G-Cloud 15 Lot 3 - Cloud Support
Penetration Testing Services Overview

Prism Infosec

Prism Infosec supports organisations globally to prepare for, respond to and manage cyber security threats.

Service name	Description
Application Code Review	A comprehensive security-focused review of application source code designed to identify vulnerabilities, insecure coding practices, and logic flaws that may not be detectable through automated scanning alone. The review assesses adherence to secure coding standards, input validation, authentication and authorisation logic, cryptographic implementation, and error handling. Findings are prioritised by risk and accompanied by clear remediation guidance to help development teams improve security throughout the software development lifecycle.
Attack Surface Mapping	A detailed discovery exercise that identifies and documents all digital assets exposed to attackers, including domains, subdomains, IP addresses, cloud services, APIs, third-party integrations, and shadow IT. This service provides organisations with a clear understanding of their true attack surface, highlighting unknown or unmanaged assets. The results support risk reduction by enabling informed decisions around asset management, exposure reduction, and continuous monitoring.
CHECK Penetration Testing / IT Health Check Service	A UK government-approved penetration testing service delivered by CHECK-certified testers, designed to meet public sector and regulated environment requirements. The service simulates real-world attack scenarios against systems handling sensitive or classified data. Testing outcomes provide assurance to stakeholders that security controls are effective, while detailed reports highlight vulnerabilities, exploitation paths, and practical remediation actions in line with CHECK and NCSC expectations.
Cloud Architecture Reviews	An in-depth assessment of cloud platform architectures across environments such as AWS, Azure, or Google Cloud. The review evaluates identity and access management, network design, data protection, resilience, logging, and monitoring controls. It ensures cloud environments are designed securely from the ground up, aligned with industry best practices, compliance obligations, and shared responsibility models, reducing the risk of architectural weaknesses.
Cloud Configuration Review	A focused assessment of cloud service configurations to identify security weaknesses caused by misconfiguration, excessive permissions, insecure defaults, or policy gaps. The review covers areas such as identity roles, storage access, network security groups, encryption settings, and monitoring controls. Findings help organisations strengthen their cloud security posture and reduce the likelihood of data breaches caused by common configuration errors.
Cyber Essentials Certification	Provides structured guidance and technical support to help organisations achieve Cyber Essentials certification, the UK government's baseline cyber security standard. The service ensures that key controls such as access management, secure configuration, patch management, and malware protection are correctly implemented. Achieving certification demonstrates a commitment to cyber security and is often required for public sector contracts and supply chain assurance.
Cyber Essentials Plus Certification	An enhanced version of Cyber Essentials that includes independent technical validation of security controls through hands-on testing. This service verifies that systems are correctly configured and resilient to common cyber attacks. Cyber Essentials Plus provides higher assurance to customers, regulators, and partners by demonstrating that security controls are not only in place but operating effectively.
External Infrastructure Penetration Testing	A controlled simulation of real-world attacks against externally accessible systems such as servers, VPN gateways, firewalls, cloud services, and remote access solutions. The test identifies exploitable vulnerabilities that could lead to unauthorised access, data exposure, or service disruption. Results provide actionable insight into perimeter security effectiveness and help organisations strengthen their external defensive posture.

