution utilises an API which enables autoscale and continuous integration	· 90% saving on hosting costs · Agile development of GOV.UK, built and tested in public · New standards for development and security · Utilisation of open source technology
DVLA **Skyscape Cloud Services** **IaaS**	View driving record digital exemplar to be delivered in less than two years to deliver secure online access to driving records for up to 40 million drivers and partners including the insurance industry.	· Hosting on a secure, accredited cloud platform which offers PSN connectivity · Cisco powered using Nexus, UCS and Vblock · Successful integration with variety of external service partners	· 66% cost saving · Agile development · Ability to operate and continuously improve the live service · Cross Domain Guard between IL2 and IL3 platforms to support user access to secure data via the Internet
MOD **Skyscape Cloud Services** **IaaS**	Redesign and improve secure staff engagement scheme for worldwide defence community serving more than 200,000 users.	· Hosting on a secure, accredited cloud platform which offers PSN connectivity · Cisco powered using Nexus, UCS and Vblock	· More than 90% cost saving · Infrastructure ready in less than 48 hours · Engagement to production in three months · Project completed three weeks ahead of schedule

Back to contents

Continued...

Customer Cloud Service Success Stories

Case Study	Challenge	Solution	Result
London Borough of Hammersmith and Fulham council **Colt Technology Services** **Desktop-as-a-Service (DaaS)**	Do more with fewer resources, while protecting front-line services. Improve collaborative working with greater use of shared services and flexible working. Rationalise property portfolio.	Cisco Desktop Virtualization Solutions, running on Cisco Unified Computing System (UCS) with Intel Xeon processors	· Cost per VDI seat reduced by 20-25% · Power consumption down by 80% · Total cost of ownership cut by one-third
Salford City Council **ANS Group** **Community cloud (IaaS)**	Support growth of small and medium sized businesses. Overcome infrastructure capacity constraints. Transform IT from cost base to revenue stream.	Community cloud-based on FlexPod	· Up to 99% server virtualisation, helping provide private cloud services to local businesses · Server capacity increased by 50%, improving delivery and responsiveness of applications · 5-to-1 reduction in DC floor space requirements
Loughborough University **Logicalis** **Hybrid Private Cloud (IaaS)**	Maintain strong leadership position. Provide IT infrastructure commensurate with top student experience status. Improve sustainability and resilience.	· Cisco UCS servers, VMware virtualisation, and NetApp storage · Cisco Unified Communications hosted on UCS · Cisco VXI virtual desktop	· Agile private cloud with triangular data centre architecture · Improved productivity and efficiency from unified communications · Saved £2-3M in building costs and over 640 tonnes of CO_2 per annum

Continued...

Customer Cloud Service Success Stories

Case Study	Challenge	Solution	Result
Southern Housing Group **Sungard AS** **Disaster Recovery-as-a-Service (DRaaS)**	Southern Housing Group recognised that it needed to put in place more robust disaster recovery arrangements to enable the organisation to withstand disruption and continue to provide vital services to its 66,000 residents.	Sungard's Recover2Cloud service	• High availability of applications and services with maximum recovery time (RTO) of four hours • Saving of £250k capital investment, with comparable annual running costs to in-house solution • Peace of mind that data will always be available • Prevents financial loss due to lost or late rent payments
Police Accredited Cloud **Sungard AS** **IaaS/PaaS**	UK police forces were looking to drive smarter situational awareness, support multi-agency collaboration and meet growing demand for voice, video and data services. But at the same time, were under pressure to reduce ICT footprint, eradicate silos of under-utilised infrastructure and simplify operations.	• Secure cloud-based on FlexPod • 24 x 7 x 365 service management and operations teams • Protective Monitoring to effectively manage security alerts • Secure PSN connectivity • Dual site option with automatic failover • Integrated Disaster Recovery eliminates the need for tape back-ups • Cross Domain Guard available for public-facing components of secure applications	Police Applications: • Forensics and Fingerprint Bureaux (FISH) • Multi-Agency Collaborative Case management (Unilink) • POLE Store (Person, Object, Location, Event) • Workware Systems Situational Awareness (Workware Systems, Mapcite) • Police eCommerce (Software AG) • CCTV feeds (SiraView) • Connected vehicles (Cisco) • Secure Storage (Sungard AS)

For more case studies please visit: http://www.cisco.com/web/solutions/trends/cloud/case-studies.html

Back to contents

How Can Cisco Help?

