Service Definition – **Cyber Security Professional Services**

Version 0.1

CREST

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1. Service description

Redcentric offers a wide range of professional and managed cyber security services to support our clients in overcoming the cyber security challenges they face, delivering the outcomes they need to secure their business.

Redcentric Cyber Security Professional Services encompass a wide range of project types and deliverables.

We provide consultancy services that enable our clients to overcome their security challenges and realise the benefits of digital transformation and innovation without introducing undue cyber and operational risk, delivering key security and business outcomes.

- **Assured Availability** – Ensuring infrastructure resilience through effective cyber security defences to mitigate the impact of disruptive or destructive attacks.
- **Organisational Agility** – Adapting to and overcoming cyber and information security challenges related to the evolving threat and regulatory landscape.
- **Smarter Working** – Enabling organisations to adopt transformational technologies securely, without introducing unintended cyber and information security risk.

Our services are summarised in the table below. **Services in greyed-out boxes are managed services that are described in separate Service Description documents.**

Assurance – Testing cyber security defences to validate efficacy and identify gaps.

Penetration Testing (Applications and Network Infrastructure)	Penetration Testing is designed to uncover vulnerabilities and misconfigurations affecting digital networks, systems, and applications, providing the opportunity to identify them in a controlled environment and remediate before they can be leveraged by an attacker to cause harm.
Managed Vulnerability Scanning*	Managed Vulnerability Scanning enables clients to identify, prioritise, and remediate "known" vulnerabilities affecting digital systems and applications. The service is underpinned by our *Clarus* platform, combining automation with human analysis to consider whether the vulnerabilities can be practically leveraged by an attacker.
Design, Build, and Configuration Review	Design, Build, and Configuration Reviews are technical audits designed to identify design and configuration flaws which increase the attack surface of a device, appliance, or service. The focus of these audits ranges from Firewalls and security devices, to default server and workstation builds, to cloud service and infrastructure configuration.
Adversarial Simulation "Red Team" Testing	Adversary Simulation exercises (sometimes referred to as "Red Team" testing) are security assessments conducted from the perspective of a real-world external attacker. They are designed to stress test the organisation's defences in a realistic environment against probable attack scenarios to quantify cyber threat and risk exposure.
Human Security Services (Phishing and Social Engineering Simulation)	Redcentric provides a range of people-centric security services that are designed to reduce employee click-rate of suspicious and malicious communications, and encourage reporting of both successful and failed phishing attempts to enable proactive intervention from security teams.

Resilience – Assessing and implementing information security controls to create business and IT resilience.

Governance, Audit, and Compliance	We are experts in implementing and assessing compliance with a range of information security frameworks and standards such as ISO 27001, 27002, Cyber Essentials / Cyber Essentials Plus, PCI DSS, GDPR, SOC 2, etc., enabling our clients to meet internal security, business, and regulatory requirements.

Business Impact and Risk Assessment	Business Impact Analysis and Risk Assessment is an information-gathering exercise used to identify critical functions within a business and the potential risks that would affect normal operations by impairing these functions. It is a key component of a building business resilience, to tailor manage risks appropriately for the business context.
IT Service Continuity Assessment	IT Service Continuity consulting involves a deep-dive review of an organisation's IT services that underpin the critical functions that underpin business operations. Reviews can be conducted against specific frameworks and standards to meet a range of requirements, such as ISO 27031 and ISO 22301.
Disaster Recovery (Planning and Testing)	Redcentric provides a range of consultative services designed to help organisations to develop and test their plans to diagnose and coordinate the restoration of services following an incident, and where required recover critical IT services and infrastructure, identifying and stress-testing key recovery dependencies in realistic test scenarios.
Incident Readiness and Crisis Management	We deliver realistic tabletop exercises aligned to the different levels of decision making and response to an incident, from the executive level Crisis Management Team, to the Management layer, to first-line Incident Responders, ensuring that employees understand their roles and responsibilities and enabling effective decision making.

Defence – Monitoring IT environments for threats and responding to cyber security incidents.

