CyRisk®

Cloud Assurance Service

G-Cloud 15 – Service Description

Version: 1.0

Date: 7th January 2026

Summary

CyRisk Cloud Assurance Service offers a range of activities which can be procured individually or grouped to support phases or through-life functions. Examples include a single supplier assessment, threat model or design workshop, support for a feasibility exercise or migration project or multiple services thorough the service life.

Features

- Threat Modelling
- Risk Management (Risk Assessment and Risk Treatment)
- Policy, Process and Procedures
- Management System and Framework Compliance and Certification Support
- Security Architecture Design, Review and Training
- Security Design Authority
- Security Testing Support (Scoping, Delivery Support and Remediation Management)
- Lifecycle and Vulnerability Management (SAST, DAST, Dependency Management)
- Supplier Assessment and Assurance
- Operational Security including Protective Monitoring, Incident Management and Audit

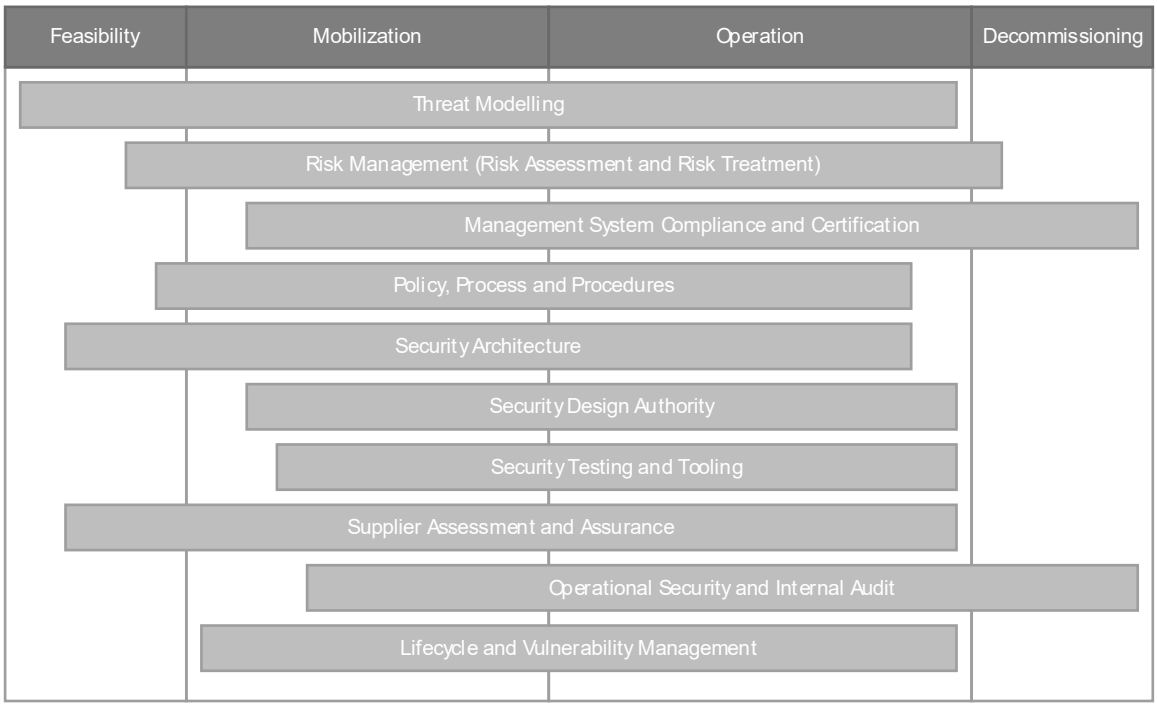
Benefits

- Choose individual activities, single phase/function, or end to end service
- Guided activities produce deliverables and upskill staff
- Options for guidance and advice or self-contained delivery
- Experience with Amazon Web Services (AWS) and Microsoft Azure
- Vendor agnostic approach
- Delivery by CIISec members.
- Tiered supplier assurance approach to support phase and risk level
- Experience with ISO27001, NIST CSF, CIS18 and NCSC CAF
- Experience working with Central Departments, ALBs, Devolved Administrations and Police
- Services designed to support knowledge transfer

1 Introduction

The CyRisk cloud assurance service has been developed to allow customers to flexibly buy the support they need for their project or service. There are options to buy a single activity, support for a single phase, a function through life or a complete end to end service. The level at which the service operates is also flexible with options for advice, guidance and training, or self-contained delivery. For ongoing support our engagement model means that you get access to a consist resource with minimum commitment equivalent to one day per month.

The following diagram provides an overview of how available functions could apply to the phases of an end-to-end service.



