ukcloud

Pure commitment.

Using the UKCloud Guard

BLUEPRINT

UKC-GEN-131

OVERVIEW

UKCloud operates two cloud platforms designed exclusively for the UK public sector. Both are CESG Pan Government Accredited (PGA) for hosting systems and data classified at OFFICIAL:

- Our **Assured OFFICIAL** cloud platform is PGA for IL2, and natively and directly connected to the internet.
- Our **Elevated OFFICIAL** cloud platform is PGA for IL3, and natively connected to government community networks such as PSN and N3. This platform is more secure because the users and devices that access it are known and trusted.

The Government Digital Strategy is driving the transformation of government systems that used to be restricted to closed communities of government officials, to make them directly accessible by citizens and businesses. The benefits of doing this include:

- Reduced costs to government, as online transactions are much cheaper than phone, postal or face-to-face transactions
- Meeting public expectations of being able to interact with government organisations online

To support this transformation, public-sector organisations increasingly need to connect citizen-facing application components hosted on the UKCloud Assured OFFICIAL (PGA IL2) cloud platform to application components hosted on the more secure UKCloud Elevated OFFICIAL (PGA IL3) cloud platform.

The UKCloud's Guard (commonly referred to as 'the Bridge') provides controlled interconnection between the two cloud platforms.

How GPMS impact levels map to GSCP OFFICIAL classification

In this document we refer to impact levels 2 and 3 (IL2 and IL3). These formed part of the Government Protective Marking Scheme (GPMS) and are consistent with our CESG Pan Government Accreditation.

The Government Security Classifications Policy (GSCP), launched in April 2014, replaces the GPMS, and combines IL2, IL3 and IL4 into a single OFFICIAL classification.

Some data classified at OFFICIAL and OFFICIAL-SENSITIVE needs different security controls from other data classified as OFFICIAL. To meet these differing requirements, UKCloud will continue to maintain both its lower-security platform (the Assured OFFICIAL (PGA IL2) cloud) and its higher-security platform (the Elevated OFFICIAL (PGA IL3) cloud).

IN THIS BLUEPRINT ▶

Key principles 4
How the UKCloud's Guard works 5
The approval process 12
About UKCloud 13

KEY PRINCIPLES

The role of the Pan Government Accreditor

There are risks inherent in allowing a lower-security domain to access systems in a higher-security domain. To mitigate the risks for organisations in the higher-security domain, the UKCloud’s Guard forms part of the CESG Pan Government Accreditation of UKCloud's cloud platforms.

However, the Pan Government Accreditor has intentionally highlighted the UKCloud’s Guard as a residual risk. This is to alert customers that they are responsible for identifying and managing risks associated with their individual use of the UKCloud’s Guard through their own accreditation and assurance activities.

To make sure customers are aware of this, the CESG Pan Government Accreditor requires each customer scenario to be reviewed and approved. To help with this process, UKCloud has created a UKCloud Guard request form that enables customers to capture most of the information needed for submission to the UKCloud Senior Information Risk Owner (SIRO) or, in exceptional circumstances, to a CESG Pan Government Accreditor.

The role of the customer’s accreditor

Although UKCloud provides its Assured OFFICIAL (PGA IL2) and Elevated OFFICIAL (PGA IL3) cloud platforms as CESG PGA services, each customer is responsible for the accreditation of their applications running on either cloud platform, including any specific use of the UKCloud’s Guard solution.

This means that your accreditor is responsible for identifying, assessing and mitigating specific risks to your individual solution that may arise through your use of the UKCloud’s Guard.

As part of your own assurance activities, UKCloud recommends that you:

- Engage a CLAS or CCP Security Professional
- Have an IT Security Health Check carried out by a CHECK test provider

Effective risk mitigation

When reviewing a UKCloud's Guard use case document that's been submitted for approval, the UKCloud SIRO will expect to see a number of controls included in the solution to adequately mitigate the risks of exposing to the internet an application that uses OFFICAL-SENSITIVE data (previously IL3).

