Provision of
IT Health Check

of

IPO Network

Ref

IT-2016-101

Evolve Secure Solutions Limited

Prepared by:	[redacted]
Version:	**1.0**
Date:	**22nd September 2016**
Quality Assured by:	[redacted]
Released by:	[redacted]

TABLE OF CONTENTS

1 MANAGEMENT SUMMARY 3
1.1 CONTACT INFORMATION 4
2 UNDERSTANDING OF REQUIREMENTS 5
2.1 OBJECTIVES 5
2.2 SCOPE OF ITHC 5
3 DELIVERING THE TESTING REQUIREMENT 7
3.1 BACKGROUND 7
3.2 PRE-TEST PLANNING MEETING 7
3.3 PHASE 1 EXTERNAL TESTING (2 MAN DAYS) 7
3.4 PHASE 2 INTERNAL TESTING (15 MAN DAYS) 8
3.5 REPORT WRITING 11
3.6 PRE-REQUISITES 11
3.7 COMMUNICATION 11
3.8 GENERAL METHODOLOGY AND APPROACH 11
3.9 PROVISIONAL RESOURCES 12
3.10 TESTING TOOLS EMPLOYED 12
3.11 CHECK TEAM LEADERS 12
3.12 [redacted] - CHECK TEAM LEADER 13
3.13 [redacted] – CHECK TEAM LEADER 15
3.14 [redacted] – CHECK TEAM LEADER 17
3.15 [redacted] – CHECK TEAM LEADER 18
3.16 QUALITY MANAGEMENT 20
4 CHARGES 21
4.1 STRUCTURE AND PROFILE OF OUR PROPOSED TEAM 21
4.2 CONSULTANT FEES 21
4.3 COMMERCIAL OFFER 21
4.4 ACCEPTANCE OF IPO TERMS AND CONDITIONS 21
5 CORPORATE CAPABILITY 22
5.1 EVOLVE SECURE SOLUTIONS LTD 22
5.2 CYBERIS 22
5.3 REFERENCES 22
5.4 CASE STUDIES 24

1 MANAGEMENT SUMMARY

Evolve Secure Solutions Limited (Evolve) is delighted to submit this proposal for an IT Health Check (ITHC) of the IPO PSN connected infrastructure.

This is an area in which we have a proven track record having delivered similar ITHC of other IPO systems. Our wider IT Security work extends the breadth of the public sector, with similar and recent assignments including the [redacted].

Our capability in this field has been recognised at the highest level. Evolve has been certified by CESG as a Cyber Security Consultancy (CCSC) and we are approved by Crown Commercial Service for the provision of the full range of ICT Security Services. Our commitment to Information Security is signalled by achieving ISO27001 certification and that combined with our ListX status sets us apart from the majority of our competitors in this field.

In addition to our security accreditations, Evolve delivers all work through an independently audited ISO9001 Quality Management System (QMS) and has signalled its commitment to the Public Sector sustainability agenda through our achievement of ISO14001 certification and approved 'Carbon Neutral' status.

In responding to this requirement Evolve has elected to work closely with our colleagues at Cyberis who are our CHECK "Green Light" accredited partners. Evolve will act as the prime contractor, with Cyberis sub-contracted to perform and fulfil the technical obligations of the contract. This is the same team which has recently delivered similar IPO ITHCs. We confirm that we can provide a fully compliant solution to your requirements in that:

- Cyberis are a CHECK company with 'Green light' status;
- All our testers are a minimum of CHECK Team Members;
- All our testers hold a minimum clearance level of SC;
- We use experienced security consultants who have a wide-range of experience in delivering ITHC and penetration tests for the public service.

In order to ensure availability and contingency, we propose a team approach comprising named CHECK Team Leaders, with support if required from other named CHECK Team Leaders and CHECK Team Members.

Assignment Management and technical overview would be provided by [redacted], Evolve's Director of Consultancy. He will ensure that the work is undertaken in accordance with the Evolve ISO9001 accredited QMS. [redacted] is a CESG CCP Lead SIRA who has extensive experience of Information Security in the UK Public Sector environment. He is a PRINCE2 practitioner, ITPC Government practitioner and Fellow of the Institute of Business Consultants.

Other key Evolve Support staff for this project are:

- [redacted] Contract & Account Manager
- [redacted] Operations Manager
- [redacted] Finance and Quality Manager
- [redacted] Information Assurance Consultant
- [redacted] CHECK Project Manager & Contingency Team Leader

In accordance with Evolve's ListX and HMG Framework Accreditations, all Evolve consultants and support staff are cleared to a minimum of SC.

It is Evolve's policy to ensure continuity of key staff throughout the entire duration of a project and we confirm that once assigned our CHECK Team Leader(s) will deliver the work throughout the entire period, with support from the nominated staff detailed above as required.