2 Threat Modelling

Threat modelling is likely to be the first information security activity to be started. An initial version of a threat model can be created as early as discovery to help understand the threats associated with the data and transacting parties. The model can then be developed as the requirements of the service are explored and expanded through Alpha, Beta and into live. Our approach to threat modelling is based on concepts such as STRIDE and is designed to help the ownership of the model migrate to the development team as the project progresses, so it is naturally reviewed and maintained as part of ongoing development.

Potential options include:

- Self-contained threat model development to support an individual phase.
- Development of the initial threat model with tapering support as the maintenance is transferred to the development team or information security function.
- Development of the initial threat model and maintenance of the model through participation in development (sprint) planning.

3 Risk Management

Identification and assessment of risks is key to communication with seniors within an organisation, so it is important that it is conducted in a manner which is consistent, intelligible and credible to support decision making.

3.1 Risk Assessment

We have experience working with a range of standardised risk assessment techniques including, IS1, CRAMM, HM Treasury Orange Book and ISO27005. We also have experience of developing bespoke risk assessment methods to focus on specific requirements, including:

- Risk landscape assessments providing rapid identification and visualisation of risk.
- Quantitative risk assessments which facilitate a top-down view of risk which is consistently and statistically linked to granular considerations.
- Personnel focused assessments which are centred on the outcomes for individuals.

Potential options include:

- Risk assessments developed using your chosen approach.
- Risk assessments conducted using our risk landscape approach.
- Risk assessment conducted using our top-down approach combined with training for your staff.
- Development of bespoke risk assessment approach to address your requirements.

3.2 Risk Treatment

Our consultants have developed and managed risk treatment plans in complex multi-supplier programmes with values in excess of £10 million. We always look to balance physical, technical, and procedural controls when mitigation is required taking into account impacts to cost and ease of use. Risk treatment plans are commonly developed using the ISO27001 or NIST Cyber Security Framework (CSF) to provide a comprehensive view of treatment although it will not always be appropriate to implement all the controls.

We understand that risk treatment needs to be designed with understanding of the operating context of the service and organisation. The balancing of business functionality and security controls can be a complex. In many situations it is a particular approach to delivering functionality which causes a security issue, and a broader review of the requirement will allow a more acceptable approach to be identified. When the delivery of functionality is perceived to move the risk beyond what would normally be acceptable, we will support the formal communication of the risk to appropriate senior stakeholders to decide if a risk should be tolerated.

Potential options include:

- Development of risk treatment plans for in-house delivery.
- Review of proposed risk treatment plans.
- Development of risk treatment plans delivered through other service activities.
- Support and guidance for specific risks including risk escalation documents for formal reviews.

4 Policy, Process and Procedures

We have worked with a range of public sector clients and their suppliers to develop and implement policy and subsequent process and procedures covering a broad range of information security areas. Our approach to structuring policy, process and procedures focuses on effectively communicating the relevant information for the audience in an accessible way.

Potential options include:

- Develop or review and implement an individual policy with associated process and procedures, such as reviewing a cryptography policy with reference to public cloud.
- Develop and implement processes and/or procedures to provide policy compliance for a new service, such as how an existing access control policy applies to AWS.
- Develop and support implementation of a governance approach for a new delivery approach, such as integrated security tools for continuous integration pipelines.

5 Management System and Framework Compliance and Certification Support

We have considerable experience on helping clients to align with and achieve compliance with management system of framework standards including the ISO27001 and the NIST Cyber Security Framework (CSF) which underpins the Minimum Cyber Security Standard.

Whilst many public sector clients choose not to formally certify their management systems, we often work with suppliers to deliver and maintain the certifications which they are required to achieve and maintain for public sector clients. This means we are well placed to conduct internal compliance exercises and to evaluate the certifications offered by suppliers.

We also have experience of working with clients to demonstrate compliance with public sector standards such as Police Approved Secure Facility (PASF).

6 Security Architecture

With many services being consumed over the internet or combining elements from different suppliers over the internet architecting solutions is key to manging the threats a system faces including commodity software vulnerabilities and particularly zero-days vulnerabilities.

We can help to ensure that services are designed using secure by design principles and that any single points of failure are identified so a conscious decision can be made about their management.

For clients who are looking to upskill their internal workforce we can offer guided design review workshops which offer a combination of security architecture training with the chance to work through a design which is relevant to the attendees.

Potential options include:

- Individual design review workshops at various stages in design evolution.
- Ongoing security architecture review and guidance whilst a service is developed and implemented.
- Guided design reviews to combine a review with the chance to upskill staff.

7 Security Design Authority

Once the initial architecture and design work has been completed it is essential that incremental changes to the solution do not erode the security posture. Security design authority may be delivered as discrete service to review proposed changes or may be integrated into other services such as ongoing threat modelling or into wider functions such as operational change management.

8 Security Testing Support

Security testing is key to assurance of cloud solutions. When services are delivered and consumed over the internet they are exposed to continuously evolving threats and vulnerabilities.