Cloud Intelligent Network: the network remains critical to the cloud. Regardless of the type of cloud, without networks users cannot access their cloud services. Without networks applications, data, and users cannot move between clouds.

Cisco provides trusted business advice to customers and providers on how to find the best path to cloud and has contributed actively to the development of cloud technologies and innovation. Cisco also has products and solutions to enable cloud and managed service providers or end-user organisations to build and deliver cloud infrastructure and services.

Cisco Managed Service Programme (CMSP) is a rigorous certification with third-party audits of cloud services, which ensures that providers align well with ISO27001:2013 and ITIL and thus some of the Cloud Security Principles. Cisco Powered Cloud Service Partners can be located using this tool here.

Cisco offers a choice of consumption models and customers can deploy cloud capabilities based on the needs of applications, SLAs, security and business objectives. The Public Sector buyer may choose to build their own private cloud, build a regional community cloud and offer it 'as-a-service' to other agencies, buy specific Line-of-Business applications (SaaS), select Cisco Powered services from cloud providers, or take a hybrid IT approach and fuse on-premise and cloud resources. The Cisco Cloud portfolio and our extensive partner ecosystem are designed to increase choices and support flexible cloud services sourcing strategies.

Cisco Services has global consulting practices which can help organisations plan a more secure path to cloud using on-premise and cloud-based solutions, identify 'shadow' cloud deployments, reduce exposure to security risks, and securely extend cloud services across multiple clouds.

Gain Cloud Visibility and Governance: Cisco Data Centre Assessment for Cloud Consumption Service is a one-time assessment that reveals which cloud services are being used within a business and clearly details cloud usage, costs, and risks. A sensor appliance is installed to discover authorised and unauthorised service.

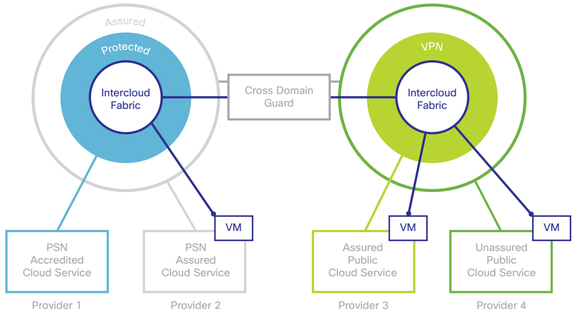
Cloud security:

- Security for the cloud – the ability to provide complete end-to-end security solutions across Hybrid Cloud environments remains a critical success factor for the adoption of cloud services
- Security from the cloud – as the traditional security perimeter continues to distribute, providing security from the cloud has become a new norm for customers with a distributed environment
- Cisco is an innovator in delivering security from the cloud; today we offer Cloud Web Security, Hosted Email and Advanced Malware Protection

Interoperability and open standards with Cisco Intercloud Fabric:

Cisco Intercloud Fabric provides the capabilities for businesses and cloud providers to implement open and secure Hybrid Cloud environments, facilitating IT *application migration across multiple clouds*, thereby matching price, performance and governance characteristics.

Cisco Intercloud Fabric



Back to contents

Cisco would welcome the opportunity to discuss the contents of this guide if you need help spotting cloud opportunities within your organisation.

Please contact your Cisco Account Manager to discuss your requirements in more detail, or email: ask-gcloud@cisco.com

References

Back to contents

Cisco References

Cisco Powered http://www.cisco.com/web/solutions/trends/cisco-powered/index.html
Cisco Cloud and Managed Services Partner Locator https://tools.cisco.com/WWChannels/LOCATR
Cloud Case Studies http://www.cisco.com/web/solutions/trends/cloud/case-studies.html
Cisco Intercloud http://www.cisco.com/cisco/web/UK/products/switches/cisco-intercloud.html
Cisco Cloud Strategy http://www.cisco.com/go/cloud

Partner References

Skyscape http://www.skyscapecloud.com/wp-content/uploads/Skyscape_GSCP_Whitepaper.pdf

CESG References

Product Assurance https://www.cesg.gov.uk/servicecatalogue/Product-Assurance/Pages/Product-Assurance.aspx
CPA Assured Products https://www.cesg.gov.uk/servicecatalogue/Product-Assurance/CPA/Pages/CPA-certified-products.aspx
Pan Government Accreditation (PGA) https://www.cesg.gov.uk/policyguidance/PGA/Pages/index.aspx

