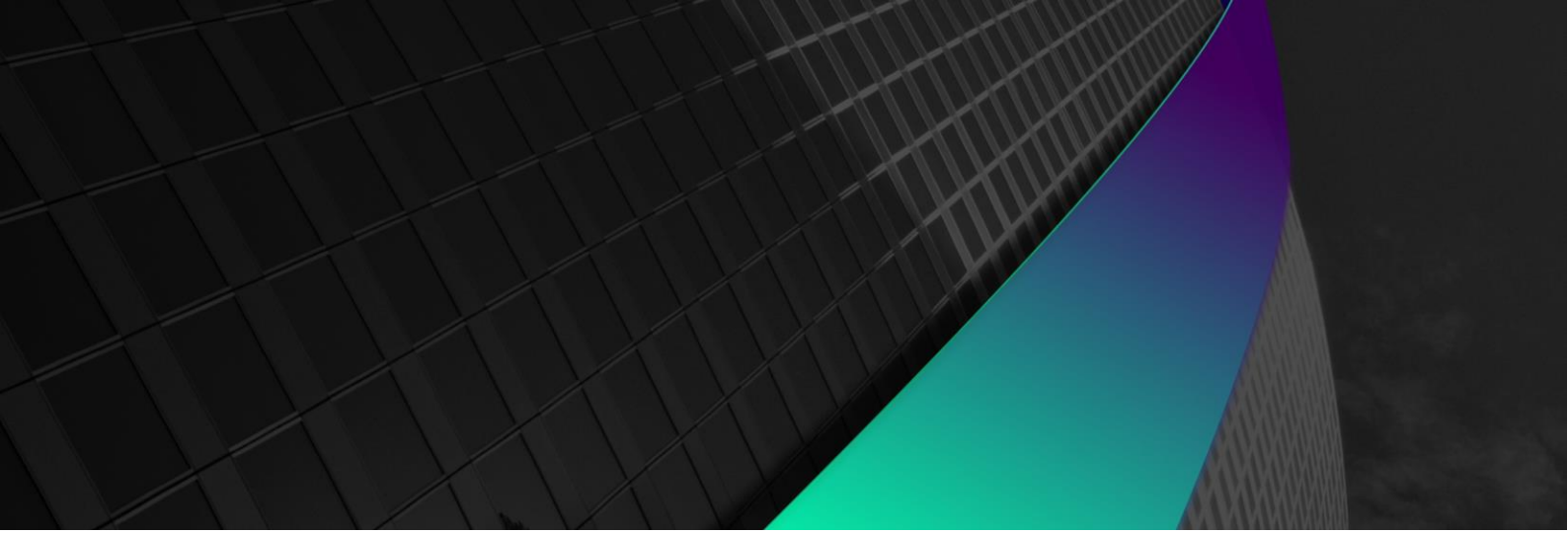

PRISM INFOSEC

IT Security Testing Service Sheets

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR | CREST | VA | PEN TEST | STAR Intelligence-led PT | AAC ISO 9001 Registered | UKAS MANAGEMENT SYSTEMS 8190 | ISO 27001 ISOQAR REGISTERED Cert: 17975 | CYBER ESSENTIALS CERTIFIED PLUS

Crown Commercial Service Supplier | pci WINNER Awards for Excellence 2020 | UK Civil Aviation Authority ASSURE | Assured Service Provider in association with National Cyber Security Centre CHECK Penetration Testing

1 Document Properties

1.1 Confidentiality & Copyright

The information contained within this proposal, including the approach, methodology and pricing, is to be considered confidential to Prism Infosec Ltd and may not be disclosed in whole or in part, to any other organisation without our previous authorisation in writing.

Date	Author	Version	Details
		0.1	Doc Setup
		0.2	Technical QA
		0.3	Management QA
		1.0	Release to Client

Table 1 – Version Information

Document Reference: PRISM-XXXX
Issued Version: 1.0
Author:
QA:
FAO:

1.2 Contact Details

+44 (0) 1242 652100

https://twitter.com/prisminfosec

contact@prisminfosec.com

https://prisminfosec.com

https://www.linkedin.com/company/prism-infosec-ltd/

Cheltenham Office:

Prism Infosec Ltd
1003/1004, Eagle Tower
Montpellier Drive
Cheltenham
Gloucestershire
GL50 1TA

Liverpool Office:

Prism Infosec Ltd
Suite 106
ABC Offices
58 Breckfield Road South
Liverpool
L6 5DR

Prism Infosec Ltd is a company registered in England & Wales with registration number 5985734 and with a registered address: Prism Infosec Ltd, 1003/1004, Eagle Tower, Montpellier Drive, Cheltenham, GL50 1TA.

VAT Number: GB 879 7957 24
DUNS Number: 67-146-5920

1.3 About Prism Infosec

Prism Infosec is an award-winning cyber security consultancy based in Cheltenham and Liverpool, UK and was founded in 2006. The Company has delivered information security consultancy and assessment services to some of the world's largest organisations.

Uniquely, Prism Infosec's consultants possess both business and management focus but also a broad range of technical skill. 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.

It is our ethos that our clients work with professional and experienced consultants (all background checked and vetted to the BS:7858 standard as a minimum and UK HMG clearance where necessary) at all times and customer satisfaction is our number one priority. We always ensure a prompt and efficient service and provide deliverables that can be used effectively by our audience at any level of the business.

Prism Infosec is a member of the NCSC CHECK scheme and a STAR member of CREST, the not for profit organisation that serves the needs of a technical information security marketplace requiring the services of a regulated professional services industry.

We are also certified to the UK Government originated Cyber Essentials Plus (CE+) scheme which independently verified that our workstations and Internet connectivity are setup securely to the standard defined by the National Cyber Security Centre. Prism Infosec is a Cyber Essentials Plus certifying body, so we also offer certification services to our clients.

Prism Infosec also maintain an ISO9001:2015 certified (UKAS-accredited) Quality Management System (QMS) and ISO27001:2013 certified (again UKAS-accredited) ISMS which ensures that quality and information security is at the heart of all our service offerings and client relationships. Prism Infosec is also a Payment Card Industry Qualified Security Assessor (QSA) Company.

The Company prides itself on the delivery of complex engagements to its customers, across a number of our service offerings: -

- ISO27001 Implementation Support through to Certification;
- PCI QSA Projects;
- Risk Assessments and Gap Analysis;
- Simulated Cyber Attacks;
- Civil Aviation Authority (CAA) ASSURE Audits;
- Governance, Risk and Compliance; and
- Enterprise Penetration Testing and Red Teaming.

Prism Infosec's innovative approach to the delivery of PCI projects and technical security testing was recognised with a PCI Award for Technical Excellence in January 2020. The award was presented for the delivery of a client project that was considered by the review panel to be an outstanding example of best practice.

2 Contents

3 Approach to Delivery

3.1 Open-Source Intelligence

Prism Infosec can conduct an open-source discovery / intelligence gathering exercise on THE CLIENT. Prism Infosec has recently conducted an information gathering exercise on a UK-based financial institution. This included finding mechanisms to bypass cloud-based Anti-Virus services, identifying ranges hosting test and development content with potential exposures and key case studies that could be used to compromise the physical security of a building.

The open source gathering exercise will include conducting reviews of public information sources such as company registration documents, IP and DNS registration records, company public web server records (including within the source of web pages), search engines, public forums, partner case studies, internal / external SMTP Servers, social media (Linked In, Facebook, Twitter, Instagram, et al) newgroups and dark web (TOR) accessible web sites. Using well-known tools such as "Maltego", Prism Infosec shall locate and track information and connections pertaining to agreed elements of THE CLIENT that would assist an attacker in conducting attacks against the organisation.

Our report shall document the information and highlight any areas that would be considered by THE CLIENT to be sensitive information leakage. Examples of this include (but is not limited to): -

- The names and contact details of key technical and management staff – could be used in a phishing campaign;
- Internal IP addressing details;
- Case studies and IPR leaks in pastebin / other sources;
- Target domain users with details leaked in previous third-party organisational password compromises;
- Technologies used within the organisation, particularly device endpoints, servers, firewalls, intrusion detection, network and client Anti-Virus
- Potentially derogatory or negative Internet postings;
- Internal / external domains; and
- Corporate network ranges and remote access endpoints.

All information that is found will be used, where possible, in subsequent test phases. For example, names or email addresses can be converted into usernames for infrastructure (e.g. IPSEC / SSL VPNs) or logins for application tests. Information could also be used in social engineering, phishing and red teaming exercises.

3.2 Vulnerability Assessments

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 CLIENT have requested Prism Infosec to provide quarterly scanning assessments. 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.

3.3 External Infrastructure Penetration Test

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, detailed in Appendix A, 12.1.1.

3.4 Internal Infrastructure Penetration Test

Prism Infosec has conducted many internal infrastructure penetration tests, across a variety of organisations ranging from SME to multinational. As part of the initial setup, Prism Infosec always seeks to understand key objectives pertaining to the internal penetration test, including attempting to gain unauthorised access to sensitive data or systems within the organisation. Where possible, we work with the client to try and define target "flags" which can be used to measure whether the objectives could be attained given the time available and allocated to the assessment.

The tests are mainly conducted from a "black box" perspective without any privileges provided, other than access to a desk and network connection.

Often, this also requires bypassing controls such as 802.1x network access control. Additionally, Prism Infosec has experience in working in datacentres on the delivery of reviews of n-tier application architecture, segregated network zones or testing based upon PCI penetration testing requirements.

Internal testing will be conducted, from zero knowledge other than having gained a network connection (using in-house scripts designed to bypass 802.1x / Network Access Control) and without any further access rights (e.g. domain user). Prism Infosec shall use network mapping and scanning tools to locate targets of interest (authentication servers, databases, application servers, workstations of support staff et al) in an attempt to gain access to sensitive data within the organisation and to escalate privileges from network access to domain administrator.