Managed Detection and Response*	Redcentric's Managed Detection and Response service deploys highly certified security analysts in your environment 24/7 to detect, analyse, investigate, and actively respond to threats and security incidents across technologies, providing round-the-clock security in the face of malicious activity affecting your business.
Incident Response Retainer*	Redcentric's Incident Response Retainer provides on-demand access to Redcentric's incident response specialists in the event of a major cyber incident. The service is backed by a 5-hour SLA with guaranteed support, ensuring rapid remote support can be made available whenever a major incident occurs.

*These services are described in separate Service Definition documents which can be found alongside this document on the Redcentric website: https://www.redcentricplc.com/service-definitions/.

In addition to defined service offerings, Redcentric provides bespoke professional services projects with specific deliverables and custom methodologies in order to deliver specific cyber security and business outcomes.

2. About our consultants

We retain highly skilled, qualified, and experienced consultants with diverse backgrounds and skill sets, including penetration testers, ethical hackers, incident responders, threat hunters, risk managers, and information security managers. Our breadth of capabilities, experience, and expertise enables our clients to tackle a range of cyber security challenges and realise the outcomes they need to be secure.

We are a trusted provider for UK public and private sector clients, including organisations forming part of Critical National Infrastructure (CNI). Within the private sector, we support organisations of varied scale and cyber-maturity, from tech start-ups to FTSE100 members across a range of industry sectors, including Healthcare, Financial Services, Law, Marketing, Logistics, Education, Retail, Manufacturing, Logistics, and Insurance.

Our consultants possess a wide range of certifications that demonstrate their breadth and depth of cyber security knowledge and expertise across technical testing, information security and risk management, and incident response and forensics. These include, for example:

Offensive Security Testing	Defensive Security Operations	Cyber Resilience Consulting
Offensive Security Certified Professional (OSCP)	CREST Practitioner Security Analyst (CPSA)	Member of the Business Continuity Institute (MBCI)
Offensive Security Wireless Professional (OSWP)	GIAC Advisory Board	Certified Information Systems Security Professional (CISSP)
Systems Security Certified Practitioner (SSCP)	GIAC Certified Forensic Analyst (GCFA)	Certified Information Security Manager (CISM)
Certified Ethical Hacker (CEH)	GIAC Certified Detection Analyst (GCDA)	PRINCE2 and APM Project Management
CREST Registered Penetration Tester (CREST CRT)	GIAC Certified Incident Handler (GCIH)	ACII Chartered Insurance Risk Manager
GIAC Penetration Tester (GPEN)	Microsoft Certified: Azure Security Engineer Associate	ITIL v3 2011 Release and Change Management
CREST Certified Tester - Applications	CREST Practitioner Security Analyst	ISO 27001 Lead Implementer
Cyber Scheme Team Leader (CSTL) – Applications	EC-Council Certified Security Analyst	Security Cleared (SC) Consultants
Cyber Scheme Team Leader (CSTL) – Infrastructure		
CompTIA Security + & Pentest +		
Cisco Certified Network Associate (CCNA) (CyberOps)		

Our approach is underlined by our CREST accreditation for penetration testing services. Our CREST status can be verified via the following link: https://www.crest-approved.org/member_companies/7-elements-ltd/

Redcentric retains SC cleared consultants able to deliver work on behalf of UK government agencies and departments.

3. Engaging our services

The scoping and proposal process for a new project will conform to the following standard process:

- An opportunity will be raised and a scoping call will scheduled with the customer to discuss their requirements and ensure that their expectations are clearly understood and clarified.
- Where required the scoping consultant will request any further information needed to scope the project and accurately assess the time and materials required to deliver the project, as well as any other resource considerations (e.g. security clearance, seniority, specific technical credentials, required delivery timescales).
- A proposal will be issued confirming Redcentric's approach and providing pricing information.
- Once confirmed by the customer, the Proposal will be followed up with a formal Statement of Work for signature via the Redcentric Sales Support team. Where required, any additional customer onboarding activities will be initiated.
- Once authorised, the project will be scheduled by the Redcentric Cyber Security Delivery and Operations team. The team will be in touch prior to delivery commencement to ensure that all pre-requisites can be met for the designated start date to ensure smooth service delivery in line with the agreed timescales.