Service name	Description
External Vulnerability Assessment	A structured assessment using automated and manual techniques to identify known vulnerabilities, outdated software, and misconfigurations on externally facing systems. Unlike penetration testing, this service does not attempt to exploit findings, making it suitable for regular security hygiene checks. The assessment delivers prioritised results and remediation advice to support ongoing vulnerability management.
Firewall Ruleset Review	A detailed analysis of firewall configurations and rulebases to assess alignment with security policies and operational requirements. The review identifies overly permissive rules, unused or redundant entries, and potential misconfigurations that increase attack surface. Recommendations help improve security, simplify rule management, and support compliance and audit readiness.
IT Health Check Service (ITHC)	A comprehensive security assurance service combining penetration testing, vulnerability assessment, and risk analysis. Commonly required for UK government and critical systems, ITHC provides confidence that systems meet defined security standards. Deliverables include detailed technical findings and management-level assurance reporting to support accreditation decisions.
Mobile Application Testing	A thorough security assessment of mobile applications on iOS and Android platforms, covering application logic, data storage, authentication, encryption, and backend API interactions. Testing identifies platform-specific vulnerabilities and insecure design choices. The service helps protect user data and maintain trust by addressing risks unique to mobile environments.
Infrastructure Testing	An in-depth security assessment of internal networks, servers, endpoints, and supporting infrastructure. Testing identifies vulnerabilities that could allow attackers to gain initial access, move laterally, escalate privileges, or compromise critical systems. Results help organisations understand internal security weaknesses and improve overall resilience.
Web Application / API Testing	Comprehensive testing of web applications and APIs to identify vulnerabilities such as injection attacks, broken authentication, insecure access controls, and sensitive data exposure. The service combines automated scanning with manual testing to uncover both common and complex flaws. Findings are prioritised by risk and supported by clear remediation guidance.
Phishing Simulation / Social Engineering	Simulated phishing campaigns and social engineering exercises designed to replicate real-world attack techniques. The service assesses staff susceptibility, awareness levels, and reporting behaviours. Results provide insight into organisational risk and support targeted security awareness training and cultural improvement.
Red Team / CREST / GCASE / GBEST / CBEST	Advanced adversary-led security testing that simulates realistic and sophisticated threat actors targeting people, processes, and technology. The exercise evaluates detection, response, and recovery capabilities under real-world conditions. These tests provide strategic insight into organisational resilience and support regulatory and assurance requirements.
Physical / Building / Premises Security Review	An assessment of physical security measures including access controls, surveillance, visitor management, environmental controls, and staff practices. The review identifies weaknesses that could enable unauthorised access to facilities or systems. Recommendations help strengthen physical security as part of a holistic cyber defence strategy.

Service name	Description
Server and Appliance Build Review	A detailed review of server, network, and security appliance builds to ensure secure configuration, hardening, patching, and alignment with best practice standards. The service identifies configuration weaknesses that could be exploited and provides recommendations to improve baseline security and operational stability.
Wireless Security Assessment	A comprehensive assessment of wireless networks to identify weak encryption, insecure authentication, rogue access points, and misconfigurations. Testing evaluates how wireless access could be abused to gain unauthorised entry to internal systems. Findings help strengthen wireless security and reduce the risk of network compromise.

Sample Approach To Deliveries for Core Services

Cloud Configuration Review:

The purpose of a Cloud Security Configuration Review is to assess the security posture of resources at the Cloud Provider level. This can provide additional security assurance for a project in the case that a staff member's cloud account or a cloud hosted resource is compromised, helping to ensure that effective defensive depth is in place to mitigate the potential impact.

Prism Infosec will review the security of the Cloud implementations, against common best practice standards such as the NCSC cloud security principles and the Cloud Security Alliance Cloud Controls Matrix. This can include (but is not limited to) the following approach:

- Virtual Machine Cloud Configuration Review
- Cloud NACL and Firewall Review
- Review the Cloud Configuration of PaaS Compute and API Deployments
- Review of Serverless Computing Cloud Configurations
- Review of both Public and Private Cloud Data Storage
- Cloud Database Configuration Review
- Review Deployed Application Co-Ordinations
- Review of Deployed Messaging Services
- Load Balancer Cloud Configuration Review
- Cloud Permissions Review
- Cloud Monitoring and Security Configuration
- Review of Cloud Settings for other relevant Deployed Cloud Resources

The review will identify issues within three main categories:

- Misconfigurations that may lead to the compromise of the environment or data.
- Permissions issues that may lead to privilege escalation.
- Missing hardening measures.

The report will provide practical recommendations and improvements to address these issues and help further secure the environment.

It is envisaged that some changes may not be implemented immediately as they may require dependencies or have some risk to existing access and should be managed over time. As such, Prism Infosec recommend that the client commission a report to outline the current configuration, gaps and any changes that were or could be made and the associated benefits.