Based on the information provided, we estimate that [redacted] man days may be required to complete the testing and report writing, together with reasonable contingency. We would only charge for the days actually required to be worked. Our day rate for this is [redacted] + VAT to include all expenses for working at Concept House. Therefore, our quote for the up to [redacted] days work is £14,960 + VAT.

1.1 Contact Information

We have provided contact information for [redacted] who is responsible for this submission and if successful would be responsible for all contractual matters and customer care, the consultants, their deliverables and the quality of support provided by Evolve.

Company Name	Evolve Secure Solutions Ltd (Evolve)
Address	A1/1001, Cody Technology Park, Farnborough. GU14 0LX
Telephone	01252 781000
Fax	01252 781001
Email	enquiries@evolvesecuresolutions.com
Company Registration	3956682
ISO14001:2004	BSI 7241464
ISO27001:2005	BSI 7241466
ISO9001:2000	LRQ 0928543/C
Contact	[redacted]

2 UNDERSTANDING OF REQUIREMENTS

2.1 Objectives

We understand that The Intellectual Property Office (IPO) requires an IT Health Check (CHECK) penetration test of its PSN connected infrastructure, as detailed within the following specification from the ITQ.

The assessment will focus on the following:

i. IT Health Check - White Box test on infrastructure components where full disclosure will be allowed to enable the team to do their work in the most effective manner. For this part of the assessment the Check Team will be allowed access to site to perform a full IT Health Check of:
   - The remote access components
   - The mail gateway control components
   - Proxy internet access
   - The IPO Network that provides access to PSN

ii. Firewall rules review;

iii. VLAN configuration;

iv. Mobile device configuration review; and

v. Desktop build setup and configuration review.

The tests will be focused on demonstrating that IPO has sufficient controls in place and doesn't provide any unauthorised entry points to the IPO networks and onward to the PSN.

The data processed and stored on IPO Networks holds a maximum protective marking of Official - Sensitive.

2.2 Scope of ITHC

IPO Boundary DMZ

The IPO have a number of internal and externally facing web facing services, including:

- Web forms linked, internal applications and databases to blogging (e.g. WordPress) and information services;
- Web browsing for internal users; and
- Remote access.

These services are presented via IPO's external DMZ, with further architectural (layer 3) separation provided by subsequent layers within the DMZ. All external web services utilise reverse proxies and utilise services provided by the front node firewall.

Web browsing by internal users is controlled by group policy applying proxy pac files for user group access.

Remote access is via the following:

- Laptop access via an X-Kryptor; and
- Cisco ASA appliance for iPhone and iPad.

Remote access devices are then provided access to the corporate network via VRF to dedicated internal VLANs.

All @ipo.gov.uk email transits inbound and out bound through the DMZ via the internet, and is transferred via the MailGate, which provides the content scanning on the IPO network and a mail forwarding component MailEdge in the DMZ.

The full range of all IPO's internal and external IP addresses, URLs and protocols will be made available prior to commencement of testing. All VLAN details and number and type of server will also be made available prior to testing.

PSN Connectivity
The connection to the PSN is routed via a VLAN off the front node Checkpoint Firewall and is used for the following services:

All @ipo.gsi.gov.uk email transits inbound and out bound through the PSN, and is transferred via the MailGate which consists of a content scanning component on the IPO network and a mail forwarding component MailEgde on the PSN LAN, DNS for the PSN is also provided on this server.

Access to specific web sites hosted on the PSN are controlled via proxy settings within the browser (proxy pac file) and the external PSN Proxy.

Protocols will be HTTP(S) and SMTP with defined endpoints such as the PSN mail gateway and the external proxies.

Desktop build
The IPO run Windows 7 throughout their estate on a combination of physical desktops and VMs through Wyse terminals, these access the Internet and the PSN for services such as email and web access as described above. Web access is via IPOs internet proxies and it is intended to demonstrate that these devices are not vulnerable to attack and do not present threat to the internal IPO network or the PSN.

Remote access
The IPO run a number of remote access devices including Windows 7 laptops, iPhones and iPads, as with the desktop estate, mobile access use the same email and web browsing services through the external web access through the IPO internet and PSN proxies, it is intended to demonstrate that these devices do not pose a higher threat to the IPO or PSN.

IPO Business Infrastructure
The IPO infrastructure supporting the business operation of IPO is out of scope of this ITHC and is physically isolated by a combination of the IPOs internal Cisco ASA firewall and the VSS Switch.

3 DELIVERING THE TESTING REQUIREMENT

3.1 Background

This section explains the methodology used when performing testing engagements, including information on activities prior to performing any work. All IT Health Check activity complies with the methodologies defined for the CHECK scheme. This has been enhanced by our own quality assurance procedures. There are a number of generic procedures that cover all testing scenarios. Specific techniques are described in the following sections.

We will take a manual, consultant-driven approach to your requirements, but one that also follows tried and tested procedures and techniques, meaning that the specific deliverables of the assignment will be delivered in a methodical, organised and timely manner. We will seek to work closely with your staff to ensure the most valuable outcomes, including elements of skills transfer inherent in collaborative working.