GOV UK G-Cloud References

Digital Marketplace https://www.digitalmarketplace.service.gov.uk/
G-Cloud Buyers Guide https://www.gov.uk/government/publications/cloudstore-buyers-guide/cloudstore-buyers-guide--2
G-Cloud Sales Statistics https://digitalmarketplace.blog.gov.uk/sales-accreditation-information/
https://www.gov.uk/performance/g-cloud/cumulative-spend-by-customer-type

GOV UK Security Policy References

Government Security Classifications https://www.gov.uk/government/publications/government-security-classifications
Cloud Security Principles https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles
ICO Resources - Data Protection Act 1998 (DPA) http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

Appendix: The 14 Cloud Security Principles

Cloud Security Principle	Description	Why this is important
1. Data in transit protection	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit. Implementing 'Data in transit protection'
2. Asset protection and resilience	Consumer data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.	If this principle is not implemented, inappropriately protected consumer data could be compromised which may result in legal and regulatory sanction, or reputational damage. Implementing 'Asset protection and resilience'
3. Separation between consumers	Separation should exist between different consumers of the service to prevent one malicious or compromised consumer from affecting the service or data of another.	If this principle is not implemented, service providers can not prevent a consumer of the service affecting the confidentiality or integrity of another consumer's data or service. Implementing 'Separation between consumers'
4. Governance framework	The service provider should have a security governance framework that co-ordinates and directs their overall approach to the management of the service and information within it.	If this principle is not implemented, any procedural, personnel, physical and technical controls in place will not remain effective when responding to changes in the service and to threat and technology developments. Implementing 'Governance framework'
5. Operational security	The service provider should have processes and procedures in place to ensure the operational security of the service.	If this principle is not implemented, the service can't be operated and managed securely in order to impede, detect or prevent attacks against it. Implementing 'Operational security'
6. Personnel security	Service provider staff should be subject to personnel security screening and security education for their role.	If this principle is not implemented, the likelihood of accidental or malicious compromise of consumer data by service provider personnel is increased. Implementing 'Personnel security'
7. Secure development	Services should be designed and developed to identify and mitigate threats to their security.	If this principle is not implemented, services may be vulnerable to security issues which could compromise consumer data, cause loss of service or enable other malicious activity. Implementing 'Secure development'

Back to contents

Cloud Security Principle	Description	Why this is important
8. Supply chain security	The service provider should ensure that its supply chain satisfactorily supports all of the security principles that the service claims to implement.	If this principle is not implemented, it is possible that supply chain compromise can undermine the security of the service and affect the implementation of other security principles. Implementing 'Supply chain security'
9. Secure consumer management	Consumers should be provided with the tools required to help them securely manage their service.	If this principle is not implemented, unauthorised people may be able to access and alter consumers' resources, applications and data. Implementing 'Secure consumer management'
10. Identity and authentication	Access to all service interfaces (for consumers and providers) should be constrained to authenticated and authorised individuals.	If this principle is not implemented, unauthorised changes to a consumer's service, theft or modification of data, or denial of service may occur. Implementing 'Identity and authentication'
11. External interface protection	All external or less-trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.	If this principle is not implemented, interfaces could be subverted by attackers in order to gain access to the service or data within it. Implementing 'External interface protection'
12. Secure service administration	The methods used by the service provider's administrators to manage the operational service should be designed to mitigate any risk of exploitation that could undermine the security of the service.	If this principle is not implemented, an attacker may have the means to bypass security controls and steal or manipulate large volumes of data. Implementing 'Secure service administration'
13. Audit information provision to consumers	Consumers should be provided with the audit records they need to monitor access to their service and the data held within it.	If this principle is not implemented, consumers will not be able to detect and respond to inappropriate or malicious use of their service or data within reasonable timescales. Implementing 'Audit information provision to consumers'
14. Secure use of the service by the consumer	Consumers have certain responsibilities when using a cloud service in order for this use to remain secure, and for their data to be adequately protected.	If this principle is not implemented, the security of cloud services and the data held within them can be undermined by poor use of the service by consumers. Implementing 'Secure use of the service by the consumer'

You can find full details of the 14 Cloud Security Principles here: https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.