The controls the UKCloud SIRO will expect to see are as follows:

- Is there a protective monitoring system in place, covering both sides of the UKCloud's Guard, which can be shown to meet the requirements of CESG Good Practice Guideline 13 (GPG13)?

- Has a CHECK Test been conducted on the solution, including the UKCloud Guard, which confirms that no risks higher than 'medium' remain?

- Is an accreditor's approval certificate available that confirms they are satisfied with the overall security regime of the solution which uses the UKCloud Guard?

- Host-based intrusion detection system (HIDS):

    - Agents installed within virtual machines (VMs) collect log data and alert on unusual behaviour or potentially forward alerts to a security operations centre (SOC)

- IT Security Health Check (CHECK)

    - Penetration test performed by a CESG CHECK approved tester

- Content type checking

    - Security policy defining which HTTP document types are permitted (such as text, XML, JSON)

- Deep content inspection

    - Inspection of an HTTP request or response body including, for example, XML schema validation and field length checking

- Data loss prevention (DLP)

    - Software which prevents data leaving an organisation without permission

- Anti-virus

    - The UKCloud's Guard is powered by Trend Micro technology. Accreditors may insist on VMs having an AV product from a different supplier installed

HOW THE UKCLOUD GUARD WORKS

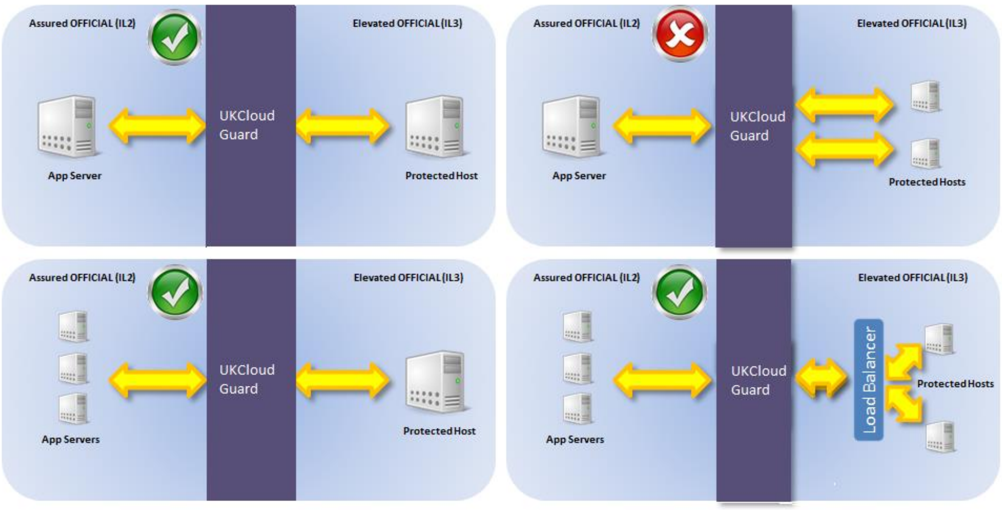
The UKCloud's Guard is an application proxy with security controls built in. It allows us to configure security policies governing which IL2 services can communicate securely with IL3 services via HTTP protocols.

When we implement a UKCloud Guard solution, we use information from the UKCloud Guard request form, such as permitted content types and maximum request size, to create a security policy on the UKCloud Guard. Traffic that doesn't match the policy will be blocked. Requests through the UKCloud's Guard must originate from the IL2 zone.

We implement the UKCloud Guard as a virtual appliance hosted on dedicated infrastructure in our data centres. It can be configured to accept requests from single or multiple application servers in IL2, but each instance may protect only a single service in IL3. This means that each service (for example, an authentication service and a search service) in IL3 requires its own UKCloud Guard.

The UKCloud Guard can, however, forward requests to multiple services on the IL3 side (for example, as part of a micro-service architecture) — as long as it's protecting a single IL3 IP address. This normally involves implementing a load balancer/proxy solution in the IL3 zone, and must be documented in detail in the UKCloud's Guard request form approval document.

Figure 1. Schematic of the UKCloud's Guard



Four-tier architecture

The UKCloud SIRO (or CESG PGA) will expect to see a four-tier architecture in the UKCloud's Guard request form. The architecture description must clearly show how the application has been split into the four tiers, shown below in Figure **2**.