As part of any project, we will use some automated tools, typically to allow the consultant to quickly gain a broad understanding of the target environment before proceeding with the manual testing and auditing elements, as required by the project.

3.2 Pre-test Planning Meeting

Prior to the testing (and as soon as possible), we will arrange a conference call with IPO to discuss the scope in more detail, as well as relay the testing pre-requisites.
All parties will exchange key information necessary for the smooth running and successful completion of the project. The agenda will typically include the following:

- Confirmation of the exact system number at each location and the provision of network diagrams to confirm scope and sample sizes;
- Agreement of the timescale for the test programme, including start date, key milestones and estimated completion, with milestones where appropriate;
- Establish joining arrangements, vetting and access;
- Exchange of relevant contact details to allow both project teams to contact each other, as required;
- Agreement of a method of exchanging the draft and final reports.

Following this initial meeting we will produce a plan for the testing which will incorporate the key requirements and other inputs such as specific threat information, from the relevant project stakeholders.

3.3 Phase 1 External Testing ([redacted] man days)

We will undertake a CHECK Penetration Test of the systems in scope from an internet based perspective, in line with CESG CHECK guidelines and our Penetration Test Methodology.

It is understood that the scope of the external testing will encompass two /28 address ranges, and hence a maximum of 32 IP addresses as part of this assessment.

3.4 Phase 2 Internal Testing ([redacted] man days)

Information for scoping is indicative, and IPO will provide full details at the time of testing. The following systems have been noted as of particular concern with respect to the PSN testing:

- DMZ - PSN VLAN
  - Mail Edge – Appliance
  - PSN Proxy
- DMZ - Reverse proxy VLAN
  - eServices
  - w.w.w
- DMZ – web presentational (optional)
  - IIS server set up if required
- DMZ - Mail edge
  - Remote Access
  - X-Kryptor
  - iOS devices walled garden
- Internal
  - Mail Gate server
  - Web proxy servers (1 general user, 1 IT user)
  - MAG endpoint
  - Airwatch for iOS device configuration

1. **Internal Vulnerability Scan**
   Cyberis will perform a vulnerability scan of all networks to establish where vulnerabilities exist in the environment that may expose the network or onward connections to the PSN. In addition, we will identify weaknesses in the delivery of internet and mail services via the proxy servers, mail gateways and PSN.

   The following networks are thought to be in scope for testing:

   2 x /24 ranges within the DMZ
   1 x /25 range within the DMZ
   5 x /28 ranges within the DMZ
   3 – 4 ranges within the internal network

   Full access to all ranges will need to be provided for a testing laptop.

2. **Firewall Rule Base Review**
   A review of the relevant firewall rules will be undertaken and compared to firewall good practice guidelines to identify areas where the configuration of the firewalls can be improved to better protect the systems in scope. Specific focus will be made to the separation of the DMZ from the internet, trusted IPO networks and the PSN networks, to ensure that DMZ controls are appropriate and meet the architectural design.

   On the external firewall, approximately four firewall rules and five NAT rules are relevant to the PSN connection.

   Internally, there are around 40 VLANS and 200 outbound rules, but review will be concentrated on the rules influencing the servers of specific interest, namely:

   - Mail Gate server
   - Web proxy servers (1 general user, 1 IT user)
   - MAG endpoint
   - Airwatch for iOS device configuration

   IPO will need to provide the tester with the relevant extracts from the firewall rulebases for review.

3. **VLAN Bridging**
   Whilst undertaking the internal testing, attempts to bypass network perimeter controls using VLAN hop techniques will be undertaken to ensure the network switching infrastructure is appropriately configured.

4. **Virtualisation Review**
   The IPO have stated that a full review of the virtualisation technologies is not in scope for this assessment, though a review of key virtual machines is required.

   In order to meet this requirement, Evolve proposes to conduct a review of the virtual machine configuration of the key control points for the PSN, including the mail gateways, the mail edge and the proxy servers.

5. **Server build review**
   A configuration review of the Windows and Linux servers in scope will be undertaken and compared with CESG and good practice guidelines to highlight areas of weakness.

   The IPO has requested a comprehensive review of one of each type of gold build present within the environment. The number of gold build has not been specified. For the purposes of this quotation, a maximum of five different gold builds has been assumed for this review.

6. **Database configuration review**
   A configuration review of the SQL servers in scope will be undertaken and compared with CESG and good practice guidelines to highlight areas of weakness.

   IPO has indicated that no database servers are specifically in scope for a detailed review, and hence any review of database configuration will be conducted from an anonymous position across the network, during the vulnerability scan.

7. **Web server configuration review**
   A configuration review of the Apache / Tomcat / IIS servers in scope will be undertaken and compared with CESG and good practice guidelines to highlight areas of weakness.

   One sample IIS server within the DMZ will be in scope for a configuration review.