3.1. Engagement lifecycle

Key to our approach is working in close partnership with our customers. This builds long term relationships that enable tailored security approaches to be implemented that meet the organisation's business objectives. As such, we work with the customer to tailor our engagement model to suit their specific requirements. Our baseline engagement process is outlined below.

Pre-project

Redcentric will assign two individuals to this stage of the engagement. One will provide the Technical Point of Contact and will be the person responsible for the overall delivery of the test. They will work with the customer to ensure that all required information has been provided, agree testing windows, drive pre-requisites and ensure tests are carried out under the appropriate change management process. They will also work with the customer to provide technical information and briefings on the test approach to ensure organisational buy-in, as required.

The second point of contact will be with the Redcentric Relationship Manager. They will be on hand to provide engagement updates and act as a point of escalation as required. Prior to testing, all parties will agree to an escalation process in the event of any impact to the network or systems.

Delivery

Redcentric will perform the agreed testing/consultancy against the scope identified during the pre-project phase. During delivery phases, the Technical Point of Contact will keep the customer informed of any issues that arise, such as serious fault notifications or test limitations. Any additional requirements set out by the customer will be met.

Report

Redcentric will complete a detailed report on all findings from the engagement using an agreed format. The report will go through internal quality assurance (QA) prior to release to the customer. Redcentric will deliver the report within five working days of the test completion date.

On completion, the following will be submitted to the customer.

- High-level executive report outlining the overall testing engagement and any specific findings.

- Technical summary of key findings.
- Detailed technical report covering all security related issues found during the engagement and covering remediation recommendations.

Review

At the end of each test the Redcentric Relationship Manager will review the output from the test, any issues raised during testing, and the final report to ensure that our high standards of technical output and customer service have been met.

3.2. Project-specific elements

The following areas will be defined in the Proposal and/or Statement of Work documents that will be issued per each opportunity/customer project.

- The specific service(s) in-scope and a description of any relevant methodologies or approaches.
- A description of any technical or functional elements in-scope.
- Specific pre-requisites and the obligations of both Redcentric and the customer.
- Pricing and any specific terms and conditions relating to the project or service.
- Optional add-on services or deliverables relating to the services in-scope.

4. Testing Methodologies

High-level methodologies for defined services have been provided below. Specific and/or tailored methodologies and approaches may be developed to deliver key customer outcomes based on the requirements of a given project.

4.1. Application Testing

Redcentric will perform testing to identify vulnerabilities that could affect the confidentiality, integrity or availability of the data or systems, providing specific recommendations for remediation. Redcentric will also provide broader recommendations where flaws are identified that are likely to be duplicated across multiple systems to generate wider improvements to security posture, addressing the underlying root cause of issues – not just the symptoms.

Maintaining a repeatable and effective approach is core to the effective delivery of security testing. As such Redcentric has developed methodologies for all security engagements. However, as Redcentric utilises a manual testing approach, our methodology combines the need to establish a robust and repeatable approach while enabling the tester to react to individual situations and to test functionality, such as business logic as well as to develop custom code or discover previously unidentified attack vectors.

All of our methodologies are based upon industry recognised standards such as, but not limited to, Open Web Application Security (OWASP), ISECOM (the Institute for Security and Open Methodologies), The National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). Where required, Redcentric has experience of delivering bespoke methodologies created for individual clients.

Testing will be completed from both an unauthenticated and authenticated perspective as required. Deliberate denial of service or destructive testing will not be undertaken and testing will be completed in a risk-controlled manner. Testing typically covers a range of technical and logical vulnerabilities, such as:

Technical Vulnerabilities	Business Logic Issues
Command Execution Buffer Overflow OS Command Injection Xpath / XQuery Injection	**Authentication** Brute Force Account / Password Recovery Validation
Information Disclosure Directory Indexing Predictable Resource Location Improper Error Handling	**Authorisation** Credential/Session Prediction
Client-Side Content Spoofing Format String Attack SQL Injection Information Leakage Cross-site Scripting LDAP Injection SSI Injection Directory Traversal HTTP Response Splitting HTTP Parameter Pollution Clickjacking	**Logic Based Issues** Abuse of Functionality Insufficient Process Validation Insufficient Authorisation Cross-site Request Forgery Insufficient Session Expiration Denial of Service Conditions Weak Password Session Fixation Insufficient Anti-Automation

Where the assessment is broader in scope and includes testing of the underlying infrastructure components, Redcentric will identify weaknesses or vulnerabilities within the target network infrastructure and in components exposed to the Internet. This allows a profile of the security to be gathered and recommendations given on how best any problems can be mitigated.