External Infrastructure Penetration Testing:

Prism Infosec shall test network ranges for active hosts and investigate further the responses to protocols, ports and services. Using a combination of manual reviews and automated port and vulnerability scanning tools (such as “nmap”, “Nessus” and “dirsearch”), Prism Infosec shall identify vulnerabilities and weaknesses (such as authentication, account or password issues) in the client’s Internet facing infrastructure.

With permission from the client, Prism Infosec can then conduct controlled exploitation attempts on any vulnerabilities and weaknesses using custom exploit code or using off-the-shelf exploitation frameworks such as “Metasploit”.

Should an attack be successful we will assess the extent of the breach, including whether access is limited only to a DMZ, or that compromised hosts do not have data, passwords or password hashes that could lead to further access into the client’s environment. All password hashes that are identified will be subjected to an offline password attack using our dedicated cracking server to determine the strength and susceptibility to compromise.

Our external testing methodology follows a refined test methodology that ensures a comprehensive attack simulation against the organisation.

External Vulnerability Assessment:

The CREST-Approved Vulnerability Assessment (VA) service delivered by Prism Infosec searches host devices and infrastructure for known vulnerabilities and will consist of a process where the vulnerability scan will be automated and conducted at regular intervals within a calendar year. Regular vulnerability scanning is necessary for maintaining information security across an ever-changing environment.

Vulnerability Assessments identify vulnerabilities in a network and estimate how susceptible the network is to the identified vulnerabilities. The VA utilises automated network security scanning tools, whose results are listed in the report. The findings reflected in a vulnerability assessment report are not always able to be supported by an attempt to exploit them, therefore some of them may be deemed false positives.

The proposed approach will involve the following steps:

Remote Setup
- Initial set up and configuration of the security scanning tools.
- Initial VA conducted remotely as part of the initial setup and test.
- Ongoing updates, provided remotely, to the deployed tools in readiness for all subsequent testing.

Vulnerability Assessment - Test Execution
- Will detect the open ports and identify the services running on these ports. It will identify possible vulnerabilities associated with these services and the underlying infrastructure.
- This process is conducted using industry recognised network-based scanners.

Findings Analysis
- Analysis of the tool output to identify security threats and eliminate any potential false positives.
- Identification of legitimate threats to services and infrastructure.

Reporting
- A comprehensive report as outlined in section 6.9.

Remediation (conducted by the client)
- Concluded between the scheduled Vulnerability Assessments.
- Fixing identified vulnerabilities to reduce existing threats and exploitation paths.
- Any remediation status would be confirmed within the next assessment.

The VA will detect security issues and vulnerable services such as missing patches, outdated protocols, certificates and services. Any vulnerabilities introduced as a result of ongoing configuration changes to the equipment or network services will be identified within the next scheduled vulnerability scan.

After the initial set-up and VA scan activity, the subsequent VA’s will be conducted remotely across the calendar year at quarterly intervals. The testing will provide a comprehensive baseline of what vulnerabilities exist and what (if anything) has changed since the last VA. This will also verify the status of any remediation actions that have been conducted since the previous assessment.

All VA's will be conducted by our CREST accredited consultants, this may be conducted with or without credentials, depending on the level of detail required by the client.

All active network services will be checked for security vulnerabilities and their associated risk. Vulnerabilities are identified by the following methods:

- automated testing – use of automated vulnerability scanning tools;
- checking identified services and associated version numbers for known vulnerabilities through the use of vulnerability databases such as the CERT, Bugtraq and manufacturers security notes;
- our consultants use their experience to check for false positives;

Possible vulnerabilities in a network service may include:

- Vulnerabilities that could allow sensitive information to be leaked;
- Vulnerabilities that could allow an attacker to gain control of that service, such as the web service;
- Vulnerabilities that could potentially give an attacker system level access to host devices;
- Vulnerabilities that could potentially lead to a Denial of Service attack. This could lead to either failure in that service or the entire host.

A security risk is associated with each identified vulnerability that is discovered during the assessment.