8.1 Integrated Security Tools

Security tools such as Vulnerability Scanners, Static Application Security Testing, Dynamic Application Security Testing and Dependency Monitoring all have a potential role in helping to address rapidly evolving threats. These are in addition to tools which you might include as part of your security architecture such as Web Application Firewall (WAF), Intrusion Prevention System (IPS) or Security Orchestration, Automation and Response (SOAR). These integrated tools can be run on a very frequent basis and identify some of the issues which would have conventionally only been discovered during penetration testing.

We can support you in identifying which tools will provide the greatest value, where they should be deployed in your architecture and how you build processes and procedures that ensure you maximise the value from your investment.

8.2 Penetration Testing

Penetration testing continues to offer value in addition to integrated security tools, but careful scoping of testing is necessary to maximise value. We can work with you and your chosen testing provider to build scopes for single systems or provide a co-ordinated approach to test an entire estate. Using outputs from integrated security tools, protective monitoring, and threat models we can help you to really target penetration testing in the areas which pose the greatest risks. Having defined scopes, we can work with you and your testing provider to manage the testing programme, look for opportunities to educate your staff and potentially validate remediation during the testing. When the results of the testing are received, we can help you to contextualise the vulnerabilities and then design and prioritise remediation.

If you have mature security practices or high-risk systems, we can advise on engaging providers to perform red team or purple team exercises to test services in their operating context.

9 Supplier Assessment and Assurance

Many cloud solutions involve not just one provider or service but the composition of services from multiple suppliers. This may include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) or even specialist offerings like Identity as a Service (IDaaS). Some of these offerings may be unique to a single supplier and so early initial assessment is important to avoid designing in a component which is later going to prove unsuitable.

As the design progresses it is likely that the role of providers will be risk assessed and additional scrutiny will be required for services which play a key role in delivery. This could

range from reviewing supplier materials released under NDA through to conducting audits and on-site inspections. Once a service is operational it is important that supplier compliance is monitored, and changes implemented by the supplier and the way that services are consumed are assessed.

We can offer a range of supplier assessments from a single feasibility assessment for a provider through to a through life programme of assessment and ongoing assurance.

10 Operational Security

Operational security includes a broad range of activities. Whilst we are able to advise across the spectrum those which we are able to deliver will depend on the scope of the engagement. The following is a selection of activities we frequently work with clients to deliver.

10.1 Lifecycle and Vulnerability Management

Lifecycle and vulnerability management is key to operating a service that retains its security posture throughout its life. We work with clients to benchmark their current position and if necessary, build prioritised remediation plans. Our approach helps to address the situation when patches, updates and migration are non-trivial to implement. We identify lifecycle points early so upgrades can be included in planning. We risk assess vulnerabilities and look for mitigations, so priority is based on contextualised risk of exploitation.

10.2 Incident Management

We work with clients to review their incident management processes and procedures. These reviews often involved conducting incident simulations. These simulations help to identify the steps which are actually taken provide and opportunity to feed lessons learnt into the review. These simulations also expose potential incident responders to decisions and challenges which they may face so they are better prepared for real incidents.

We facilitate lessons learned exercises following incidents, gathering information from the relevant parties and then providing commentary, insights and recommendations based on our breadth of experience and independent position.

10.3 Internal Audit

We can provide services from a single targeted audit through to the planning and delivery of a full internal audit programme. Our consultants have experience of auditing the full ISO27001 standard and conducting programmes of physical security audits for operational and administrative sites.

10.4 Protective Monitoring

Our consultants have experience of delivering the whole protective monitoring lifecycle including building strategy, defining requirements, project managing implementations and managing live operation.

Our consultants have worked hands-on with a number of public sector bodies to deliver tactical and proof of concept protective monitoring using open source and office productivity tools. These tactical solutions help clarify requirements before starting a formal procurement and address gaps whilst implementation is taking place.

11 Our Delivery Approach

We strive to deliver the most appropriate service for each client, which will inevitably mean different amounts of time, sometimes delivered remotely, sometimes on site, using a team or just a single consultant. With all these variables our overarching delivery approach remains consistent providing the following features:

- Engagement managed by a knowledgeable cyber security practitioner.
- Weekly reports delivered every week for the duration of the engagement detailing activities delivered and planned, delivery risks and issues, and when appropriate time booked or current service metrics.
- Services reviews every 30 days.

12 About CyRisk

CyRisk was founded in 2020 to focus on providing services to clients which need to comply with UK Public Sector requirements or have other elevated assurance requirements. CyRisk is led by Phil Harding who has spent the last 20 years working with a range of companies providing consultancy on information assurance to the UK Public Sector, its suppliers and other organisations with elevated information security and assurance requirements.