The Active Directory servers within the organisation shall be analysed for vulnerabilities and weaknesses, including username enumeration attacks, issues with patching, further unnecessary software installed on them.

They shall also be investigated for susceptibility to known vulnerabilities and weaknesses such as Kerberos Golden Ticket, use of deprecated hash (LM) and encryption formats (SMBv1), adequate message signing is enabled on the domain and whether administrators are carrying out regular assessments of such attacks.

Where vulnerabilities and weaknesses are identified within the environment, Prism Infosec shall conduct (with permission) controlled exploitation attempts to compromise systems and applications and to gain increased permissions to devices on the network.

Should access be gained, further reviews and privilege escalation attempts shall be attempted, including password gathering and cracking, pass the hash attacks, pivoting to other systems and networks within the environment. Attempts will be made to leverage further access into other systems and to gain access to sensitive data and key objectives.

Our internal testing methodology follows a refined test methodology that ensures a comprehensive attack simulation against the organisation, detailed in Appendix A, 12.1.1.

3.5 Web Application Security Assessment

External (Internet) Web Application Penetration Test – To test the web application layer providing the front-end to the CLIENT applications, following the methodology outlined in Appendix A, 12.1.2.

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.

3.6 Application Programming Interface (API) Security Assessment

The web service endpoints will be investigated following the testing methodology in Appendix A, 12.1.3. Prism Infosec will investigate the web services' input validation, authentication and authorisation functions to ensure that they are well setup and configured.

The API assessment will investigate the security controls of the API interfaces and its associated commands and data and will "fuzz" the API to determine how it handles malformed input and data types. Prism Infosec shall ensure that malformed input messages does not result in significant information leakage such as stack traces and instructions on how to build syntactically correct queries, all of which would assist an attacker.

This will include ensuring that adequate whitelisting has been implemented to ensure that API cannot be abused from IP addresses that are not associated with the service (where public access is not required).

Additionally, Prism Infosec shall investigate the handling of data passed over the APIs. This will include fuzzing of fields being passed into the endpoint for common attacks such as data injection techniques and incorrect input / output validation which normally lead to attacks such as Cross Site Scripting against support agents.

In particular, we will investigate whether: -

- The APIs are suitably whitelisted (where appropriate);
- The APIs are properly authenticated;
- The APIs are properly encrypted;
- The data in the APIs is sufficiently handled and validated such that it does not pose a risk to the consent handling servers or agents.

The scope will include: -

- Network connectivity (e.g. encryption in transit) – applied to public-facing IP addresses;
- Vulnerability assessment (e.g. OWASP Top 10) – applied to public-facing IP addresses and the RESTful interfaces;
- API security (e.g. RESTful) sampled testing of the RESTful interfaces and API message handling;
- Access controls (e.g. RBAC) – applied to the RESTful interfaces – validation of authentication and access control pertaining to message calls;

3.7 Mobile Application Security Assessment

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 following the infrastructure methodology, as shown in Appendix A, 12.1.1. In particular, this will cover the security of any exposed interfaces including: -

    a. 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;

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

2) **Web Service Endpoints Message Handling** - The web service endpoints will be investigated following the application layer testing methodology, as shown in Appendix A, 12.1.3. 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 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);

3) **Mobile Applications** - To deliver a mobile application security test of the iOS and Android applications, provided by THE CLIENT, following the mobile application testing methodology shown in Appendix A, 12.1.4.

    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.

3.8 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.

3.9 Source Code Review

Prism Infosec can conduct source code analysis of client desktop, web and mobile applications, using a combination of automated static analysis and manual reviews. Prism Infosec has completed source code analysis over the last 12 months in the following languages: -

- Oracle Java;
- Microsoft C# / ASP.NET;
- PHP;
- Ruby;

- ABAP;
- C/C++;
- Swift; and
- Objective C.

In these engagements Prism Infosec has identified serious issues pertaining to SQL injection, cross site scripting and potentially malicious code.

Prism Infosec can identify flaws in the source code, which typically range from serious issues associated with command execution, database queries, backdoor code and input validation through to issues associated with class instantiation, code structure weaknesses, exception handling, session management and logging of sensitive data.

The output of the exercise will be a report pertaining to the individual applications and will include detailed information on any vulnerabilities and weaknesses identified, with example indicative code and affected code classes/modules and associated line numbers. Furthermore, pragmatic recommendations will be provided on how issues can be remediated, including the approach to correct code standards.

Whilst this will not be a full manual source code review, our full source code analysis methodology can be viewed in Appendix A – Section 12.1.5.

3.10 Physical Security Assessments

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.

3.11 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.

3.12 Phishing Attack Security Assessment

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 Bell Integration 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.

3.13 Server and Appliance Security 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.

3.14 Active Directory Security Review

Active Directory is widely used to configure access to all resources on a Windows estate. Thus, it is of paramount importance that Active Directory be configured securely. Common misconfigurations can lead to unauthorised access to resources. An Active Directory audit will carry out an in-depth assessment of the configuration

against current best practices. Common issues include poor password policy, account lockout policy, security options, and poorly deployed group policy objects.

The assessment takes the form of a server-based audit of domain controllers. Common issues identified include:

- Insufficient patching of the servers;
- Poor application of password and account lockout policies;
- Wrongly configured or applied insecure policies and permissions;
- Poorly applied GPOs leading to incorrect configuration;
- Insufficient event auditing, and storage of logs;
- Excessive share permissions;
- Poorly defined domain trust relationships leading to excessive network access permissions; and
- Excessive users with domain admin privileges.

Active Directory audits are carried out in line with industry best practices such as SANS and CIS, together with our own experience.

3.15 Patch Management Review

Prism Infosec conduct a scan of the environment during an assessment to determine whether there are any missing security patches (pertaining to both the underlying Operating System or additional software installed) or outdated / unsupported software versions on the network. Additionally, the scan will detect other misconfigurations that could lead to privilege escalation on the system such as unquoted Microsoft service paths, or permission issues on system drives.

Prism Infosec use the Tenable Nessus Professional tool to conduct the assessment and will present the results in the report, with particular focus on software or missing patches with exploits that are available and which should be remediated as a matter of urgency, followed by other issues that should be remediated at a lower priority.

3.16 Network Design and Segmentation

Prism Infosec review the design of the network with a THE CLIENT network architect to understand the layout of the network and particular sensitive zones and data flows. We aim to understand areas of sensitivity including hosting of data considered sensitive to the organisation, management interfaces and logging / Intrusion Detection facilities. Common network zones such as DMZs and storage areas will be identified, and we will determine permitted traffic flows and how access is managed to those network areas.

Prism Infosec then conduct network segmentation testing of the core zones encountered. This ensures that IP protocols and traffic types including ICMP, UDP (common ports) and TCP (common ports) are being properly segregated between zones. Where any traffic flow or high-level architectural weakness is identified, this shall be reported to THE CLIENT.

Additionally, we sweep each network under test to ensure that there are no high-risk vulnerabilities and weaknesses in any of the devices on that network, which should be immediately remediated as it may lead to immediate system breach.

3.17 Workstation Security Assessment

Prism Infosec assess the security posture and attack resilience of standard workstation builds. The workstation build review will focus on assessing whether the builds are affected by any vulnerabilities that could be used to elevate an attacker's position within the network. The assessment will also involve testing the build's resilience and technical controls to combat malicious intrusion by a weaponised file or suspicious/dangerous activity.

The assessment will include but is not limited to the following tests, to ensure that:-

- The build is not susceptible to local privilege escalation vulnerabilities;
- User rights have been sufficiently locked down;
- User's cannot make changes to the registry;
- Antivirus protection is operating properly on the builds;
- The Antivirus solution cannot be evaded;
- There is sufficient logging of activity on the build and are the logs are being stored elsewhere and parsed into a SIEM solution;
- PowerShell and other scripting/development tools have been adequately restricted;
- Unauthorised / unnecessary command execution is not possible;
- Local password hashes or other sensitive data cannot be obtained;
- Unnecessary Internet access is being restricted; and
- Removable media is blocked in line with organisational policies.

Prism Infosec review the build of the Operating Systems (whether standard desktops/laptops or AWS machine images for Windows/Linux), against common best practice standards including the Centre for Internet Security (CIS) and DISA. The testing reviews any desktop hardening controls (for graphical based systems) 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;

The output from the assessment would 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.

3.18 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.

3.19 Mobile Device Management Review

The Mobile Device Management solutions shall be reviewed to ensure that it is operating correctly, and that the policies implemented are effectively matching the business objectives associated with the use of mobile devices.

In particular, we shall assess whether: -

- The MDM is providing reasonable coverage of the estate;
- The MDM is tracking device firmware versions correctly;
- That adequate device authentication and access control functions are setup;
- That device storage and encryption is properly implemented;
- That unnecessary mobile device functions (such as file sharing over Bluetooth functions, or use of storage devices) are disabled in line with company policy;
- That devices can be locked or wiped if necessary and within a reasonable timeframe.

The configuration shall be reviewed in line with company policy (which we will seek to understand prior to the assessment) as well as industry best practice from sources such as the National Cyber Security Centre End User Device (EUD) guidance, as well as the Centre for Internet Security (CIS) Benchmarks.

The output shall be a report detailing any gaps in the configuration, the associated risk profile and recommendations that could be implemented to address those risks.

3.20 Stolen Endpoint Test

The assessment is expected to determine any weaknesses that could be exposed should a THE CLIENT endpoint be lost or stolen or be targeted by a malicious user.