Firewall Ruleset Review:

To complement firewall network exposure testing, conducted during internal network security assessments, firewall ruleset reviews can be conducted.

The firewall rulesets will be subjected to analysis against the firewall policy and best security practice with the aim of identifying:

- Insecure firewall rules including any rules and those deemed overly permissive;
- A complete listing of permissible protocols including those restricted to specific source addresses unidentifiable from a network perspective;
- Plaintext protocols permitted though the firewall and those used for management of the firewall itself;
- Use of additional firewall security features and IDS/IPS.
- Undocumented rules;
- Absence of stealth and logging rules;
- Other rulebase misconfiguration;
- Missing firmware updates / obsolete firewall software;
- Exposure of administrative interfaces / unnecessary VPN or other features installed; and
- Possibility of firewall performance optimisation.

Using a combination of open source and commercial software (Nipper), Prism Infosec shall provide a breakdown of the firewall rules affected by individual issues and highlight any of significant risk to the client, particularly that might allow unnecessary communications or significant data exfiltration.

Mobile Application Testing:

The following items shall comprise the scope of the testing for each mobile application to be tested:

1)Underlying Server Infrastructure - The infrastructure associated with the web services endpoints will be investigated. In particular, this will cover the security of any exposed interfaces including:

- The web service endpoints – only the required services are exposed and that they are configured to reduce unnecessary content and information leakage and are setup in line with best practice for web service endpoints and web servers;

- That no other services are exposed (e.g. management interfaces, SSH login, et al).

1)Web Service Endpoints Message Handling - The web service endpoints will be investigated. We will investigate the web services' input validation, authentication and authorisation functions to ensure that they are well setup and configured.

The security of the endpoints will be investigated remotely. Prism Infosec will interact with the web services and attempt to identify any common security flaws in the web service message handling (following the OWASP Top 10 framework), including input validation (various injection types, cross site scripting and request forgery problems et al), authentication and access control, session handling, transport encryption and error handling.

Additionally, we will look at specific flaws that may be associated with the the client's applications including whether: -

- It is possible to gain unauthorised access to any administrative functions;
- Customers can gain unauthorised access to other customer's data or there are no Personally Identifiable Information (PII) exposures that would lead to incompliance with data proception laws (UK DPA, EU GDPR);
- That there are no flaws in the registration, identification and authentication processes;
- Whether payment processes can be subverted or are not compliant with the Payment Card Industry (PCI) Data Security Standard (DSS);

1)Mobile Applications - To deliver a mobile application security test of the iOS and Android applications, provided by the client.

To test the mobile applications providing the front-end to customer data, including how they are installed and configured on both iOS and Android devices. We will also look at how the application is installed on a device and identify any flaws in its operation.

The testing will also include reverse engineering and Java source code analysis will be undertaken of the Android code, looking for obvious weaknesses (for example, static keys in the code, security mechanisms, effectiveness of code obfuscation et al).

We will look at specific high-risk flaws that may be associated with the mobile applications including ensuring that:

- Unnecessary screens, functionality, activities, services, broadcast receivers are not present in the applications;
- It is not possible to gain unauthorised access to any administrative functions;
- Customers cannot gain unauthorised access to other customer's data;
- That there are no flaws in the registration, identification and authentication processes;
- Data is properly protected at rest and in transit;
- That the application's core security controls around data (ticket) storage cannot be circumvented;
- Sensitive functions such as payments authentication, authorisation and account management cannot be accessed via runtime manipulation; and
- Adequate protective measures have been built into the applications including code obfuscation, jailbreak detection, certificate pinning, code hashing, use of native code for sensitive functions et al.

Web Application Testing:

To test the web application layer providing the front-end to the client's applications:

The security of the applications will be investigated remotely. Prism Infosec will interact with the applications and attempt to identify any common security flaws in the application code (following the OWASP Top 10 framework), including input validation (various injection types, cross site scripting and request forgery problems et al), authentication and access control, session handling, transport encryption and error handling.