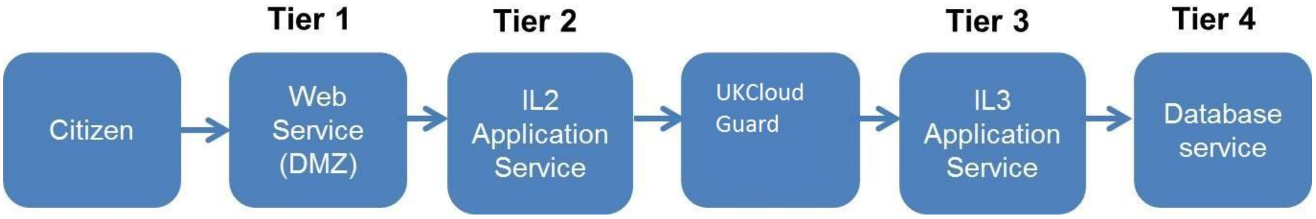
Any other architecture will be questioned in some depth by the UKCloud SIRO which may add delay to the project. The principles behind this design are to provide protocol separation at each tier of the application, and ensure that a minimal subset of application traffic is passed between the IL2 and IL3 zones.

You need to consider what happens at each tier of this architecture and clearly document it in the UKCloud Guard request form.

Tier 1: Web service (DMZ)

The web service within the DMZ tier is the public-facing component of your application. This tier serves the HTML pages for your application and makes calls to an application server to access data and business logic. The DMZ tier doesn't directly access data and should not host an application server (eg Tomcat, Rails). It's worth considering whether this tier can be restricted to a closed community such as N3 or PSN.

Figure 2. Four-tier architecture



If the application needs to reside on the public internet, it should use SSL and enforce authentication so that access to the system can be audited.

It is preferable to place a proxy server or layer 7 firewall in front of the web server to run content filtering and SSL offload, to add further protection to the service. Although a dedicated application firewall is desirable, DMZ tier servers can also do this (eg URL filtering).

Machines in the DMZ tier are vulnerable to attack, so each one should be configured to run the minimum number of services, and have its operating systems and applications hardened. Anti-virus and host-based security sensors should be deployed to each machine to monitor malicious behaviour. Logging should be enabled and the logs included as part of a protective monitoring solution.

The web service should be configured to meet the following controls (C*nn*) as described in GPG8:

- C03, User access and service limitation
- C04/C25, Content checks
- C07, System hardening (including host based IDS)
- C10, trusted source
- C24, web hosting security (eg being locked down and regularly patched)

Tier 2: IL2 application service (IL2 app tier)

The IL2 app tier is where the bulk of application code is deployed. It provides business logic and a data access layer. If the application has a database in IL2, this tier will be responsible for accessing that data.

This tier is responsible for generating web service requests which are sent to the UKCloud Guard to be inspected, and then forwarded to an application service in IL3. Data inside web service requests must be submitted to the UKCloud Guard as structured data (eg JSON, XML).

Anti-virus and host-based security sensors should be deployed to each machine to monitor malicious behaviour. Logging should be enabled and the logs included as part of a protective monitoring solution.

Content checking can provide an additional defence against content attacks, which traditional network defences such as firewalls and routers don't do. Both the underlying web content and associated payloads should be subject to strict content checking (eg filtering file types, validating actual content) with appropriate blacklisting and quarantining.

The UKCloud's Guard

The UKCloud's Guard operates as a secure proxy between the IL2 and IL3 application services.

It accepts requests from the IL2 app tier, and performs a virus scan and security policy check before forwarding the request to a single host IP on the IL3 app tier. This single IP can be a virtual IP for an IL3 load balancer, as long as:

- The load balancer forwards requests to IL3 application services
- This use pattern is documented in the UKCloud Guard request form

The UKCloud Guard security policy ensures that only requests matching the content types, HTTP methods and URLs (eg GET/auth.svc, POST/search.svc) are allowed to traverse to the IL3 side of the UKCloud's Guard.