Prism Infosec appreciates that organisation laptops can have the same access and privileges as those connected directly to an internal network but are at greater risk of compromise if lost or stolen. As part of our methodology Prism Infosec will look to circumvent security controls from a zero-knowledge perspective in the guise of a malicious attacker. We will look to identify flaws in the operating system hardware and software, and its network bios including, but not limited to, the following types of activity:

- Physical inspection of the device with the aim of identifying organisational information or attached password and pins;
- Attempts to configure/access the BIOS to allow for booting from alternate media such as floppy drives, CD-ROM and USB devices;
- Attempts to access hard disks either through alternate operating systems or after bypassing authentication measures;
- Search of hard drives for sensitive data, deleted files and cached credentials; and
- Attempt to access corporate network through any pre-configured VPN connections and using any user accounts and passwords identified.

Additionally, Prism Infosec will conduct an authenticated review of the device/workstation endpoint, against common best practice standards including the Centre for Internet Security (CIS) and DISA. The testing reviews any device hardening controls (for graphical based systems) 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; and
- Sensitive files.

3.21 Remote Access Solution Security Review

Prism Infosec conduct a review of the security of technologies used to gain remote access to the organisation. This shall include assessing: -

- Encryption strength used to protect data in transit;
- Authentication strength used, including the use of multiple factors;
- Information leakage from endpoints;
- Susceptibility of the endpoint to compromise using known exploits;
- Validation of trusted clients (patch checking, AV checks, trusted machine etc); and
- Access provided to authorised clients and strong network architecture.

The output from the assessment shall be a report detailing any gaps in the configuration and pragmatic recommendations on how to implement improvements.

3.22 VoIP Security Assessment

Prism Infosec can assess the security of the VoIP implementation, including on-premise devices, the supporting networks and infrastructure as well as the cloud-based portal. This will include a phased approach which will cover reviewing the: -

- **VoIP phones and Handset Physical Interface Security** – to ensure that information leakage is minimised from the interface, access to sensitive settings is restricted and default PINs have been set. Additionally, to ensure that it is not possible to compromise voicemail settings or conduct toll fraud associated with out of country call forwarding and other malicious call techniques;

- **Network connectivity and Data Port Access** – ensuring that robust network architecture is in place and that data and voice networks are not aggregate and are robustly separated either physically, on VLANs or using VLAN tagging. Also, to review the security of any network access control (802.1x) that has been implemented and to try and compromise it using bespoke hardware which will bridge a rogue device to an authentication session. Attempts will be made to "hop" from data VLANs onto the telephony network;

- **Device Network Security** – following standard penetration testing methodology reviewing the configuration of the phones and the supporting infrastructure (call managers, routers, gateways etc) to ensure that management interfaces are not available and/or properly locked down and that it is not possible to gain unauthorised access to devices on the VoIP network and that information leakage is minimised and that devices (firmware, management interfaces, ancillary network servers et al) are properly patched and up to date;

- **Communications Security** – Prism Infosec shall review the communications passing across the network and ensure that it is adequately encrypted and/or adequately protected from compromise from man-in-the-middle attackers. As a Proof of Concept, Prism Infosec shall attempt to record a call initiated by ourselves between two handsets from a separate access point;

- **External Interactions** – where external interactions are made, for example to cloud-based management solutions for the VoIP service or Internet-facing SIP gateways Prism Infosec shall review the security of those interfaces to ensure that they are suitably secured, patched and maintained. Interfaces shall be tested for default accounts or SIP access strings. Additionally, access to cloud-based service management interfaces shall be reviewed from a white box perspective (i.e. with administrative accounts) to ensure that accounts and settings are adequately setup in line with our configuration review methodology and that VoIP specific settings are optimal with regard to cyber security.

Open-source tools shall be used to conduct the assessment, including "Cain & Abel", VoIPhopper, sipcrack, sipdump et al, as well as other common penetration testing tools listed in the other sections.

3.23 GitHub Repositories Testing

The methodology outlined below provides a comprehensive approach to assessing the security of using GitHub within an organisation. The methodology details the process of ensuring that updating and releasing code is done with security best practices, and that the deployment pipeline is secure and efficient.

Testing the access rights across a company's GitHub implementation helps to identify any potential weaknesses in the configuration that could be abused, such as unauthorized access by former employees, or overly permissive rights. By verifying that each user has the correct level of access to the repositories, we can help to prevent unauthorized access to sensitive information, reduce the risk of data breaches, and maintain the confidentiality, integrity, and availability of information.

Prism Infosec shall review the existing process for updating and releasing code via the following process:

1. Familiarise and evaluate the client's code release process.
2. Review the companies code repositories and previous code released to understand the current practices and identify potential areas for improvement.
3. Evaluate the existing review process.
4. Verify objectives and scope of code reviews, including expected outcomes.
5. Evaluate the company's existing process for releasing code.
6. Identify gaps or areas for improvements when releasing code.
7. Evaluate the use of comments within code commits merge requests and code.

Prism Infosec will test the access rights across different repositories, as outlined below:

- Identify the different types of users and their associated roles within the GitHub organisation.
- Test the permissions of each role to determine if they have the correct level of access to the repositories.
- Verify that sensitive data is properly secured and encrypted, and that access to it is restricted to authorised users only.
- Evaluate the use of multi-factor authentication for privileged users and verify that it is properly configured and enabled.
- Test the process for revoking access for former employees or contractors to ensure that their access is terminated in a timely and secure manner.

3.24 Cloud Security 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.

3.25 AWS Security Configuration Review

The purpose of an Amazon Web Services (AWS) Security Configuration Review is to assess the security posture of resources hosted within AWS. This can provide additional security assurance for a project in the case that a staff member's AWS account or an AWS 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 AWS 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:

- EC2 Configuration Review
- Security Group and Network Access Control List Review
- Review the Cloud Configuration of Elastic Beanstalk and API Gateway Deployments
- Review of Lambda Cloud Configurations
- Review of both Public and Private S3 Buckets
- DynamoDB, Aurora and RDS Configuration Review
- Review Deployed AWS Step Functions
- Review of Deployed Simple Notification/Queue Services
- Elastic Load Balancing Cloud Configuration Review
- IAM Permissions Review
- CloudWatch and GuardDuty Configuration
- Review of AWS Settings for other relevant Deployed AWS 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.

3.26 Azure Security Configuration Review

The purpose of an Azure Security Configuration Review is to assess the security posture of resources hosted within Azure. This can provide additional security assurance for a project in the case that a staff member's Azure account or an Azure 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 Azure 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:

- Azure VM Cloud Configuration Review
- Network Security Group and Azure Firewall Review
- Review the Cloud Configuration of Azure App Service Deployments
- Review of Azure Functions Cloud Configurations
- Review of both Public and Private Storage Accounts
- Cosmos, Azure Database and Azure SQL Configuration Review
- Review Deployed Logic Apps
- Review of Deployed Storage Queues and Service Buses
- Load Balancer, Application Gateway and Front Door Cloud Configuration Review
- Azure and Entra Roles and Permissions Review
- Anomaly Detector, Defender and Sentinel Configuration
- Review of Azure Settings for other relevant Deployed Azure 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.

3.27 GCP Security Configuration Review

The purpose of a Google Cloud Platform (GCP) Security Configuration Review is to assess the security posture of resources hosted within GCP. This can provide additional security assurance for a project in the case that a staff member's GCP account or a GCP 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 GCP 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:

- Compute Engine Configuration Review
- VPC Firewall Review
- Review the Cloud Configuration of App Engine Deployments
- Review of Cloud Functions Configurations
- Review of both Public and Private Cloud Storage
- Firestore, Cloud SQL and Cloud Spanner Configuration Review
- Review Deployed Cloud Tasks
- Review of Deployed Pub/Sub resources
- Cloud Load Balancing Configuration Review
- IAM Review
- Anomaly Detection and Chronicle Configuration
- Review of GCP Settings for other relevant Deployed GCP 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.

3.28 Reporting

Following the penetration testing assessments, Prism Infosec shall provide a full technical report. The report shall be delivered within a maximum period of 10 working days following the last day of the testing.

All elements of the assessment shall be comprehensively reported, including details of issues identified and include practical recommendations and references to further information. The report will be delivered within the agreed timescales following the conclusion of the testing.

Prism Infosec shall produce and deliver a report containing the following sections:

- **Management Summary** – detailing a non-technical management overview of the testing;
- **Introduction, Scope & Approach** – outlining the objectives of the testing and our approach to delivering it;
- **Technical Findings** – delivering the output of the testing, including detailed findings, practical recommendations, risk priorities and references to further information; and
- **Appendices** – further supplementary evidence and screenshots.

A summary report can be made available at THE CLIENT's request in advance of the full report. The summary report is provided as a brief summary of the issues that were identified during the assessment, before the full report has been issued. This summary report provides:

- a management summary
- a list of the findings
- the risk score (CVSS rating)
- the recommendation

Reporting requirements can be discussed and refined during the initial scope of work call for each security assessment.

3.29 Re-Testing

Following a period of remediation conducted by the client, Prism Infosec will conduct a retest of all critical and high-risk issues identified during the security assessment. This effort will be limited to a single day with focus upon the critical issues, with remaining time allocated to any high-risk issues as time permits.

Should no critical or high-risk issues be identified then the focus will be on the lower risk issues identified within the security assessment report.

This retest activity must be scheduled within 30 days from the delivery of the security assessment report.

4 Project Team – Sample Profiles

Prism Infosec will deploy a team of experienced consultants on the THE CLIENT project. The table below provides sample profiles from within our team.