8. **Audit and logging review**
   Cyberis will seek to understand and obtain evidence that system logging across all areas of testing is appropriate to capture malicious activity.

9. **Desktop review**
   The IPO run windows 7 throughout their estate on a combination of physical desktops and VMs through Wyse terminals, these access the Internet and the PSN for services such as email and web access. Cyberis will review the build of these desktops to highlight where the build of these systems is not in line with CESG guidelines.

   Around seven different workstation templates are in use throughout the organisation. One different workstation from each template will be reviewed.

10. **Remote access review**
    The IPO run a number of remote access devices including Windows 7 laptops, iPhones and iPads, as with the desktop estate, mobile access use the same email and web browsing services through the external web access through the IPO internet and PSN proxies. Cyberis will review the configuration of these devices to ensure that any risks to the IPO or PSN are identified.

    185 Wyse terminals, 220 laptops, 169 iPads and 121 iPhones are in use for remote access. Cyberis will examine one of each type of device in respect of configuration to ensure a good coverage of the solution.

    The configuration of key remote access devices, such as a XKryptor services will also be included.

3.5 Report Writing

Cyberis will produce reports as per section 4.14 of the ITQ (IT-2016-101). The report will be protectively marked 'OFFICIAL – SENSITIVE' and handled by Cyberis as such.Reports on the findings of the CHECK IT Security Health Check will be provided to the project staff and any affected suppliers (if applicable), IPO Accreditor, IPO ITSO and to the CHECK administrator at CESG.

3.6 Pre-requisites

In order to conduct the ITHC, we will require the following:

- Confirmation of external IP addresses in scope
- Confirmation of internal IP addresses in scope for vulnerability scanning
- Confirmation of host names and server roles in scope for a comprehensive build audit.
- Desk space and connectivity to all VLANs / networks in scope for Cyberis laptops.
- Administrator / root credentials for servers and workstations in scope for review
- Digital, or paper based copy of the firewall rules in scope.
- Virtual machine configuration files for key systems
- Remote access devices (Laptop, iPhones, iPads) to assess remote access.
- Access to appropriate personnel to understand logging/ auditing across the environments in scope.
- Technical point of contact throughout the engagement
- Completed 'Authority For Security Testing' form (https://portal.cyberis.co.uk/loa)

3.7 Communication

Our consultants will provide frequent communication, including attendance of daily 'wash up' meetings. Where critical or high impact vulnerabilities are identified, they will be brought to the immediate attention of stakeholders. At the end of the ITHC, an informal report to IPO staff will be submitted.

3.8 General Methodology and Approach

Our consultants follow comprehensive testing methodologies for all engagements, as reviewed and approved by CESG. Our methodology, covering infrastructure and application security assessments will be used by all CHECK consultants engaged in the project (available on request).

During your engagement, we will assign a CHECK Team Leader as Principal Project Consultant who will be responsible for overseeing delivery of your work and keeping you up to date with progress reports. You will also be provided with an initial escalation point of contact (the Project Manager) in the event that any issues arise which cannot be addressed by your Principal Project Consultant. Evolve points of escalation are [redacted], Contract Manager and then [redacted], Director of Consultancy.

The Principal Project Consultant will attend the pre-engagement planning meeting, and will be responsible for managing all aspects of the service delivery for IPO, including co-ordinating Cyberis resources and providing a single point of contact for IPO staff.

The Principal Project Consultant will agree deliverables with IPO staff at the pre-engagement planning meeting and will ensure that these are produced in the agreed timescales in accordance with the test plan provided.

3.9 Provisional Resources

We will be able to confirm named resources for the project once approval to proceed has been obtained from the IPO. However, the project will be led by a highly experienced CHECK Team Leader, and will be supported by other members of the CHECK team as required. All CHECK resources hold a minimum SC clearance.

3.10 Testing Tools Employed

Our consultants use a wide range of tools when carrying out testing services, depending on the technology they are testing. We ensure that our consultants are experienced and familiar with using all tools within a controlled environment before they are used on client engagements.

To ensure that we provide a comprehensive service, we use a variety of Open Source, commercial and proprietary tools. All our tools are sourced from a trusted supplier so that we can be sure that they are free from malicious code.

The source code of any exploit scripts from untrusted sources is examined prior to use and thoroughly tested within a controlled environment before being used. This will ensure that their function is understood and that they will not introduce any vulnerabilities to our clients' systems.

So that we can provide extra value to our clients, we have developed a number of proprietary tools. In addition, our consultant can write scripts or develop tools as necessary if a particular test scenario requires.

If required, we will provide IPO with a list of all tools to be used.

3.11 CHECK Team Leaders

The work will be undertaken by two of the following CHECK Team Leaders. The nominated CHECK Team Leaders will be confirmed at time of order and will be allocated to the work for the duration of the assignment.

3.12 [redacted] - CHECK Team Leader

Profile

[redacted] is an IT security professional with extensive managerial experience. He has a track record for innovation, having conceived and delivered new security products and service lines for established information security consultancies.