Tier 3: IL3 application service (IL3 app tier)

The IL3 app tier accepts web service requests from the UKCloud Guard, and converts the structured data they contain into native database calls to be forwarded to the database (eg SQL, Oracle, Key/Value stores).

This tier should inspect the incoming requests to ensure they haven't been tampered with and that they contain valid data. This could include checks such as schema validation or in-depth field validation (such as data type, length).

The application service in the IL3 app tier should be hardened to the same standard as the application services in the IL2 DMZ tier. Anti-virus software, host firewall functionality, appropriate HIDS technologies, logging and auditing should also be applied to critical system servers.

Tier 4: Database service (data tier)

The data tier may consist of any appropriate technology as long as it's decoupled from the application using the tiered model documented in this Blueprint.

The data may not actually reside in the UKCloud environment at all, if the application needs to post data to a data source held elsewhere. In these cases, the application should:

- Communicate with the data source via a secure network (for example, GSI, PSN IPED)
- Preferably use an encrypted transport protocol such as HTTPS or IPSEC in line with CESG good practice around the transport of IL3 data

Networking

Each tier of the application should be placed on a dedicated network segment, which can be securely separated from other segments using firewall access control lists (ACLs) managed by you via your dedicated vShield Edge virtual firewall.

The following networks would support the architecture documented in this Blueprint.

IL2 zone

- DMZ tier
    - hosts web service only
    - accepts public internet traffic on required ports (HTTP/HTTPS) to the web servers
    - translates public IP addresses to internal IP addresses assigned to the web servers (DNAT)
    - permits application traffic to the IL2 app tier on specific ports
- IL2 app tier
    - hosts IL2 application service only
    - accepts application traffic from the DMZ tier on specific ports (eg HTTPS)
    - translates IL2 application traffic to a public IP (SNAT)
    - permits HTTP traffic from IL2 app tier to the UKCloud Guard via SNAT IP

UKCloud Guard zone (managed by UKCloud)

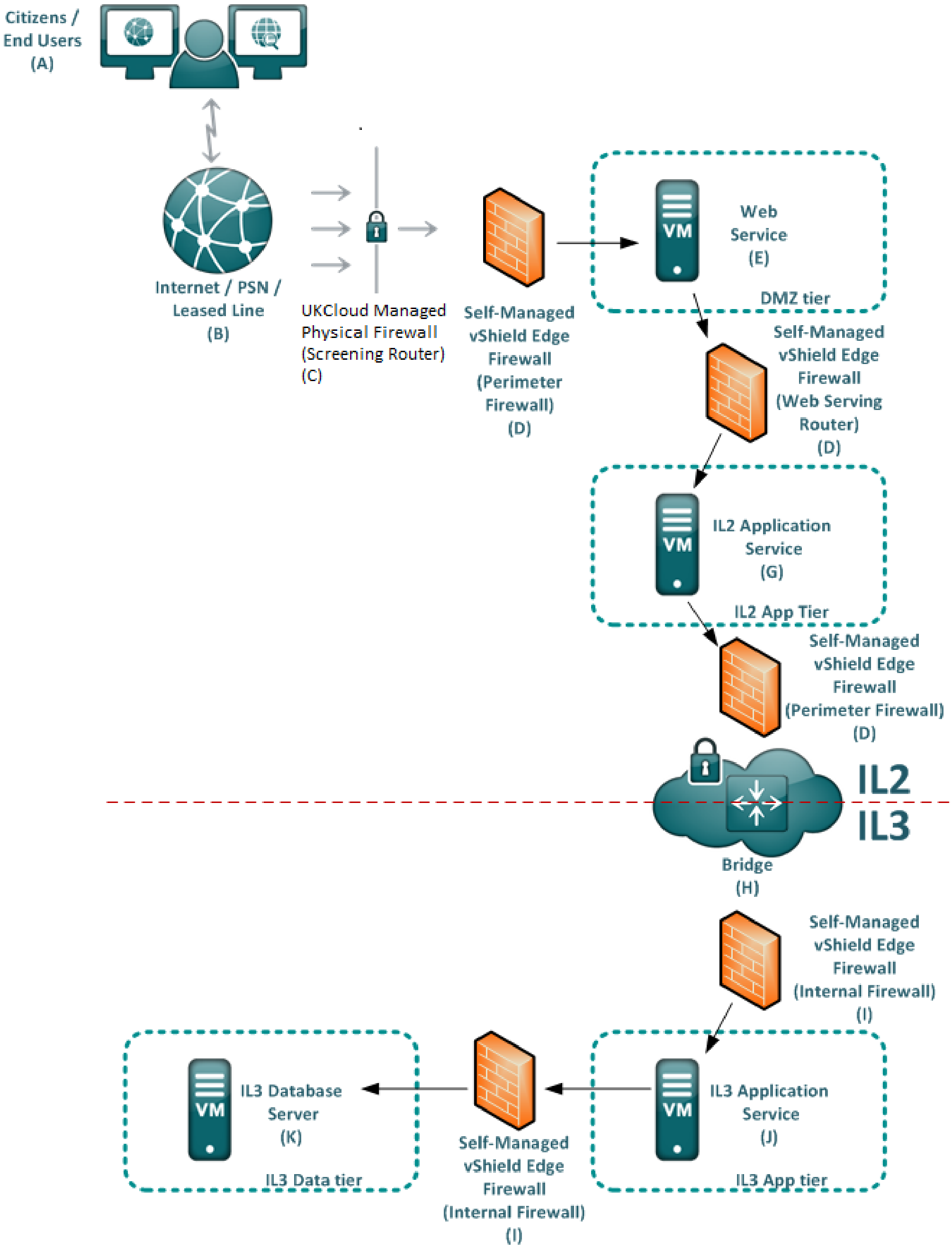
- UKCloud Guard — IL2 side
    - permits HTTP traffic from IL2 application service SNAT IP to Guard IL2 IP
- UKCloud Guard — IL3 side
    - permits HTTP traffic from UKCloud Guard IL3 side to IL3 application service DNAT IP