Phil R **Project Lead, QSA & Company Director**	Phil has worked in information security for over 20 years, having originally worked on the security of Unix systems in his first position as a Systems Engineer and later Security Architect at NTL (now Virgin Media). Phil has worked in penetration testing and security consultancy since April 2000, having previously worked as a director / founder at IRM Plc and Digital Assurance. Phil has contributed to the development of well-known hacking tools (such as THC-Hydra) as well as publications (Hacker's Challenge 3, Osborne and the Open Source Testing Methodology Manual [OSSTMM]). Phil has previously found and published CVEs. Phil is a CREST Tester (Infrastructure) a CISSP, CISA, PCI QSA and Chartered Member of the British Computer Society. Phil has previously delivered security assessments and consultancy to the UK Government (CHECK TEAM LEADER and CLAS) as well as multinational organisations such as Google and Vodafone. He will be responsible for leading the testing and the end-to-end quality of the project and associated deliverables. Phil is also registered with the PCI Council as a certified QSA.
Alan M **Senior Security Consultant**	Alan is a Senior, CREST qualified, consultant who has been working in the Information Security industry since 2011, for global companies such as Cisco, Finmeccanica and Marconi. For over 7 years Alan has worked in an integral role within penetration teams catering for both Government and public-sector organisations and has partaken in numerous penetration tests across different disciplines and on various platforms. Additionally, Alan has a strong background in software development and testing, both at an application, component and a system level. A very able communicator Alan has built relationships at all levels, from a technical to executive. Overseen by the project lead, Alan will be responsible for core elements of the technical testing.
Alexis VE **Senior Security Consultant**	Alexis is a senior consultant with over 8 years' professional experience within the security industry and has worked with several security consultancies including MDSec and A&O Corsaire. Alexis has a background in software development and has used this to develop tools and training material specifically focused on security, this has included building custom extensions for widely popular testing tools such as PortSwigger's Burp Suite. Alexis has also delivered web application testing training at the major security and hacking conference 'Black Hat' for two years. Alexis has performed technical security assessments for government, financial, software and other commercial and non-commercial sector customers including FTSE 100 companies. These security assessments include a range of testing services, including Application, Web-Services, Infrastructure and Mobile testing.
Mike C **Senior Security Consultant**	Mike is a security consultant with a broad range of skills and experience, and brings a fresh perspective to the area of security, drawing on a background in mechanical engineering. Mike is well-

	versed in infrastructure security, but also has a keen eye for testing web applications. As a CHECK team leader, Mike operates with a focus on industry best practices and standards. He takes a detail-oriented approach to his work and is dedicated to providing clients with the highest level of security.
Karolis N **CHECK Team Leader**	Karolis is a Cyber Scheme, CREST, CHECK and OSCP certified consultant with a First-Class award in BSc Ethical Hacking & Cyber Security. Has carried out in excess of 250 penetration tests since September 2020, with a primary focus on Web Application and API testing. Karolis has previously found and published CVEs in enterprise-level web applications and currently is a CHECK Team Leader (Web).
Ryan H **Senior Security Consultant**	Ryan is an experienced and accomplished Penetration Tester with 6 years of expertise in identifying vulnerabilities and assessing security measures for a wide range of systems. Possesses a first-class degree in Computer and Digital Forensics, complementing practical skills with a strong theoretical foundation. Proven track record of delivering high-standard tests for web applications, network infrastructure, bespoke web applications, phishing campaigns, and break out scenarios. Specialises in Active Directory offensive attack paths and incident response, providing comprehensive insights and actionable recommendations.
Shinoj J **Senior Security Consultant**	Shinoj is a senior security consultant at Prism Infosec. Shinoj has over 5+ years spanning Consultancy and Healthcare type organisations; He is a Check Team Member, and holds a BSc (Hons) in Cyber Security Management. Shinoj delivers a broad range of assessments for Prism Infosec, but is particularly adept in infrastructure and cloud-based environments. A remarkable track record of conducting thorough security assessments for organisations of all sizes and is highly proficient in not only identifying and exploiting vulnerabilities, but also working together with clients to assist in the remediation process of identified risks. Shinoj has led and delivered large and complex engagements for a range of clients, including Financial Services, Public Sector, and Corporates.
Ben A **Senior Security Consultant**	Ben is a highly skilled and experienced security consultant with over 6 years in the cyber security industry. He has a strong background in red teaming, red team tool development, malware development/analysis, reverse engineering, exploit development, web application security, and infrastructure assessment. Proven track record of identifying vulnerabilities, assessing security risks, and developing robust strategies to protect critical systems and data Ben has led and successfully delivered large scale research/penetration testing engagements for government clients and has worked on many TS level projects.

Table 4 – Sample Profiles

5 References & Previous Experience

References and previous experience are included below. All case studies relate to work completed within the last two years.

5.1 Leicestershire Police & Pervade Software

Organisation Name: Leicestershire Police / Pervade
Scope of Services Provided: Software Solution & Web App Penetration Test
Period of Contract: 2020 – ongoing

On the behalf of Leicestershire Police and Pervade Software, Prism Infosec conducted a web application and virtual machine review of the National Police Chief's Council CyberAlarm initiative.

An application assessment was conducted, with particular attention upon the potential to compromise users of the application and the protection of personal data. Testing included the login and authentication functionality across a variety of users roles and test installation/download and transmission of data logs to the receiver. Attention was focused upon the validate for potential issues, information Leakage, Man in the Middle Attacks as well as the receiver security and key exchange and any Installation / configuration weaknesses

The Web Application Security Assessment included the assessment of pre-authentication functionality providing the front-end to the Police CyberAlarm application.

Prism Infosec interacted with the application with attempts 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 tested for specific flaws that may be associated with the business logic of the application 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 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.

The output of the security assessment was a detailed security assessment report for client review which included a management summary, summary of issues, a clear indication of scope and resources involved and a comprehensive results section that includes detailed description, issue rating, supporting data and detailed recommendation for the issues identified. End of day and end of test wash up meetings where provided through the assessment including updates on issues as they were identified where they were deemed high or critical.

5.2 IASME Cyber Essentials Portal

Organisation Name: IASME
Scope of Services Provided: Software Solution & Web App Penetration Test
Period of Contract: 2020 – ongoing

As part of supporting the Cyber Essentials scheme, IASME and its supplier company have developed a portal which can be used by certifying bodies as part of the Cyber Essentials scheme to offer their clients the Self-Assessment Questionnaire (SAQ) for response and marking. The portal also allows IASME to manage the assets such as the SAQ and administer the certification bodies and CE applicant organisations.

To ensure strong due diligence on information security issues that could affect the portal, IASME approached Prism Infosec to provide to deliver a set of security tests. The tests investigated key security issues associated with web application and Application Programming Interface (API) vulnerabilities of the platform that might affect the confidentiality, integrity and availability of the data stored within the portal.

Prism Infosec delivered the information security testing services to IASME to established security testing methodologies and certified processes including those defined by CREST, the National Cyber Security Centre, the Institute for Security and Open Methodologies (ISECOM), the Open Web Application Security Project (OWASP). Prism Infosec interacted with the application 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), authentication and access control, session handling, transport encryption and error handling.

Prism Infosec investigated the web services' input validation, authentication and authorisation functions to ensure that they are well setup and configured. The API assessment investigated the security controls of the API interface and its associated commands and data and "fuzzed" the API to determine how it handles malformed input and data types. Prism Infosec shall ensure that malformed input messages does not result in significant information leakage such as stack traces and instructions on how to build syntactically correct queries, all of which would assist an attacker.

Additionally, Prism Infosec also investigated the handling of data passed over the API. This included fuzzing of fields being passed into the endpoint for common attacks such as data injection techniques and incorrect input / output validation which normally lead to attacks such as Cross Site Scripting against support agents. Prism Infosec shall investigate the handling of data passed over the API. This will include fuzzing of fields being passed into the endpoint for common attacks such as data injection techniques and incorrect input / output validation which normally lead to attacks such as Cross Site Scripting against support agents.

The output of the security assessment was a detailed security assessment report for client review which included a management summary, summary of issues, a clear indication of scope and resources involved and a comprehensive results section that includes detailed description, issue rating, supporting data and detailed recommendation for the issues identified. End of day and end of test wash up meetings where provided through the assessment including updates on issues as they were identified where they were deemed high or critical.

5.3 The National Lottery Community Fund

Organisation Name: UK Government: Derbyshire District Council
Scope of Services Provided: Organisational Penetration Test
Period of Contract: 2016 – ongoing

For over four years, Prism Infosec has provided a comprehensive set of security tests to the National Lottery Community as part of their ongoing programme of assurance for their existing IT estate as well as associated with new projects.

This programme of work has included: -

- Annual IT Health Check of the organisation, covering on-premise and cloud (Azure) deployed infrastructure;
- Enterprise web application testing of back-end grant management applications;
- Front-end web sites and APIs based upon Sharepoint and Wordpress technologies;
- Wi-Fi Security assessments;
- Network architecture and access control reviews;
- Desktop and Server Build and configuration reviews;
- External infrastructure testing;
- Social engineering and simulated phishing attacks; and
- Red team assessments on building across the United Kingdom.

The primary delivery focused upon the internal and external network infrastructure, supplemented with a range of configuration and build reviews across a wide range of hosts and operating systems. Additionally, web applications and APIs were tested on an as required basis as they were called off by TNLCF.

Testing included the full range of penetration testing services including to reviews the security of the remote access solution, including the configuration of the encryption ciphers that are used, and the exposure of the Internet interface to anonymous attacks. Additionally, Prism Infosec spent time over the entire project making attempts to compromise the organisation via any means necessary. This included conducting background research on people, premises and infrastructure within the Big Lottery Fund and attempt to bypass physical security measures. Examples of such attacks include copying / cloning access control passes, tailgating into buildings, using emails and telephony-based social engineering attempts to gain access.

We also facilitated requests made for additional call off time to be added to the proposal to be used on an ad-hoc basis where additional requirements arise or further support was to be required by TNLCF.