4.2. Infrastructure Testing

In depth security analysis is required to ensure that services are adequately protected from attack by accidental or malicious attackers. The primary aim is to identify weaknesses or vulnerabilities within the target network infrastructure and in components exposed to the Internet. This allows a profile of the security to be gathered and recommendations given on how best any problems can be mitigated.

Testing will focus on the following areas:

- System discovery - Active probing of system ports to enumerate live or accessible services as well as probing, and traversing firewalls to find additional live systems. This involves open source/commercial scanning tools, firewall assessment applications and retrieving data from relevant servers where applicable.
- System fingerprinting - Identification of operating system and service versions will be undertaken against live hosts.
- Service probing - Where open ports are identified, service probing will then provide further details on applications and services running behind these ports.
- VPN & remote access - Virtual Private Networks (VPN) provide connectivity between geographically spread sites or allow remote users internal access to the corporate LAN. Both of these situations present a significant risk should the security of the VPN end point be poorly implemented. Where identified, VPN centric tests will be conducted. Tests are specific to the VPN end point and attempt to identify as much information regarding the server as possible.
- Automated Vulnerability Testing - The test team will use a range of tools to examine the network and systems for exposure to common vulnerabilities.
- Manual vulnerability testing and verification - The test team use their specialised knowledge of network security and knowledge of the latest vulnerabilities to re-examine network perimeters and systems. This process reduces as much as possible ‘false positives’ thereby improving the accuracy of testing results.
- Information Leakage - Excessive or unnecessary information disclosure, which gives information to an attacker that can aid in further attacks.
- Denial of Service - Attackers can consume resources to a point where other legitimate users can no longer access or use the client application. Testing is not directly conducted to confirm the existence of denial of service conditions, but inferred through known security weaknesses and environmental conditions.
- Insecure Data Storage - Insufficiently protected data storage that could provide partial or complete compromise of an application or its data. Such items can include, registry settings, system memory, poorly protected credentials or file permission issues.
- Other Issues - Other issues that would still result in a compromise to the confidentiality, integrity or availability of the system.

4.3. Thick Client Application Testing

The installation of thick client based software can cause a number of changes to the security posture of the environment. Client-server focused security testing aims to identify and analyse these changes to understand the changes made by the installation and use of software, and how it effects the overall security of the host operating system, internal network and data processed, transmitted and stored within.

Testing will be carried out within a specifically created virtual environment. Snapshots will be taken at various stages of testing to allow the consultants greater control of the environment with the ability to create snapshots of the system in various states.

Gaining assurance through client-server security testing is achieved by completing the following phases of activity:

1. Environmental Baseline and Comparison

Firstly a baseline is created to understand the configuration of the host operating system prior to the software being installed. Establishing a baseline will enable clear identification of any changes made to the initial configuration through software deployment. Software is then installed and a new baseline created allowing comparison of the following components

- New files written to disk
- New registry keys created
- New services created
- New user accounts added to the operating system
- Changes to files or service permissions
- Monitoring tools will be used to record any changes made to the system during installation.

2. Threat Surface Analysis

All changes made by the installation of software will be analysed manually to understand how, from a security perspective, they impact the host operating system and data stored or processed within.

3. Dynamic Analysis

Exposed components will be assessed for:

- Un-Validated Input - Information from client requests is not validated before being used by the application. Attackers can use these flaws to attack backend components through a client application.
- Broken Access Control - Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorised functions.
- Weak Authentication and Session Management - Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
- Improper Error Handling - Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the client application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the service.