[redacted] experience encompasses in-depth infrastructure and application penetration testing, and [redacted] is a CREST Certified Tester for applications. He is also a recognised expert in the field of network forensic analysis, holding the CREST Certified Network Intrusion Analyst qualification. He was also a member of CESG's review panel for technical architectural solutions whilst working for [redacted], offering technical project advice and assurance to multiple government and private organisations.

Before joining Cyberis, [redacted] was responsible for meeting demanding financial and delivery targets as the head of a service line for one of the UK's foremost consultancies. [redacted] continuously shares research and development across the security industry through various conferences, information exchanges and published tools.

Qualifications

- CHECK Team Leader (Infrastructure and Applications)
- CREST Certified Tester (Applications and Network Intrusion Analysis)
- HMG SC and DV clearance
- Non-Police Personnel Vetting
- First Honours Degree in BSc Software Engineering

Employment History

- [redacted] – Present: Director (Cyberis Ltd)
- [redacted]: Security Consultant ([redacted])
- [redacted]: Head of Network Forensics ([redacted])
- [redacted]: Emerging Threats Team Lead ([redacted])
- [redacted]: Lead Analyst and Incident Handler in GovCertUK ([redacted])

Areas of Expertise

- Computer forensics
- Network forensics
- Development of security tools and products
- Web application architecture, design, implementation and penetration testing
- Infrastructure penetration testing
- IDS architecture, deployment, analysis and rule development
- Open source information gathering
- Linux/Unix operating systems

Example Engagements

Incident Response and Forensic Investigation - Major High Street Retailer

[redacted] was assigned to investigate a reported compromise of credit card data from an Internet store of a major high street retailer. As many thousands of transactions passed through the site each day, it was critical to minimise downtime to reduce the cost to the business. [redacted] led the investigation from the outset, including conducting complex acquisition of several servers and workstations out-of-hours at a customer data centre. An in-depth review of the web application code and decoding of several covert web 'back-doors' revealed a sophisticated theft of over 500,000 credit cards.

[redacted] has developed specialist acquisition techniques which have been proven in the field, dealing with high availability, scalable and redundant e-commerce systems that cannot simply be disconnected and detained. In addition to the numerous PCI related engagements delivered, [redacted] has carried out several investigations surrounding acquired workstations and laptops on behalf of UK government at SECRET level and above. Technical knowledge gained and regularly exercised during penetration testing allows [redacted] to understand the motivation and techniques used by attackers and nefarious individuals to uncover covert data, tools and other incriminating evidence from an engagement.

CHECK Test – Central Government Departments

As an active member of the CESG 'Virtual Team', [redacted] regularly worked on many of the UK's most critical networks and systems. This often involved a full IT Health Check of high classification systems, identifying vulnerabilities that may be exploited by an attacker, assessing the level of skill required to exploit, and the impact to UK national interests if an attacker were to actually compromise the systems. Many of the tests that [redacted] has carried out have identified risks that have implications government-wide.

Finance – European Online Banking Site

In 2011 [redacted] conducted a remote web application test of a European bank. Despite the client spending significant budget on the security of the public website, [redacted] was able to circumvent authentication to the website in a multitude of ways. As a result of testing, it was possible to demonstrate to the client how an attacker could easily transfer funds using techniques such as cross-site request forgery (CSRF), and gain access to administrative functions of the host across the Internet without any valid credentials.

3.13 [redacted] – CHECK Team Leader

Profile

Over a decade working in the security consultancy industry, [redacted] has delivered information assurance consultancy engagements and compliance audits, together with numerous public and private sector infrastructure and application penetration tests. [redacted] is a CHECK Team Leader and CREST certified tester for both infrastructure and applications.

[redacted] wide experience includes engagements across Government, law enforcement, retail, financial, telecommunications and gambling sectors, and participation in a large range of projects including infrastructure and application penetration testing, information risk assessment, due-diligence compliance auditing, network forensic analysis and social engineering exercises.

Her strong communication skills and technical acumen allows her to engage at all levels, in order to deliver quality services to clients.

Qualifications

- CHECK Team Leader (Infrastructure and Applications)
- CREST Certified Tester (Infrastructure and Applications)
- HMG SC clearance
- Non-Police Personnel Vetting
- Imperial College, B. Eng. (Hons.) Computing

Employment History

- [redacted]: Director (Cyberis Ltd)
- [redacted]: Security Consultant ([redacted])
- [redacted]: Head of Technical Consultancy ([redacted])
- [redacted]: Security Consultant ([redacted])

Areas of Expertise

- Web application architecture, design, implementation and penetration testing
- Infrastructure design and penetration testing
- Information security risk assessment
- Information security consultancy
- Compliance auditing
- System build hardening and secure network device configuration
- Open source information gathering
- Linux/Unix operating systems

Example Engagements

Application Security Test for Government

A Government organisation required a web application to go live at very short notice. The penetration test revealed serious flaws, both in application design and business logic, potentially allowing malicious entities unauthorised access to highly personal information stored in the application's database. Deploying the application without these vulnerabilities being uncovered could have led to a serious data breach, leaving the client open to prosecution under the Data Protection Act, and the target of bad publicity. [redacted] recommended a complete redevelopment of the application, offering advice to the developers about secure coding practices from the start. As a result, the client was able to address the weaknesses in the application at the root cause level, reducing the on-going risk of compromise and support costs.