All projects were delivered to the complete satisfaction of the client, who has engaged Prism Infosec for further work and to provide remediation advice and management of vulnerabilities and also to assist with the implementation of Network Access Control (NAC) within the organisation.

5.4 Financial Services – Elliptic Enterprises Ltd

Organisation Name: Elliptic Enterprises Ltd
Scope of Services Provided: Web Application & API Security Assessment

Prism Infosec has provided penetration testing services for Elliptic overseen throughout by the Information Security Lead, who kindly supplied the following reference statement in respect of the Prism Infosec services:

Prism Infosec were the perfect partner for our pen testing needs. Right from the start they were highly engaged and extremely responsive, supplying quick feedback to all our queries. They provided timely updates throughout the testing engagement and delivered a detailed technical report, complete with remediation advice for all identified issues, at the end.

Their experience with API testing was obvious from the start due to the questions their testers asked and their testing methodology. I thoroughly enjoyed working with Prism and cannot wait to work with them again.

All services were delivered on agreed time and budget and the reports were fully accepted by the organisation and its accreditation bodies.

5.5 Financial Services – Aviva Group / Virgin Money

Organisation Name: Aviva Group / Virgin Money
Scope of Services Provided: Web application testing / CHAPS/FPS API testing and database reviews, Infrastructure Testing, Database configuration reviews

Prism Infosec worked on web and API penetration tests, to the head of information security in both organisations a number of years. The head of information security provides the following reference with regard to Prism Infosec's services: -

"I have experience of working with Phil and his team at Prism Infosec at Virgin Money and also in my previous role as UK IT Security Manager at Norwich Union (now the Aviva Group). This goes back over 15 years in the field of penetration testing including the delivery of internal and external infrastructure tests, web application tests and API reviews.

The quality of the work has invariably been of a high standard including their approach to testing (ensuring the scope of testing is complete and properly understood by both tester and client), relationships with both key stakeholders and technical subject matter experts and notably the quality and timeliness of their reports.

They have been punctilious about ensuring that testing is non-intrusive, takes account of the environment (particularly when testing is on Live Production Systems rather than on mirror sites) and also covers the full extent of the agreed brief.

I have no hesitation in recommending Prism Infosec under Phil Robinson's leadership for the delivery of web and infrastructure testing in a banking environment, and can think of three separate occasions this year alone when I have specifically assigned them to key pieces of work (the most recent being one of our most important and regulator visible projects this year)."

5.6 NHS England & Improvements / NHS-X

Organisation Name: NHS England & Improvements / NHS-X
Scope of Services Provided: Web App Penetration Test, Code Review, Cloud Configuration Reviews
Period of Contract: 2020 – ongoing

On the behalf of NHS England & Improvements, Prism Infosec conducted a web application testing, supporting code reviews and a review of the supporting Azure configuration of a key application that was in development.

An application assessment was conducted, with particular attention upon the potential to compromise users of the application and the protection of personal data.

Prism Infosec interacted with the application with attempts 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 tested for specific flaws that may be associated with the business logic of the application.

Furthermore, the code of the application was reviewed to identify whether there were any inherent flaws that could not be identified from the front-end.

A review of the supporting Azure and Office 365 cloud PaaS and SaaS services was also conducted to determine whether there were any gaps in the supporting platform, particularly those associated with management of the solution and the potential for unauthorised access and information leakage.

The output of the security assessment was a detailed security assessment report for client review which included a management summary, summary of issues, a clear indication of scope and resources involved and a comprehensive results section that includes detailed description, issue rating, supporting data and detailed recommendation for the issues identified. End of day and end of test wash up meetings where provided through the assessment including updates on issues as they were identified where they were deemed high or critical.

5.7 Financial Services – YBS / PFG

Organisation Name: Yorkshire Building Society / Provident Financial Group
Scope of Services Provided: Web application testing / Red Teaming

Prism Infosec worked on a package of web application tests for Yorkshire Building Society (internal and external applications) and red team engagements for Vanquis Bank / PFG on the behalf of the Head of Security who is now the Head of Information Security at Plus Net ISP. The following reference was provided with regard to Prism Infosec's services: -

"I have worked with Phil Robinson and his team in two of my previous positions as Information Security Manager at Yorkshire Building Society (UK) and Vanquis Bank

UK / Provident Financial Group. This included the delivery of internal enterprise class web application assessments and red team reviews respectively.

The tests have always been delivered with the utmost professionalism with respect to the banks' service levels, the quality of test delivery onsite and the detail in the subsequent reports. Additionally, risks and results were well articulated to all levels of the business and were at all times pragmatic and prioritised correctly.

I would have no hesitation in recommending Prism Infosec for the delivery of cyber assessment work within a Financial Services environment."

5.8 Financial Services – Schroders / Evora Global

Organisation Name: Evora Global
Scope of Services Provided: Cloud-based application testing.

Following a review of a cloud-based energy management solution the customer made the following reference with regard to Prism Infosec's service: -

"Schroders required us to procure the services of a CREST approved penetration testing company to review the security of our web application and its implementation in the cloud on Amazon Web Services.

We engaged Prism Infosec who assisted us with the end-to-end delivery of the requirement, including scoping the work, conducting the review and providing the report and summary of results.

Prism Infosec produced a statement of work which offered real value and they understood and identified the type of tests that our client needed to ensure adequate assurance of the security of our implementation.

We were impressed with the quality of the service and report that they delivered as well as their communication throughout the process and it helped us to move the project forward successfully with our own client. We would have no hesitation in recommending Prism Infosec."

All services were delivered on agreed time and budget and the reports were fully accepted by the Organisation and its accreditation bodies.

5.9 Technology - OPIA Ltd

Organisation Name: OPIA Ltd
Contact Name: Adam Nicholson
Title: Head of Informational Technology
Scope of Services Provided: Organisational Web Application security assessments
Period of Contract: 2017 – ongoing

Prism Infosec has provided security and penetration testing services for OPIA overseen throughout by the Head of Informational Technology, who kindly supplied the following reference statement in respect of the Prism Infosec services:

"As part of delivering services to our clients we are regularly requested to conduct penetration tests on our applications and servers. As part of our own due diligence we engaged Prism Infosec to review some of our web sites and their team found issues and vulnerabilities that other providers failed to identify. We were impressed with Prism Infosec's level of service and the quality of their deliverables and will certainly use them again for future assessments".

All services were delivered on agreed time and budget and the reports were fully accepted by the Organisation and its accreditation bodies.

6 Information Security & Risk Management

The security and protection of THE CLIENT's data shall be paramount at all times, and Prism Infosec is fully aware of the need to ensure that working with a cyber security partner or conducting penetration tests does not itself impact on the security of the environment. All testing will respect strict confidentiality rules and non-disclosure of information.

Prism Infosec is an ISO27001:2013 certified organisation and is also Cyber Essentials Plus certified and as such its internal security handling, systems and workstations are assessed on an annual basis by an independent security consultancy. Furthermore, Prism Infosec's customer engagement and data handling policies are reviewed on an annual basis by CREST.

We also take the following security measures to ensure that protection of customer data: -

- Prism Infosec operates an ISO27001:2013 certified (UKAS-accredited) ISMS;
- Encryption of data at rest on all of our testing devices;
- Data retention policies that define how long we store customer data and reports;
- All test data and reports are stored in an encrypted vault following a period of three months (or sooner if required by a client) after a penetration test up to the agreed data retention period;
- All data is hosted in ISO27001 and SOC 2 certified locations;
- All data is stored within the boundaries of the European Union (EU);
- Prism Infosec delivers all work by UK-based testers. We do not outsource testing outside of the UK;
- All data is securely deleted from the encrypted vault when it is no longer required;
- All sensitive data is transferred to clients via our Send Safely portal instance and/or PGP/GPG encrypted;
- All testers are governed by our information security management policies, customer engagement process and penetration test execution policies;
- All documents handled by Prism Infosec are protectively marked and as such their use are governed by our information handling policies;
- Regular internal vulnerability scans and penetration tests;
- Other than when hosted on a testing laptop (always encrypted), client data is never stored in Prism Infosec's offices, rather this is hosted in ISO27001 certified data centres;

- All Prism Infosec employees are background checked to the highest standards (BS:7858) and/or have UK Government security clearance;
- All Prism Infosec employees are under strict Non-Disclosure Agreements (NDAs) as part of their employment contracts;
- Prism Infosec consultants are trained to always remove accounts, tools or changes that were made during testing prior to the testing conclusion and the importance of not leaving "backdoors" into client infrastructure or applications;
- All testing tools are either established open source software or licensed commercial products; and
- Regular training and updates on all of our internal staff on the importance of protection of client data.

Prism Infosec has experience of working in sensitive client environments, across financial services, government and technology and ensures that the availability of services and data is respected at all times.

To ensure that this is the case, Prism Infosec ensures: -

- Consultants are briefed and reminded of the risks of penetration tests and respecting client availability during all tests;
- All tests are planned to follow our engagement processes, which incorporates phases around understanding sensitive systems and services, ensuring backups of data and discussing the risks around the delivery of penetration tests;
- To limit areas of test methodology where necessary such as certain exploitation techniques (buffer overflows et al) that carry more risk;
- Planning for testing of systems out of hours where required to avoid potential disruption;
- Planning for testing on UAT environments where available to avoid potential disruption and then validating potential issues on live (where permitted and safe to do so);
- Working in partnership with clients to understand and manage the risks at all times; and
- All consultants adhere to a strict penetration test execution policy, which is available on request.