4.4. API Endpoint Assessment

API security testing follows a similar methodology to web application testing, with a focus on issues which are specific to web services. As such we would adopt the following approach:

- **Enumeration of API endpoints** - This work is carried out to gain an understanding of the attack surface of the service under review. Commonly this exercise is completed either from the service itself advertising available endpoints, or by review of service documentation and calls made through valid applications.
- **Review of Authentication and Authorisation** - A critical point in web services security is ensuring that only valid users may process transactions within the application. The test team review each web services action from the perspective of an unauthorised user and then as an authorised user, to ensure that appropriate controls are correctly enforced.

- **Input Validation** - In common with most web applications, input validation is a key concern for web services. The test team reviews all inputs to the application to ensure that invalid input is correctly handled and includes reviewing for injection and external entity attacks.
- **Replay attacks and Session Management** - The test team will review the application to ensure that it is not possible for replay attacks and that appropriate session management is in place.
- **Encryption** - The test team will review sensitive data, whether in transit or stored on the client side, to assess its state and ensure that it is appropriately protected.

4.5. Wireless Security Assessment

The use of wireless networking within the office environment will pose a degree of risk to the information processed on that network. Additionally due to the nature of wireless networks where they can be accessed outside of a controlled environment, it is important to ensure that they are securely configured and that devices involved in the provision of wireless networking services do not have security weaknesses that could be exploited by an attacker. Further to this, if an organisation stores, processes or transmits card data, then under PCI DSS Requirements, scanning to detect and identify all authorised and unauthorised wireless access points has to be undertaken on a quarterly basis.

Our wireless security assessment methodology covers five key areas of activity:

-
- Passive Review of Wireless Infrastructure.
- **Error! Reference source not found.Active** Assessment of Wireless Infrastructure.
- **Error! Reference source not found.**.
- Extent of Coverage.

1. Passive Review of Wireless Infrastructure

By utilising non-invasive techniques, the current state of configuration and its level of security can be established. During this stage we will:

- Identify all Wireless Access Points (APs).
- Identify publicly available information broadcast by the APs

2. Active Assessment of Wireless Infrastructure

Attack scenarios will be developed according to the wireless configuration, but are likely to include areas such as the following:

- Session hijacking.
- Man in the middle attacks.
- Evil Twin attacks.
- Client-side attacks.
- Specific testing based upon threat profile

3. Discovery of Rogue Wireless Devices

Rogue APs can result in unauthorised data egress or in compromise of an internal network. This stage looks to identify if any rogue APs are connected to a secure physical network. In addition, other wireless activity will be scanned for, such as the probing attempts of clients in ad-hoc mode. These clients may include PDAs, laptops and other mobile devices.

4. Extent of Coverage

In order to limit exposure of the wireless network beyond the physical business environment, signal strength and location of APs should concentrate the wireless signal within a defined area. During this stage of the review a wireless site survey will be conducted. This review will look at wireless activity from outside and inside the organisation's premises to establish the extent of wireless connectivity

4.6. Breakout Testing

In depth security analysis is required to ensure that services are adequately protected from attack by accidental or malicious internal and external attackers. The primary aim is to identify weaknesses or vulnerabilities within the environment and associated network infrastructure that would result in an escalation of privileges within the environment, ability to bypass the operating system or network controls and therefore gain access beyond the intended isolated environment. This allows a profile of the security to be gathered and recommendations given on how best any problems can be mitigated.

Testing will focus on the following areas:

- Escalating Privileges - Is it possible to use the provided tools/permissions to escalate privileges either locally or on the network.
- Moving Laterally - Is it possible to abuse the provided permissions in order to access other customers data or systems that the user should not be able to access.
- Data Exfiltration – Is it possible for unauthorised or sensitive data to be removed from the device/network.
- Workspace Security Requirements - A list of security requirements has been provided and will be tested as part of the breakout assessment.

4.7. Mobile Application Security Testing

Redcentric follows a structured mobile application testing methodology based on the industry standards, as defined by OWASP.