Additionally, we will look at specific flaws that may be associated with the business logic of the applications including whether:

- That any objects stored within the application are properly protected;
- That it is not possible to manipulate any process;
- That there are no flaws in the registration, identification and authentication processes;
- That it is not possible to access functions within the application outside of a user's defined role;
- That there is no information leakage in the localised Javascript that would assist an attacker with compromising the API;
- That HTML5 local storage it adequately protected and does not leak sensitive information;
- That data imports and exports into and from the application respectively are suitable validated; and
- That the platform complies with regulatory requirements, e.g. for the protection of any personal data.

Phishing Simulation / Social Engineering:

Prism Infosec shall use its in-house social engineering / phishing server (setup to support DKIM and SPF records to bypass spam filters) and the "Gophish" campaign software to conduct a phishing attack security assessment to the client. Prism Infosec can either source the target list from our open source investigation or be provided with lists of personnel from the client. From initial discussions, the client will provide an agreed list.

Prism Infosec shall then agree and design the campaign scenario with the client which could vary, such as appearing to originate from internal support (using the client's logos and mail footers) or others from external entities (cloud providers, competitions, Covid related etc). The mails shall then provide a link to a website which will require input of potentially sensitive details such as email address and/or a password as part of an additional prompt.

Prism Infosec will schedule the phishing attack scenario to take place on a date agreed with the client and this will be targeted to approx. XXX members of staff.

It is proposed that the results will show statistics (usernames and IP addresses) of the personnel that opened the mail item (if the mail client will download remote images), those that clicked on the link and those that entered information into the target website.

Recommendations will be made on security awareness training and techniques that can be made to improve staff susceptibility to phishing attacks.

Red Teaming:

Prism Infosec has recently led the delivery of a red teaming engagement of clients in the United Kingdom with offices in three locations, including head offices, contact centre and technical premises. The testing allowed for any break-in technique over the period of 3 months and included physical break-in, placement of custom inhouse “black box” using 4G and wireless for persistent remote unauthorised access, phishing campaigns, delivery of branded USB sticks, standard external attacks (with decoys) et al.

Any red team engagement would authorise Prism Infosec to attempt a break-in using any means necessary and could include one or more of the following techniques:

- Phishing attack / custom malware;
- Telephony or physical social engineering;
- Malicious removeable media sent to office premises;
- Physical break-in;
- Network compromise; and
- Other attack methods.

Only senior management within the organisation will be aware of the attacks. Prism Infosec shall attempt to be as stealthy as possible with the aim to infiltrate the client, escalate privileges, gain access to target resources and exfiltrate them without being identified by internal monitoring personnel (“Blue Team”).

The output shall be a full narrative of the red team exercise, including source material and evidence, along with description of security measures that were compromised as well as those that were successful in identifying our attacks and how they were responded to by internal security.

Following the exercise Prism Infosec will work with the blue team to understand which attacks were identified and those that were not. There shall then be knowledge handover to the Blue Team to improve security monitoring and protection techniques within the client.

Physical / Building / Premises Security Review:

Prism Infosec can conduct a physical security assessment of client buildings. The testing shall include initial reconnaissance of the buildings to determine whether there are any alternative means to gain physical access (via loading bays or fire exits) and also to understand security measures that are deployed to protect standard entrance via reception.

Different break-in scenarios will be attempted pertaining to each building, these could include attempting to clone a staff pass, using social engineering or tailgating techniques to bypass standard security, gaining access via a loading bay or fire escape or gaining access to useful information at the organisation’s perimeter.

Tests will be scheduled at different times of the day (e.g. lunchtime, early morning, evening / weekends) to determine whether any change in security controls occur.

Should a breach be successful, Prism Infosec can then go on to determine whether access can be gained to sensitive information internally (e.g. in/on desks or whiteboards) or how long access could be gained to the network (e.g. in a meeting room), or whether access could be gained to more sensitive environments such as a data room.

The output shall be a report pertaining to each location investigated, including photographic evidence of any breach and recommendations on how security can be improved.

Server and Appliance Build Review:

Prism Infosec review the build of the appliances and device Operating Systems, against common best practice standards including the Centre for Internet Security (CIS) and DISA. The testing shall review any hardening controls as well as the individual configuration of security settings applied to the Operating Systems.