7 Key Benefits

It is our belief that Prism Infosec is ideally placed to deliver the security assessment package for the following reasons: -

- Prism Infosec was founded in 2006, is privately owned and not part of a larger IT group. THE CLIENT can be assured on our longevity and commitment to providing independent boutique security consultancy services;
- Prism Infosec is a NCSC CHECK 'Green Light' Company;
- Prism Infosec's testing services were recognised at the PCI London 2020 Award Dinner for demonstrating excellence in the field;
- Prism Infosec is ISO27001:2013 certified (UKAS-accredited) so clients can be confident of our commitment to maintaining the security of the data that we handle;
- Penetration testing and security consultancy is Prism Infosec's core business. THE CLIENT can be assured that we will be truly independent and not attempt to upsell other products and services such as SIEM or SOC;
- Prism Infosec has the skills and capability to deliver services beyond penetration testing, including CCP/ex-CLAS support, PCI expertise, GRC consultants and staff who can offer pragmatic advice on the implementation or evaluation of cyber security architectures and controls;
- Prism Infosec's management and principal consultants have inherent experience during their careers associated with the project management of large-scale penetration testing projects including the Royal Bank of Scotland, the Bank of England, Kuwait Finance House, Cable and Wireless / Vodafone and British Airports Authority (BAA), now Heathrow Airports Limited;
- Prism Infosec will provide highly skilled consultants to THE CLIENT with many years of experience of delivering complex security assessments in the information / cyber security industry. Prism Infosec is frequently engaged by other security consultancies in the UK when their own internal teams do not have the skills to deliver sophisticated tests such as reverse engineering, red teaming, social engineering or reviews of bespoke / complex technologies;
- Prism Infosec's technical team have contributed toward industry standard tools such as THC Hydra, identified bespoke vulnerabilities (CVEs) as well as industry publications, press and public speaking events. Our consultants have been involved in the foundation and management of key industry schemes such as CREST and Tiger and have contributed to open methodologies such as the OSSTMM (our director is listed as a contributor to OSSTMM 3.0). THE CLIENT can therefore be assured that by engaging Prism Infosec to deliver the penetration testing requirement, they will receive bespoke and cutting-edge guidance on vulnerabilities and weaknesses in the environment;

- Prism Infosec's security consultants have additional skills and certifications which will be beneficial to THE CLIENT including PCI QSA, ISO27001 Lead Auditor, CLAS / CCP, CISA and CISSP;

- Prism Infosec is committed to continual improvement and is a member of CREST as well as operating a certified (UKAS-accredited) ISO9001:2015 Quality Management System (QMS). THE CLIENT can be assured of Prism Infosec's commitment to customer care and quality, throughout the life of the relationship;

- Prism Infosec is a member of CREST (STAR certified for the delivery of advanced threat-based penetration testing simulations), the not for profit organisation that serves the needs of a technical information security marketplace requiring the services of a regulated professional services industry; and

- Prism Infosec is innovative and agile and will be responsive and flexible to THE CLIENT's requirements with regard to delivery and reporting.

8 Appendices

8.1 Appendix A – Testing Overview

A sample of methodologies aligned to some of the services provided by Prism Infosec are included in the following sections. A full list of services and associated methodologies can be made available on request.

12.1.1 Infrastructure Testing

Our infrastructure testing methodology is designed to be compatible with those commonly accepted industry-wide including the ISECOM OSSTMM and from generally accepted techniques and advice from CESG, Tiger Scheme and CREST in the United Kingdom as well as NIST in the United States.

Figures 1 & 2 describe the Prism Infosec infrastructure penetration testing methodology. The testing incorporates a structured mechanism that assures the client of a comprehensive test.

The testing uses a combination of manual investigation and analysis alongside automated testing tools and vulnerability scanners.

Figure 1 – External Penetration Testing Methodology

Figure 2 – Internal Penetration Testing Methodology

12.1.2 Application Testing

The Prism Internet-based application testing methodology is aligned with the Open Web Application Security Project (OWASP) Top 10 methodology. The methodology follows the phases outlined in Figure 3.

Effective application testing can only be delivered using a manual testing approach, which walks-through the entire application from both unauthenticated (public) areas and protected areas that require authentication credentials.

Some areas of the application will be subjected to automated vulnerability analysis using tools such as 'Burp Suite Professional' to determine whether any issues exist with the application's handling of input from a user in all areas of a web session's header and body.

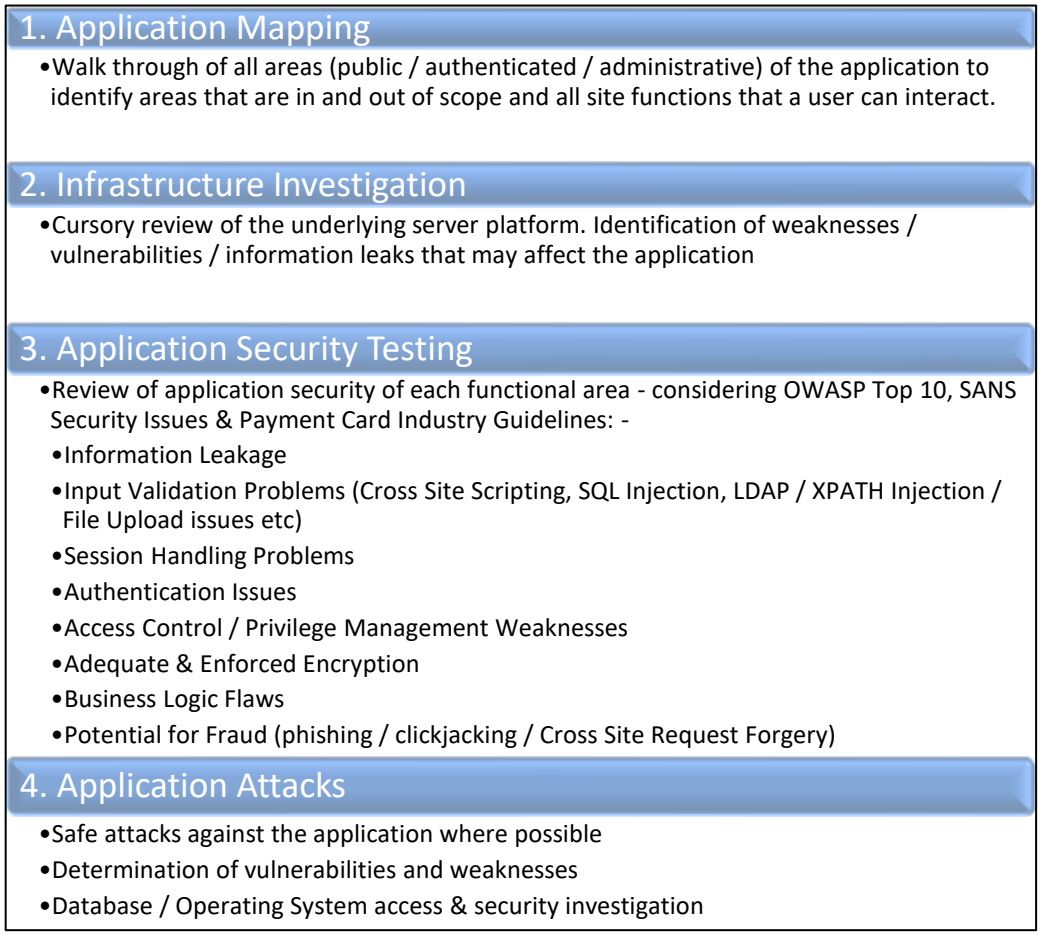

Figure 3 – Application Testing Methodology

12.1.3 Web Service Testing

Web services testing can be either a standalone assessment, or as part of a full application security test. Therefore, a number of factors are generally considered when determining the scope and size of a web services testing engagement:

a) Is the entire application to be included or just the web services element?
b) Is the web server infrastructure to be included?
c) Is the web service exposed to the public (e.g. through the Internet)?
d) How important is the data from a business perspective?
e) How complex is the web service, how many operations are there?
f) Will authentication credentials be provided?
g) What type of authentication is being used (Basic, NTLM, Kerberos)?
h) What type of web services framework is in use (WCF, APACHE Axis, ZEND)?
i) What are the technologies and protocols in use (REST, SOAP, WCF)?
j) Is BPEL being used?
k) Does the service accept attachments over SOAP?
l) Will there be any examples of valid SOAP requests?
m) Is development documentation available?
n) Where are the DISCO/UDDI directories and WSDL endpoints?
o) Do the web services us WS Security or SSL?
p) How do end users interact with the web service, are portals or client apps being tested?
q) How do other systems interact with the web service, are these being tested?

Approach
Web services provide a secondary vector to an attacker that potentially, could be utilized in order to bypass the application's security controls if the web services have not been effectively secured. Therefore, a web services security assessment will take a complete approach similar to that of the web application but will be unique and thorough to ensure no areas are exposed to weakness, this can include:

a) The web service itself;
b) The web service communications.
c) Client software and system, including mobile code;

Testing is generally performed using specialised web services testing software and using standard client systems installed with application software. Application user accounts are used throughout the testing to simulate user behaviour and access application functionality with the aim of identifying security weaknesses and exposures.

The specific tests are entirely dependent on the type of web services in use; however the following areas have regarded as potential threats to web services by industry experts.