Technical Security Consultancy for Government Agencies

As part of the accreditation process for a client's restricted network, [redacted] coordinated the delivery of a multi-phase engagement, covering the client's networks and third parties in multiple locations across the country. In addition to enumerating individual vulnerabilities, the environment-wide testing revealed a number of serious underlying process failures that needed to be addressed to ensure that data within the network would be properly protected. The report from [redacted] team allowed the client to relate these findings constructively to the third parties involved in network and infrastructure management, and effect long-term changes in their internal security management processes to prevent recurrence of the issues identified.

User Access Review for Financial Organisation

A financial organisation was required to perform an internal due diligence audit, ensuring that all critical IT systems and applications conformed to the organisation's central policies with regards to user access, authorisation and accounting. Over the course of three months, [redacted] led a team of consultants conducting audit interviews with key systems administrators and business stakeholders, supplementing this with a hands-on technical investigation, to accurately establish the user access models present across the wide variety of technologies in use.

The result of the assessment was a documentation set identifying where current system management practices deviated from the organisation's internal policy requirements, including the identification of unnecessary access privileges, poor password management, areas where obsolete accounts had been left active and areas where system management did not conform to best practices.

[redacted] team also produced an access control framework report for each of the organisation's most critical applications, documenting exactly which employees had access to what, and what processes and procedures were in place to control access. The project was instrumental in allowing the client to focus their remediation effort on the most adversely affected systems in preparation to meet the requirements of their own group policies and an impending internal audit.

3.14 [redacted] – CHECK Team Leader

Profile

[redacted] is a CHECK Team Leader and security specialist with significant experience in technical security, penetration testing, application security testing, security infrastructure design and implementation and security best practices. He has a proven track record in the security and risk management field with practical experience of implementing security management frameworks (BS7799 / ISO27001).

He brings significant experience in design, configuration, maintenance and troubleshooting of layer 2 and layer 3 networks and VOIP solutions.

More recently, [redacted] has been responsible for running a team of consultants, managing workloads and maintaining budgetary control across a team of 20 consultants whilst ensuring that skills and personal development of team members is appropriate.

Qualifications

- CHECK Team Leader
- SC Cleared
- [redacted] - BSc (Hons) Psychology - [redacted].
- [redacted] - A Levels (Maths Physics Chemistry) - [redacted]
- [redacted] - GCSE's (9), including Maths, English, Computer Science

Employment

- [redacted] – CHECK Team Leader - Cyberis Limited
- [redacted] - Managing Consultant - [redacted]
- [redacted] - Senior Consultant - [redacted]
- [redacted] - Consultant - [redacted]
- [redacted] - Security and Networks Analyst - [redacted]
- [redacted] - Network support technician - [redacted]
- [redacted] - Support Engineer - [redacted]
- [redacted] Research Assistant - [redacted]

Areas of Expertise

- Network penetration Testing
- Application security and penetration testing
- Networking and security infrastructure.
- Team Management

3.15 [redacted] – CHECK Team Leader

Profile

[redacted] is a CHECK Team Leader and CREST certified Information Security Consultant with over [redacted] years' experience in IT, the past [redacted] of which have been in dedicated information security roles. He has expert technical knowledge of web applications, networks, all major desktop and mobile operating systems and is skilled at both offensive and defensive security techniques.

He is used to working across all levels of an organisation and is highly adept at discussing technical content with both technical and non-technical audiences. [redacted] is an active member of the Information Security community, learning and working for constant improvement through knowledge sharing and personal research.

Qualifications

- [redacted] CHECK Team Leader
- [redacted] CREST Certified Tester (Applications - [redacted])
- SC Cleared
- [redacted] Certified Information Systems Security Professional (CISSP)
- [redacted] - Cisco Certified Network Associate (CCNA)
- [redacted] - Red Hat Certified Engineer (RHCE) - [redacted]
- [redacted] - Sun Microsystems Certified Solaris 8 Administrator

Employment History

- [redacted] – CHECK Team Leader – Cyberis Limited
- [redacted] – Director – [redacted]
- [redacted] – Principal Security Consultant – [redacted]
- [redacted] – Information Security Manager – [redacted]
- [redacted] – Security and Networks Manager – [redacted]
- [redacted] – Senior Systems Administrator/Deputy IS Manager – [redacted]
- [redacted] – Senior UNIX and Networks Engineer – [redacted]
- [redacted] – IT Manager – [redacted]
- [redacted] – UNIX and Windows Administrator – [redacted]