All testing shall consider the role that the device is being deployed into and shall incorporate reviews of settings including but not limited to:

- Account security;
- Password security;
- Audit settings;
- File, drive and registry permissions;
- Kernel settings;
- Scheduling (cron, Windows scheduler)
- Network protection (e.g. handling of re-directs, protection against starvation)
- Desktop lockdown;
- Sensitive files;

Furthermore, appliances and databases shall be investigated to establish whether:-

- Application to database access roles and rights follow the concepts of least privilege;
- Default DB accounts are removed, disabled or protected with strong passwords;
- Database and appliance logging is adequate;
- Internal database and listener security settings are optimal;
- Dangerous stored procedures and other additional but often unnecessary features are removed;
- Management interfaces are not unnecessarily exposed;
- Databases are encrypted;
- Databases are backed up and stored in a secure manner;
- Databases and webservers have been sufficiently separated;
- Data depersonalization is being conducted;
- Password managers have sufficient access rights;
- The Organisational leavers policy ensures management credentials known by the leaver for the password manager are changed;
- Password managers databases are securely backed up and stored;
- SNMP and other logging / reporting protocols are encrypted and authenticated in line with best practice;
- Access rights have not been freely distributed among administrators; and
- Password repository administrative credentials are strong and regularly changed.

The output from the assessment shall be a report pertaining to each Operating System that contains a list of prioritised security vulnerabilities, weaknesses and issues. Recommendations shall be made on how these can be effectively remediated.

Wireless Security Assessment:

The security of wireless networks shall be investigated at given locations. Testing shall be undertaken from a number of different viewpoints, where available, as an anonymous attacker with no access, with guest (Internet) access, as a Bring Your Own Device (BYOD) user and as a corporate user with full access to the network.

Wireless networks on both 2.4Ghz and 5Ghz shall be identified and analysed for security vulnerabilities including ensuring that they are using commensurate levels of security for the type of network that is being investigated. Where a security type such as WPA2-PSK is supported for a corporate network, then Prism Infosec shall attempt to gain a handshake (either naturally or using a de-auth attack) and conduct an offline attack on the hash.

Network segregation testing shall be carried out between guest, BYOD and corporate networks to ensure that they are separate and that shared resources (such as corporate DNS) is not being used to provide services to less trusted networks.

Additionally, we shall conduct reviews of the Access Points to ensure that they are not susceptible to recent vulnerabilities such as “KRACK” and do not support deprecated protocols such as WPA-TKIP and WEP.

Prepare

Prepare your organisation for cyber security threats.

Prepare your organisation for cyber security threats. Understand your current posture and strengthen your defences. We can help you get ahead of the risks with tailored testing, preparedness services and red teaming.

- Cyber Security Assessments & Penetration Testing
- Cloud Security
- Red Teaming & Simulated Attack
- Regulated Testing Schemes

Respond

Respond effectively to cyber security incidents.

Take control when incidents strike and recover with the confidence to move forward. Specialist support to help you respond to cyber threats and restore operations quickly.

- Remediation Services
- Incident Response
- Digital Forensics

Manage

Manage your ongoing cyber security resilience.

Build long-term resilience with ongoing support and consultancy. From strategic governance to fully managed SOC services and incident response retainers.

- Managed Security Services
- GRC & Security Consulting
- Compliance Services
- vCISO

About Prism Infosec

Prism Infosec is an Information Security company based in Cheltenham and Liverpool and was founded in 2006. The Company has delivered information security consultancy and assessment services to some of the world's largest organisations including private enterpise, public sector, government, defence and healthcare. Uniquely, Prism Infosec's consultants possess both a business and management focus, but also a diverse range of technical skills. Whether delivering advice on cutting edge information security architectural solutions, conducting management controls audits, or in-depth technical penetration testing, our consultants always deliver a quality end-to-end service.

To book an assessment call:
+44 (0) 1242 652100

Send us an enquiry email:
contact@prisminfosec.com