Communication
a) Man-In-The-Middle attacks
b) Use of Suitable Cipher Suites;
c) Adequate Server Certification.
d) WS-routing security
e) Replay Attacks

Web Service Engine
a) Buffer Overflows
b) XML Parsing Errors
c) Spoiling Schema
d) Complex or Recursive Structure as Payload
e) Denial of Service
f) Large Payload
g) Session Information Leakage

Web Services Deployment
a) Fault Code Leaks
b) Permissions on Access Issues
c) Poor Policies – Secure Coding SDL practices
d) Customized Error Messages (information leakage)
e) Denial of Service

Web Services User Code
a) Parameter tampering
b) WSL Probing
c) SQL/XPATH/LDAP/OS Command Injection
d) Brute force
e) Directory Traversal

f) Data Type Mismatch
g) Content Spoofing
h) Sessions Tampering
i) Format String
j) Information Leakage
k) Authorization

12.1.4 Mobile Application Testing

Area	Common Control Examples
Code obfuscation and reverse engineering protection	• Disabling all debugging capabilities, unnecessary information removed from the symbol table • Ensuring applications do not generate core dumps or other sensitive information upon a crash • Obfuscation/insertion of guards into binary code - application hardening/runtime protection; method scrambling at binary level • Jailbreak/root detection using multiple methods • Protection against attacks such as "method swizzling" • Encryption/checksums of upcoming sensitive code functions • Detection of runtime manipulation, application patching • Prior checksum of critical instruction branch code immediately before code and randomly elsewhere • Do not use legitimate objective C method swizzling in the code • Do not use objective C for sensitive methods, translate into native C/C++ • Avoid direct method calls to system libraries - invoke using inline assembly • Perform regular server side re-validation of authentication
Secure communications (data in transit)	• Certificate pinning • TLS communications to server • Server-side authentication, authorisation and signing of all requests
Secure storage (data at rest)	• Sensitive information not stored on device, wherever possible • Where absolutely necessary, storage of sensitive information must be in secure areas (e.g. keychain/Shared Preferences) • Any encryption must use approved algorithms (including the use of salts) • Ensuring sensitive information is not stored in device app logs

Server-side protection	• Strong input validation, including protection against injection attacks (SQL/XML injection, etc.) • Authentication and signing of API requests • Back-end servers must be hardened and have all unnecessary web server/service content removed
General mobile application security	• Restriction of copy/paste or pasteboard for sensitive information • Restriction of background state around sensitive application areas (CHD input, etc.) • Restriction of background screenshots (e.g. for task switching) around sensitive application areas (CHD input, etc.) • Obfuscation of sensitive information in the mobile application (e.g. to last 4 digits of stored credit/debit PAN, full PII details, etc.) • Password/PIN re-entry prior to use of sensitive functions (password/personal details change, etc.) • Strong password/PIN criteria, including additional password management functions (e.g. account lockout) • Minimum device permissions required for application functionality • Client-side restrictions on user input (whitelisted characters)

Figure 4 – Mobile Application Testing Methodology

12.1.5 Source Code Review

The Prism source code analysis methodology is designed to identify and address areas of risk to the confidentiality, integrity and availability in bespoke applications.

Approach

Source code analysis is performed using industry standard automated source code review tools combined with the expertise of Prism consultants to assess the quality and security of application source code. The review provides an in-depth analysis of the source code highlighting any vulnerabilities associated with poor programming practices and offers recommendations to secure the code base.

The specific testing phases are dependent on the application functionality; however, the following areas are common to most source code analysis reviews:

Best Practices Adherence

The source code is assessed for adherence to best practices with regards to:

a) Bounds checking;
b) Memory allocation;
c) Insecure library functions;
d) Documentation;
e) Code maintainability and performance.

Input Validation Assessment

All external input into the application under review requires validation to ensure that such input is appropriate, such that it is expected, meaningful and secure i.e. will not cause the application to behave in an unexpected manner.

Thus, the source code is reviewed to ensure that inappropriate input is handled safely with regards to the following attacks:

a) Cross Site Scripting;
b) Buffer Overflow;
c) SQL Injection;
d) Command Injection.

Furthermore, validation rules are assessed to ensure that the permitted input characters are appropriate for the application type.

Error Handling Assessment

The source code review will analyse the applications error handling capability with specific checks to ensure that:

a) Any errors produced by the application are handled securely and do not leave the application in an insecure state;
b) Error handling does not provide any feedback to an attacker which may assist in further attacks such as error messages detailing inner workings of the application.
c) Session Management Assessment
d) The source code review will assess the applications security with regards to the creation, renewal and destruction of a user's session with particular emphasis given to the:
e) Session Identifier construction including predictability;
f) Session identifier creation with regards to session fixation attacks;
g) Secure session termination;
h) Secure session transportation including encryption (see below);
i) Session lifecycle including session timeout analysis.

Authentication Assessment

The code review authentication assessment will examine the application code-base to ensure that authentication methods, password acceptability and storage and account lockout configuration is appropriate. Specifically, the code base will be reviewed to identify:

a) Authentication methods in use;
b) Password complexity restrictions;
c) Account lockout configuration;
d) Password storage methods.

Cryptographic Assessment

The source code will be reviewed to assess the applications use of encryption particularly for the inclusion of:

a) Inappropriate encryption libraries;
b) Proprietary cryptographic algorithm usage;
c) Cryptographically insecure encryption algorithms, for example DES;
d) Weak encryption key lengths.

Logging Assessment

To ensure that an appropriate audit trail exists the application code base will be assessed to ensure that the following, at the very minimum, are logged and securely stored:

a) Successful and unsuccessful authentication;
b) Authorisation requests;
c) Data manipulation;
d) Session activity (Logout events).

Denial of Service Assessment

The source code will be reviewed to identify any areas in the code which have the potential to facilitate denial of service type attacks with particular emphasis on:

a) Improper Resource Handling.

Deployment Review

Furthermore, it is recommended that the deployment of the application is assessed, particularly for web-based applications, to ensure that appropriate controls with regard to the code are implemented:

a) Relevant directories and files have secure permissions;
b) Web server specific security settings are appropriately configured;
c) Web server deployment is in line with best security practices.

12.1.6 Cloud Configuration Review

A review of the configuration of a cloud environment can be performed either standalone, or in conjunction with other assessments of the targeted resources, at a code, application, or infrastructure level. It is important to consider the assurance requirements of the entire project to effectively scope a cloud review. The following questions can help to appropriately determine the scope of such an engagement:

r) Is the cloud environment dedicated entirely to a singular project, or do multiple projects share the same environment?
s) Do development and production resources share the same cloud environment?
t) Is the entire cloud environment the subject of the assessment or only a sub section?
u) Is assurance already in place, or included within the larger assessment, for in scope cloud resources at the infrastructure and/or application level?
v) What parts of the cloud environment under assessment are publicly facing?
w) Does the environment contain any VPN ingress?
x) Are there any connections between this cloud environment and any others?
y) How do staff members view the cloud environment configuration?
z) How are changes made to the cloud configuration?

Approach

The cloud layer sits above infrastructure and applications and can potentially impact an environment through three primary routes:

a) Compromise of a cloud account
b) Compromise of a cloud hosted resource
c) Misconfiguration of a cloud service

Therefore, a cloud configuration review focussed on reviewing the environment to ensure:

d) The configured permissions do not allow privilege escalation by low level accounts
e) The environment is effectively configured to reduce the potential for lateral movement
f) Resources are configured in an expected, secure and hardened manner

Testing takes place using a process that combines the use of automated tools, manual review and inbuilt cloud functionality in order to effectively assess the overall posture of the environment.

The specific checks performed are entirely dependent on the type of cloud services in use; however, the following non-exhaustive list of resources and checks provides a sample of the most deployed and misconfigured resources within cloud environments.

Virtual Machine Cloud Configuration Review
a) Sensitive Information Disclosure
b) Insecure Metadata Services
c) Excessive Permissions
d) Firewall Configuration
e) Data Storage

Cloud NACL and Firewall Review
a) Overly Permissive Rules
b) Temporary or Test Rules
c) External Internet Exposure

Review the Cloud Configuration of PaaS Compute and API Deployments
a) Weak Transit Encryption Configuration
b) Out of Date Deployed Software Versions
c) Permissive Network Access Controls
d) Excessive Permissions
e) Sensitive Information Disclosure

Review of Serverless Computing Cloud Configurations
a) Out of Date Runtimes
b) Permissive Network Access Controls
c) Excessive Permissions
d) Insecure Secret Storage

Review of both Public and Private Cloud Data Storage
a) Misconfigured Access Controls
b) Weak Transit Encryption
c) Insecure Secret Storage

Cloud Database Configuration Review
a) Data Redundancy
b) Insecure Data Storage
c) Permissive Network Access Controls

Review Deployed Application Co-Ordinations
a) Insecure Secret Storage
b) Logic errors

Review of Deployed Messaging Services
a) Misconfigured Access Controls

b) Missing Encryption

Load Balancer Cloud Configuration Review

a) Weak Transit Encryption
b) Vulnerable Configurations
c) Missing logging

Cloud Permissions Review

a) Over Permissioned Accounts
b) Missing Account Protection Controls
c) Privilege Escalations
d) Guest Access Configuration

Cloud Monitoring and Security Configuration

a) Incomplete Coverage
b) Lack of Automated Alerts
c) Unactioned Detections

Review of Cloud Settings for other relevant Deployed Cloud Resources

a) All other resources are reviewed in line with cloud provider's recommendations, industry best practices, and internal documentation based upon Prism Infosec's industry experience.

12.1.7 AWS Configuration Review

A review of the configuration of an AWS environment can be performed either standalone, or in conjunction with other assessments of the targeted resources, at a code, application, or infrastructure level. It is important to consider the assurance requirements of the entire project to effectively scope an AWS review. The following questions can help to appropriately determine the scope of such an engagement:

a) Is the AWS environment dedicated entirely to a singular project, or do multiple projects share the same environment?
b) Do development and production resources share the same AWS account?
c) Is the entire AWS account the subject of the assessment or only a sub section?
d) Is assurance already in place, or included within the larger assessment, for in scope cloud resources at the infrastructure and/or application level?
e) What parts of the AWS environment under assessment are publicly facing?
f) Does the AWS environment contain any VPN ingress?
g) Are there any connections between this AWS account and any other cloud environment?
h) How do staff members view the AWS account configuration?
i) How are changes made to the AWS account?