Areas of Expertise

OPERATING SYSTEMS: • Cisco IOS, CatOS and PixOS • Check Point SecurePlatform • Nokia IPSO up to 4.2 • GNU/Linux (Red Hat, Debian, Ubuntu + others) • Solaris 2.5.1/2.6/8/9/10 • Windows NT/XP/2000/2003/2008/Vista/7 • FreeBSD, OpenBSD, BSDi, HP-UX • Backtrack/Kali Linux • Mac OS X • Citrix XenServer • VMWare ESX/ESXi	**PROGRAMMING LANGUAGES:** • Ruby • Python • PHP • Shell Scripting • Perl • Java • C# .NET • C **COMPLIANCE:** • PCI DSS • ISO 27001
HARDWARE: • Experience across a broad range of hardware including Cisco, Nokia, HP, Dell and Sun	**SOFTWARE:** • Apache & ApacheSSL • Tomcat Java Servlet Engine • Much, much more

Example Engagements

- Successfully completed many security testing engagements for clients, responsible for scoping and proposal generation through to scheduling, delivery and post-testing wash-up;
- Wrote and delivered a workshop “Burp Suite Plugin Development for Java n00bs” at 44CON, London 2012;
- Spoken at PHP London on the state of PHP (in)security;
- Spoken at OWASP Birmingham on PHP Object Injection, Burp Suite and Splunk;
- Presented lightning talks at BruCON 2012 and 2013;
- Identified and developed an exploit module for the Metasploit Framework for a security weakness in Splunk (Enterprise and Free);
- Developed a PCI DSS compliant information security policy from scratch and implemented solutions that have seen [redacted] through two successful PCI DSS assessments in 2009 and 2010;
- Introduced a cost-effective security solutions programme utilising intelligent deployment of both open source (FOSS) solutions and commercial applications;
- Conducted internal penetration testing which identified several critical vulnerabilities. Specified and implemented solutions for all test findings;
- Designed, planned and implemented a PCI DSS 1.2 compliant network and systems infrastructure. This involved a requirements gathering exercise, followed by detailed design and submission to our QSA for approval before planning, recruiting additional resource, purchasing and ultimately, implementation. Delivered hands on technical skills as well as managing a small team of contractors for this project.

3.16 Quality Management

The established procedure for dealing with work of this type is based upon Evolve's standard ISO9001 certificated processes, augmented by additional Account Management activity, to ensure complete supplier management and quality of Management Information, reporting and communication.

Cyberis has formally committed to Evolve's ISO9001 quality management procedures together with the Evolve stated company policies, standards and values. Evolve's role in any sub-contracted assignment is a proactive and visible one, in order to provide IPO with the assurance that all work is undertaken to our usual standards and in accordance with the Crown Commercial Service framework terms and conditions.

This process is defined within our Quality Management System (QMS) that includes procedures for the selection, management and quality assurance of sub-contractors. For completeness, we have included below the relevant sections from our QMS.

- Cyberis have been subject to a range of background checks including security vetting, capability to undertake the role and financial standing;
- Evolve have verified Cyberis technical and professional qualifications, track record and taken up appropriate public sector references;
- Cyberis has signed up to the Evolve quality system, with its required controls.

Evolve have assessed Cyberis in accordance with procurement and evaluation regimes established by organisations such as the Crown Commercial Service, including tendering, evaluation and identification.

Formal contracts are in place with Cyberis, defining all aspects of the relationship, including quality, performance, confidentially (based upon our ISO27001 certification), compliance with all health & safety legislation, standards, liability and intellectual property rights.

Only where we are satisfied that the sub-contractor and their consultants meet the client's requirements will they be recommended as part of any Evolve proposal. All sub contract work is subject to management by a full time senior member of the Evolve consultancy team through the application of defined and certificated 'Assignment Management' procedures. This role will be undertaken by [redacted], Evolve's Director of Consultancy. He will ensure that the work is delivered in accordance with the Evolve ISO9001 accredited QMS and the requirements of the CHECK scheme. [redacted] is a CESG CCP Lead SIRA who has extensive experience of Information Security in the public sector. He is a PRINCE2 practitioner, ITPC Government practitioner, Fellow of the Institute of Business Consultants and was a civil servant for [redacted] years.

4 CHARGES

4.1 Structure and profile of our proposed team

We propose a team approach undertaken by nominated CHECK Team Leaders.

Assignment Management and technical overview, provided by [redacted], Evolve's Director of Consultancy, together with Customer Care and Account Management Support will be provided free of charge.

4.2 Consultant fees

We propose a single discounted day rate of [redacted] for all elements of this work.

This rate is inclusive of all framework, customer, quantity and other discounts from the commencement of the work.

Hard drives to be left on site at the conclusion of the testing (if necessary) are to be replaced at cost.

Travel and subsistence costs for working at Concept House are included.

All prices quoted are exclusive of VAT at the prevailing rate.