IL3 zone

- IL3 app tier
    - hosts IL3 application service
    - translates UKCloud-managed IP (private) to IL3 application net IP (via DNAT)
    - accepts HTTP traffic from the UKCloud Guard
    - permits database traffic to the data tier (eg SQLNet, ODBC)

Figure **3** shows this network topology graphically.

Figure 3. Network topology


Citizens / End Users (A)
Internet / PSN / Leased Line (B)
UKCloud Managed Physical Firewall (Screening Router) (C)
Self-Managed vShield Edge Firewall (Perimeter Firewall) (D)
VM
Web Service (E)
DMZ tier
Self-Managed vShield Edge Firewall (Web Serving Router) (D)
VM
IL2 Application Service (G)
IL2 App Tier
Self-Managed vShield Edge Firewall (Perimeter Firewall) (D)
IL2
IL3
Bridge (H)
Self-Managed vShield Edge Firewall (Internal Firewall) (I)
VM
IL3 Database Server (K)
IL3 Data tier
Self-Managed vShield Edge Firewall (Internal Firewall) (I)
VM
IL3 Application Service (J)
IL3 App tier

What the UKCloud’s Guard does and doesn't do

The UKCloud’s Guard supports the following functions:

- Secure proxy
- Content-type checking
- Virus scanning
- HTTP method restriction
- URL path restriction

All other checks, including DLP, schema validation and field validation, are the responsibility of the customer.

High availability

A UKCloud’s Guard solution is highly available within a single site. If site-level resilience is required, you'll need to buy a second UKCloud Guard, which will be configured with the same policy as the primary one.

You can then use the two UKCloud Guards in:

- An active/passive configuration, via application configuration updates (eg change UKCloud Guard target in the event of a failure)
- An active/active configuration, which is perhaps more useful — you'll need to implement a load balancer in the IL2 app tier to send requests to both UKCloud Guards.

The UKCloud Guard isn't session aware so requests should be stateless.

THE APPROVAL PROCESS

A UKCloud's Guard solution requires UKCloud SIRO (or CESG PGA) approval before we can implement it. The approval process can take some time as it depends on the completeness of your submission.