Approach

The cloud layer sits above infrastructure and applications and can potentially impact an environment through three primary routes:

a) Compromise of an AWS account
b) Compromise of an AWS hosted resource
c) Misconfiguration of a AWS service

Therefore, an AWS configuration review focussed on reviewing the environment to ensure:

a) The configured permissions do not allow privilege escalation by low level accounts
b) The account is effectively configured to reduce the potential for lateral movement
c) Resources are configured in an expected, secure and hardened manner

Testing takes place using a process that combines the use of automated tools, manual review and inbuilt AWS functionality in order to effectively assess the overall posture of the environment.

The specific checks performed are entirely dependent on the type of cloud services in use; however, the following non-exhaustive list of resources and checks provides a sample of the most deployed and misconfigured resources within cloud environments.

EC2 Configuration Review

a) Sensitive Information Disclosure
b) Insecure Metadata Services
c) Excessive Permissions
d) Security Group Configuration
e) EBS Storage

Security Group and Network Access Control List Review

a) Overly Permissive Rules
b) Temporary or Test Rules
c) External Internet Exposure

Review the Configuration of Elastic Beanstalk and API Gateway Deployments

a) Weak Transit Encryption Configuration
b) Out of Date Deployed Software Versions
c) Permissive Network Access Controls
d) Excessive Permissions
e) Sensitive Information Disclosure

Review of Lambda Cloud Configurations

a) Out of Date Runtimes
b) Permissive Access Controls
c) Excessive Permissions
d) Insecure Secret Storage

Review of both Public and Private S3 Buckets

a) Misconfigured Access Controls
b) Weak Transit Encryption
c) Insecure Secret Storage

DynamoDB, Aurora and RDS Configuration Review

a) Data Redundancy
b) Insecure Data Storage
c) Permissive Network Access Controls

Review Deployed AWS Step Functions

a) Insecure Secret Storage
b) Logic errors

Review of Deployed Simple Notification/Queue Services

a) Misconfigured Access Controls
b) Missing Encryption

Elastic Load Balancer Cloud Configuration Review

a) Weak Transit Encryption
b) Vulnerable Configurations
c) Missing logging

IAM Permissions Review

a) Over Permissioned Accounts
b) Missing Account Protection Controls
c) Privilege Escalations
d) Cross Account Assume Role Configuration

CloudWatch and GuardDuty Configuration

a) Incomplete Coverage
b) Lack of Automated Alerts
c) Unactioned Detections

Review of AWS Settings for other relevant Deployed AWS Resources

a) All other resources are reviewed in line with AWS recommendations, industry best practices, and internal documentation based upon Prism Infosec's industry experience.

12.1.8 Azure Configuration Review

A review of the configuration of an Azure account can be performed either standalone, or in conjunction with other assessments of the targeted resources, at a code, application, or infrastructure level. It is important to consider the assurance requirements of the entire project to effectively scope a cloud review. The following questions can help to appropriately determine the scope of such an engagement:

a) Is the Azure environment dedicated entirely to a singular project, or do multiple projects share the same environment?
b) Do development and production resources share the same Azure environment?
c) Is the entire Azure environment the subject of the assessment or only a subscription?
d) Is the related Entra tenant used for access to other resources?
e) Is assurance already in place, or included within the larger assessment, for in scope Azure resources at the infrastructure and/or application level?
f) What parts of the Azure environment under assessment are publicly facing?
g) Does the environment contain any VPN ingress?
h) Are there any connections between this Azure environment and any others?
i) How do staff members view the Azure environment configuration?
j) How are changes made to the Azure configuration?

Approach

The cloud layer sits above infrastructure and applications and can potentially impact an environment through three primary routes:

a) Compromise of an Azure account
b) Compromise of an Azure hosted resource
c) Misconfiguration of an Azure service

Therefore, a cloud configuration review focussed on reviewing the environment to ensure:

a) The configured permissions do not allow privilege escalation by low level accounts
b) The environment is effectively configured to reduce the potential for lateral movement
c) Resources are configured in an expected, secure and hardened manner

Testing takes place using a process that combines the use of automated tools, manual review and inbuilt Azure functionality in order to effectively assess the overall posture of the environment.

The specific checks performed are entirely dependent on the type of Azure services in use; however, the following non-exhaustive list of resources and checks provides a sample of the most deployed and misconfigured resources within cloud environments.

Azure VM Cloud Configuration Review

a) Sensitive Information Disclosure
b) Insecure Metadata Services
c) Excessive Permissions
d) Network Security Group Configuration
e) Disk Storage

Network Security Group and Azure Firewall Review

a) Overly Permissive Rules
b) Temporary or Test Rules
c) External Internet Exposure

Review the Cloud Configuration of Azure App Service Deployments

a) Weak Transit Encryption Configuration
b) Out of Date Deployed Software Versions
c) Permissive Network Access Controls
d) Excessive Permissions
e) Sensitive Information Disclosure

Review of Azure Functions Cloud Configurations

a) Out of Date Runtimes
b) Permissive Network Access Controls
c) Excessive Permissions
d) Insecure Secret Storage

Review of both Public and Private Storage Accounts

a) Misconfigured Access Controls
b) Weak Transit Encryption
c) Insecure Secret Storage

Cosmos, Azure Database and Azure SQL Configuration Review

a) Data Redundancy
b) Insecure Data Storage
c) Permissive Network Access Controls

Review Deployed Logic Apps

a) Insecure Secret Storage

b) Logic errors

Review of Deployed Storage Queues and Service Buses

a) Misconfigured Access Controls
b) Missing Encryption

Load Balancer, Application Gateway and Front Door Cloud Configuration Review

a) Weak Transit Encryption
b) Vulnerable Configurations
c) Missing logging

Azure and Entra Roles and Permissions Review

a) Over Permissioned Accounts
b) Missing Account Protection Controls
c) Privilege Escalations
d) Guest Access Configuration

Anomaly Detector, Defender and Sentinel Configuration

a) Incomplete Coverage
b) Lack of Automated Alerts
c) Unactioned Detections

Review of Azure Settings for other relevant Deployed Azure Resources

a) All other resources are reviewed in line with Azure's recommendations, industry best practices, and internal documentation based upon Prism Infosec's industry experience.

12.1.8 GCP Configuration Review

A review of the configuration of a Google Cloud Platform (GCP) environment can be performed either standalone, or in conjunction with other assessments of the targeted resources, at a code, application, or infrastructure level. It is important to consider the assurance requirements of the entire project to effectively scope a GCP review. The following questions can help to appropriately determine the scope of such an engagement:

a) Is the GCP environment dedicated entirely to a singular project, or do multiple projects share the same environment?
b) Do development and production resources share the same GCP environment?
c) Is the entire GCP environment the subject of the assessment or only a sub section?
d) Is assurance already in place, or included within the larger assessment, for in scope GCP resources at the infrastructure and/or application level?
e) What parts of the GCP environment under assessment are publicly facing?
f) Does the environment contain any VPN ingress?
g) Are there any connections between this GCP environment and any others?
h) How do staff members view the GCP environment configuration?
i) How are changes made to the GCP configuration?

Approach

The cloud layer sits above infrastructure and applications and can potentially impact an environment through three primary routes:

a) Compromise of a GCP account
b) Compromise of a GCP hosted resource
c) Misconfiguration of a GCP service

Therefore, a GCP configuration review focussed on reviewing the environment to ensure:

a) The configured permissions do not allow privilege escalation by low level accounts
b) The environment is effectively configured to reduce the potential for lateral movement
c) Resources are configured in an expected, secure and hardened manner

Testing takes place using a process that combines the use of automated tools, manual review and inbuilt GCP functionality in order to effectively assess the overall posture of the environment.

The specific checks performed are entirely dependent on the type of GCP services in use; however, the following non-exhaustive list of resources and checks provides a sample of the most deployed and misconfigured resources within GCP environments.

Computer Engine Configuration Review
a) Sensitive Information Disclosure
b) Insecure Metadata Services
c) Excessive Permissions
d) Firewall Configuration
e) Data Storage

VPC Firewall Review
a) Overly Permissive Rules
b) Temporary or Test Rules
c) External Internet Exposure

Review the Cloud Configuration of App Engine Deployments
a) Weak Transit Encryption Configuration
b) Out of Date Deployed Software Versions
c) Permissive Network Access Controls
d) Excessive Permissions
e) Sensitive Information Disclosure

Review of Cloud Functions Configurations
a) Out of Date Runtimes
b) Permissive Network Access Controls
c) Excessive Permissions
d) Insecure Secret Storage

Review of both Public and Private Cloud Storage
a) Misconfigured Access Controls
b) Weak Transit Encryption
c) Insecure Secret Storage

Firestore, Cloud SQL and Cloud Spanner Configuration Review
a) Data Redundancy
b) Insecure Data Storage
c) Permissive Network Access Controls

Review Deployed Cloud Tasks

a) Insecure Secret Storage
b) Logic errors

Review of Deployed Pub/Sub Resources

a) Misconfigured Access Controls
b) Missing Encryption

Cloud Load Balancing Configuration Review

a) Weak Transit Encryption
b) Vulnerable Configurations
c) Missing logging

IAM Review

a) Over Permissioned Accounts
b) Missing Account Protection Controls
c) Privilege Escalations
d) Guest Access Configuration

Anomaly Detection and Chronicle Configuration

a) Incomplete Coverage
b) Lack of Automated Alerts
c) Unactioned Detections

Review of GCP Settings for other relevant Deployed GCP Resources

All other resources are reviewed in line with GCPs recommendations, industry best practices, and internal documentation based upon Prism Infosec's industry experience.