Testing includes but isn't limited to finding the following common mobile application vulnerabilities:

- M1: Weak Server Side Controls
- M2: Insecure Data Storage
- M3: Insufficient Transport Layer Protection
- M4: Unintended Data Leakage
- M5: Poor Authorization and Authentication
- M6: Broken Cryptography
- M7: Client Side Injection
- M8: Security Decisions Via Untrusted Inputs
- M9: Improper Session Handling
- M10: Lack of Binary Protections

The mobile application security testing methodology can be broken down into the below three stages:

1. Information Gathering

The information gathering stage aims to prepare the testers for future testing phases by allowing a solid level of understanding of what the application does, how it does it, and what its functions are. This leads to identifying attack surfaces and understanding normal application activity. This stage helps to build awareness of the technologies in use within the application, mobile device and web components. At the end of this stage the tester will have gained an understanding of the application in normal use and can identify abnormal activity and functionality when exceptions occur.

2. Static Analysis

This stage focuses on the analysis of the mobile application binary or source code if available. If the source code isn't made available to test, the binary may need to be extracted from the device and disassembled, and in some cases, decrypted. During this stage the testers will attempt to identify the application permissions, frameworks, libraries, hardcoded secrets, such as API keys and credentials, data entry points, and access control measures and sanitation of data passed to the application. At the end of this stage, depending on the results, it may be necessary to go back to stage one and gather further information on the newly discovered components.

3. Dynamic Analysis

Using the data collected in the test so far, an informed security assessment of the mobile application client, servers and associated services can be performed. In this phase the use of intercepting proxies, debugging tools and scripting is used to perform dynamic access of the application in use. By the stage the attack surface of the application will have been identified, normal activity will be understood, and the tester can start to introduce unexpected data and identify how the application interacts with the various components identified in the previous stages.

Testing will focus primarily on the following components:

- Authentication
- Authorisation
- Session Management
- Data Storage
- Information Disclosure
- Common Web/API Issues
- Networking Protocols
- Transport Layer Protection

4.8. Citrix Testing Methodology

In depth security analysis is required to ensure that services are adequately protected from attack by accidental or malicious internal and external attackers. The primary aim is to identify weaknesses or vulnerabilities within the Citrix environment and associated network infrastructure that would result in an escalation of privileges within the Citrix environment, ability to bypass the operating system or network controls and therefore gain access beyond the intended isolated environment. This allows a profile of the security to be gathered and recommendations given on how best any problems can be mitigated.

Testing will focus on the following areas:

- **System Discovery** - Active probing of system ports to enumerate live or accessible services as associated with the Citrix environment. This involves open source/commercial scanning tools and retrieving data from relevant servers where applicable.
- **System Fingerprinting** - Identification of operating system and service versions will be undertaken against live hosts.

- **Service Probing** - Where open ports are identified, service probing will then provide further details on applications and services running behind these ports.
- **Automated Vulnerability Testing** - The test team will use a range of tools to examine the external network and systems for exposure to common vulnerabilities.
- **Manual Vulnerability Testing and Verification** - The test team use their specialised knowledge of network security and knowledge of the latest vulnerabilities to examine the Citrix environment. During this stage specific focus on the locked-down Citrix environment will be undertaken. This will include trying to launch arbitrary applications (for example cmd.exe) and to attempt to elevate privileges, break out of the isolated environment and attack back-end systems. Testing will also focus on infrastructure tests against the Citrix servers from the perspective of the end user to identify common vulnerabilities or security weaknesses.

4.9. Cloud Configuration Audit

Redcentric's audit approach combines bespoke audit scripts and evidence gathering with industry recognised benchmarks. Our approach has been further informed through the use of defined audit verification checks and associated white papers.

AWS audits are tailored to specific requirements of our clients on a per engagement basis, but in general cover the following core areas:

- Network Configuration and Management
- Asset Configuration and Management
- Logical Access Control
- Data Encryption
- Security Logging and Monitoring
- Security Incident Response
- Disaster Recovery
- Inherited Controls

Azure audits are tailored to specific requirements of our clients on a per engagement basis, but in general cover the following core components:

- Security Roles & Access Controls
- Data Collection & Storage
- Security Policies & Recommendations
- Identity & Access Management
- Ongoing Security Monitoring and logging
- Azure Security Center detection capabilities

4.10. Software Configuration Review Methodology

Correctly configured software is paramount to the security of an organisation. Often providing protection from a variety of issues, it is vital that these solutions are appropriately configured and maintained. Our approach focuses on a manual review of the device’s configuration to identify weaknesses within the firewall that may lead to a compromise of the network.