4.3 Commercial Offer

Based on the information provided, we estimate that up to [redacted] man days may be required to complete the testing and report writing, together with reasonable contingency and follow up. We would only invoice for the days actually worked.

Based upon these assumptions we estimate a total cost of up to [redacted] at [redacted] per day = £14,960+ VAT.

We can confirm that this proposal shall remain valid for 30 days from the date of close of tender.

4.4 Acceptance of IPO Terms and Conditions

Evolve confirms acceptance of the IPO Standard Terms and Conditions and that no other Terms and Conditions shall apply.

Evolve confirms acceptance of the IPO Intellectual Property Rights as outlined within Clause 27 of the above IPO Standard Terms and Conditions.

Evolve confirms acceptance of Section 9 of the ITQ regarding the Requirement to Publish Contractual Information.

5 CORPORATE CAPABILITY

5.1 Evolve Secure Solutions Ltd

Evolve is an independent Cyber Security Consultancy, focused on providing high quality consultancy solutions to the Public Sector. We are on a number of Crown Commercial Service and other frameworks, providing a range of services such as IT Security, Information assurance and Business Continuity Planning. We have an established Information Assurance and Security Practice, which is managed by [redacted], our Director of Consulting, who is a Lead SIRA and ISO27001 Lead Auditor.

We certified by CESG as a Cyber Security Consultancy and were founder members of the CESG Listed Advisor Scheme (CLAS) for security consultants. All of our ISO27001 focused consultancy services were designed by a qualified ISO27001 Lead Auditor. Evolve holds its own certification to ISO27001. Our Quality Management system is ISO9001 certificated, and all our consultants receive full account management and technical support from our dedicated operational team.

In accordance with the Public Sector commitment to the environment and sustainability, Evolve is certificated to ISO14001 and is also an accredited 'Carbon Neutral' company. We are committed to continuing improvement of sustainability across all our corporate operations.

5.2 Cyberis

Cyberis is a CESG IT Health CHECK service company and is a CREST member.

All of their consultants are recognised experts in the security field, holding qualifications such as CHECK Team Leader, CREST Certified Infrastructure Tester and CREST Certified Application Tester. Our consultants have extensive experience working within multiple industry sectors and in similar projects, and are able to apply a wealth of historical knowledge to the project.

Cyberis prides itself on offering pragmatic and sensible solutions to risk management within business, taking business needs into account when prioritising remediation advice. We like to work closely with our clients to understand their business objectives, and their information assets, so that the advice we provide is relevant and contextualised.

5.3 References

We have provided the following references and case studies for our CHECK delivery partner Cyberis. Evolve references and track record can be provided upon request.

[redacted]
Cyberis has recently delivered a number of similar ITHC in respect of the [redacted] Protect Network under contract to Evolve.
[redacted] **– Operations ICT Manager**
[redacted]

[redacted]

Cyberis performed an application penetration test of an HMG system for [redacted] in September 2012.

[redacted] **– Technical L&D Manager**

[redacted]

[redacted] is a financial software development house. Cyberis has conducted a number of technical assurance engagements with [redacted] in recent months including extensive application and infrastructure level assessments.

[redacted] **– Head of Testing**

[redacted]

Cyberis staff have performed work with the [redacted] in the past, in many areas, but particularly infrastructure security testing and incident response.

[redacted] **– NDA Security Manager**

[redacted]

5.4 Case Studies

Within the last 12 months, Cyberis has delivered numerous engagements with HM Government, including:

- Four ITHC engagements conducted with [redacted], incorporating both infrastructure level assessments and application security testing;
- A multi-phase ITHC of a ministerial department network, including full internal and external infrastructure penetration tests, build reviews of servers and workstations, and password audit of the domain – providing a comprehensive assessment and level of assurance. Cyberis was commended for providing a 'first-class service with great helpful people';
- An extensive assessment of a sensitive internal production environment which incorporated infrastructure IT Health Checks, firewall configuration reviews, system and host build analysis and application security assessment. The organisation in question manages several large databases containing large quantities of personal data, and a review of this data protection against the requirements of GPG13 was also mandated;
- An extensive application security test against a platform providing statistical information to various Government agencies. The assessment revealed horizontal access control weaknesses that could compromise the confidentiality of the information. Following advice from Cyberis, our client was able to remediate these issues.

In the commercial arena, Cyberis has been recently involved in a number of relevant engagements, including:

- A full security assessment of public-facing transactional web applications, associated APIs and supporting infrastructure, identifying serious weaknesses in sensitive data handling and session management;
- An extensive and long term security consultancy engagement with a large organisation in the gambling sector which involved end-to-end security consultancy and technical assurance – covering everything from data mapping and migration plans, to the technical security of customer information, the security of associated web applications and payment details stored within back end processing systems;
- A full application security assessment for a financial software house which revealed a number of important access control issues within the application configuration. The weaknesses identified could have caused significant financial and reputational damage to the organisation concerned.