The approval process is as follows.

1. Read the UKCloud's Guard guidance document

Contact UKCloud if you have any queries at this stage. The better defined the architecture is, the faster it's likely to be approved.

2. Submit the UKCloud's Guard request form

A completed worked example of this document is available to help you understand what content is required and how to present it.

3. Get approval in principle from the UKCloud SIRO

At this stage UKCloud will implement the UKCloud Guard so that your application can be deployed and tested. The accreditor will usually require restrictions for this implementation, such as limiting the number of users and IP addresses that can access the application.

4. Test the application

Test that the controls on the UKCloud Guard are functioning as expected (eg disallowing blocked URLs and file types).

5. Produce IL3 accreditation document set (RMADS) and perform CHECK Test

- Is a protective monitoring system in place, covering both sides of the UKCloud Guard, which can be shown to meet GPG13 requirements?

- Has a CHECK Test been conducted on your solution, including the UKCloud Guard, confirming that no risks higher than 'medium' remain?

- Is an accreditor's approval certificate available to confirm they are satisfied with the overall security regime of the solution which uses the UKCloud Guard?

6. Submit CHECK test results to the UKCloud SIRO for approval

UKCloud's approval usually depends on a successful CHECK Test. We aren't allowed to remove the pre-production restrictions on the UKCloud Guard solution until we receive the test results.

7. Go live

We remove test restrictions and the UKCloud Guard becomes available for production traffic.

Bear in mind that steps 5 to 7 can take up to 90 days.

8. Ongoing assurance

At least once a year we'll need to see updated evidence to support the ongoing UKCloud Guard deployment.

ABOUT UKCLOUD

UKCloud has developed a range of cloud services designed specifically for the UK public sector, to help increase efficiencies, reduce costs, significantly improve procurement times and increase transparency. Our services are *easy to adopt, easy to use and easy to leave* to ensure that our customers remain in complete control with minimum risk. We were one of the first G-Cloud providers to achieve Pan Government Accreditation (PGA) up to Elevated OFFICIAL, and our services continue to achieve formal UK Government accreditations which make them suitable for all data at OFFICIAL (including OFFICIAL-SENSITIVE).

UKCloud's full offering consists of:

1. Infrastructure as a Service (IaaS) – seven offerings around Compute and Storage on demand

2. Software as a Service (SaaS) – offerings for email and collaboration as well as secure sync-and-share of files to help teams work effectively in groups, using a variety of devices

3. Platform as a Service (PaaS) – based upon Open Source Digital Application Platform and Hadoop which provides organisations the benefits of using a commodity cloud platform without the added management overheads

All of UKCloud's UK sovereign cloud computing services are hosted in one (or both) of our highly resilient tier 3 UK data centres in Farnborough and Corsham. UKCloud services are delivered with leading technologies from UKCloud Alliance Partners: QinetiQ, VMware, Cisco, EMC and Ark Data Centres. The Cloud Alliance also provides a collaborative resource which drives innovation and technical product development, helping to continually improve UKCloud's offering to meet the needs of the UK public sector.

UKCloud is focused on providing cloud services in a more agile, secure and cost effective manner. We strive to deliver solutions that harness technology as a way to facilitate the changes that are needed to streamline processes and reduce costs to support the UK public sector and, ultimately, UK citizens and taxpayers.

MORE INFORMATION ▶

For further information about UKCloud and how we can help you, please send an email to info@ukcloud.com

UKCloud Ltd

A8 Cody Technology Park
Ively Road
Farnborough
Hampshire
GU14 0LX

+44 (0)1252 303300

info@ukcloud.com

www.ukcloud.com

Reasonable efforts have been made to ensure the accuracy of the information contained in this document. No advice given or statements or recommendations made shall in any circumstances constitute or be deemed to constitute a warranty by UKCloud Ltd as to the accuracy of such advice, statements or recommendations. UKCloud Ltd shall not be liable for any loss, expense, damage or claim howsoever arising out of the advice given or not given or statements made or omitted to be made in connection with this document.