1. Security Audit

Review of the device configuration settings in order to identify security weaknesses within the following areas:

- Software Version
- Authentication
- Administration Services
- VPN Configuration
- Web Services
- IDS/IPS Functionality
- Routing Protocols
- Cryptographic Settings
- Logging

2. Configuration Audit

Review of the device configuration settings to identify security weaknesses within the following areas:

- General Device Settings
- Network Services
- Administration Settings
- Authentication Settings
- Network Interfaces
- Routing Protocols
- Logon Banners
- SNMP Settings
- Message Logging
- Time And Date Settings
- Network Filtering

4.11. Firewall Configuration Review Methodology

Correctly configured firewall devices are paramount to the security of an organisation. Often providing protection from Internet based attacks, it is vital that these devices are appropriately configured and maintained. Our approach focuses on a manual review of the device's configuration to identify weaknesses within the firewall that may lead to a compromise of the network.

1. Security Audit

Review of the device configuration settings in order to identify security weaknesses within the following areas:

- Software Version
- Authentication
- Administration Services
- VPN Configuration

- Web Services
- IDS/IPS Functionality
- Routing Protocols
- Cryptographic Settings
- Logging

2. Firewall Ruleset Audit

Review of the firewall rules in order to identify security weaknesses within the following areas:

- Conflicting rules
- ‘Any’ rules – Rules allowing any source, destination or port
- Rules that have no effect
- Unused rules, or rules with no purpose
- Lack of ‘catch all’ or ‘cleanup’ rules

3. Configuration Audit

Review of the device configuration settings to identify security weaknesses within the following areas:

- General Device Settings
- Network Services
- Administration Settings
- Authentication Settings
- Network Interfaces
- Routing Protocols
- Logon Banners
- SNMP Settings
- Message Logging
- Time And Date Settings
- Network Filtering

4. Review and Analysis

Review and analysis of all findings to look for issues, such as contradictory settings, that may impact the security of the network or device.

4.12. Digital Forensics

Our Digital Forensics service is based on the SANS Institute’s Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned (PICERL) framework. This tried and tested structure ensures our team delivers systematic and robust incident response that mitigates risks and secures your business.

Cyber Incident investigations relating to a compromise can include the following:

- Investigation into what happened, where and how.

- Log, host, and traffic analysis.
- Analysis of forensic artifacts and indicators on compromised servers and workstations.
- Malware analysis.
- Containment, eradication, and remediation assistance.
- A report of all findings, including recommendations to prevent further breaches.

Redcentric is typically engaged at the **Identification** stage.

A high-level table of activities that are typically performed at each stage is provided below.

Phase	Stages & Descriptions
Identification	• Identify the scope, impact, and potential root cause of the incident.
Containment	• Implement containment measures to limit the spread and impact of the security incident. • Coordinate with appropriate members of the IR team to isolate affected systems and implement short term mitigations. • Document efforts utilised to contain the security incident.
Eradication	• Investigate the root cause of the incident and develop a strategy for removing the threat from the environment. • Collaborate with relevant stakeholders to eradicate the threat and eliminate vulnerabilities. • Verify that the threat has been completely eradicated before moving to the recovery phase. • Document efforts utilised to eradicate threats during the security incident.
Recovery	• Restore affected systems and services to normal operations, following established recovery procedures and guidelines. • Coordinate recovery efforts with Redcentric and other external partners as required. • Communicate recovery status and updates to stakeholders using the Incident Response Communication Plan. • Document efforts utilised to recover from the security incident.
Lessons Learned	• Conduct a post-incident review to analyse the incident, evaluate the effectiveness of the response, and identify areas for improvement. • Update the incident response plan, security policies, and other relevant documents based on the lessons learned from the incident. • Share lessons learned and best practices with Redcentric and other partners to improve collective incident response capabilities.

At the outset it will be established whether the incident may result in a court case or involve law enforcement. If this is the case, then suitable evidence handling and chain of custody procedures must be applied. Within the UK the foundations for this approach have been well documented by the Association of Chief Police Officers (ACPO) and serve to ensure that evidence handling, investigation practices, and supporting activity are carried out legally. Where a 'forensically sound' approach is required, Redcentric can advise and co-ordinate the necessary response using forensically trained specialists.

5. Consulting Methodologies

High-level methodologies for defined services have been provided below. Whilst repeatable processes exist the majority of consultative projects are to some degree bespoke based on the customer's business and technology requirements.

5.1. Crisis Management Tabletop Exercise

Redcentric provide coached Cyber Security Incident Management Exercises for the Incident Response Team (IRT), Incident Management Team (IMT) and Crisis Management Team (CMT). The exercise involves a tailored cyber crisis scenario. Following the exercise, Redcentric make recommendations on how to further develop Incident Management and Response capabilities through providing a report with observations and recommendations.

The exercise is typically preceded by a 2-hour masterclass exercise. The purpose of the masterclass is to prepare the teams for the upcoming exercise. By delivering the masterclass ahead of the exercise, the groundwork for effective response can be laid, and the risk of participants feeling ambushed or unprepared is minimised. The best crisis management exercises involve the participation of an engaged team who embrace the exercise as a means of generating improvement in a controlled environment.

The approach to deliver the exercise will include:

- Phase 1: Scenario development, tailoring the scenarios to the technology and business context.
- Phase 2: Exercise development, including detailed plans, injects, prompts, and slides.
- Phase 3: Delivery of a 2-hour crisis management exercise.

The exercise will leverage Redcentric's experience investigating cyber security incidents to provide a realistic and authentic scenario in an interactive table-top environment. Redcentric consultants are able to draw on and incorporate experience from real world attacks to bring the scenario to life throughout the stages of the exercise. Suggested themes for the exercise include:

- Following a successful phishing attack, the attacked establishes mailbox rules facilitating a sophisticated "man-in-the-middle" Business Email Compromise (BEC). BEC often target Finance staff and seek to amend invoice payment details to syphon off significant funds from either the target business or a supplier/client. The presence of a BEC attack can often go unnoticed for a considerable period of time until either the business or the supplier/client makes a phone call to question the activities.
- Network infrastructure and systems are compromised following an advanced attack, malware is installed that encrypts critical operational applications, and a ransomware demand is received. This malware is operating for an extended period before being discovered. The malware starts 'below the radar' but then starts to have a negative impact on performance generally. On discovery, the cyber attackers activate encryption algorithms and demand payment to restore systems access and delete stolen data.

The exercise will replicate the structure of a real-world incident (albeit to an accelerated timeframe) by issuing a series of updates or 'injects' over the course of the workshop. This sees the situation evolve over time and prompts further discussion and problem-solving to take place, enabling gaps to be identified at various stages of the response timeline.

Redcentric provide all supporting material to facilitate the training, as well as a management report outlining observations and recommendations following the exercise. This report will cover the team's knowledge of policies and procedures, the performance against the scenario, and the effectiveness of the policy and procedures in supporting the team through the scenario. The exercise will enable the client to:

- Exercise roles and responsibilities after an issue is identified.
- Walk-through and become familiar with the response and resolution process.
- Become familiar with the trade-offs involved in containing incidents and the impact of decisions.
- Practice making decisions under pressure based on the evidence available.

- Understand the required recovery activities after an incident and timeline to restore BAU operations.

5.2. Business Impact Analysis

In order that effective BC capabilities and plans might be developed it is vital to have a detailed understanding of the BC priorities through an analysis of the business criticalities and the hazards and threats that may result in disruptions. The Business Impact Analysis (BIA) provides an insight into the DNA of business operations – what it does – its products/services, the consequences of a disruption to the delivery of the activities that contribute to them, a definition of the recovery requirements for the business and support functions – what must be recovered and when - and enables us to propose appropriate continuity and resilience strategy options. It also defines the resources needed for recovery and any associated key dependencies, as well as recommendations for prudent risk and impact mitigation.

The BIA Update will review and update any existing documentation and will enhance understanding of:

- Critical Activities – Identifying the activities that support the delivery of UBA UK's business services.
- Dependencies – identifying the internal and external services and assets that the critical activities require for continued operation.
- Impact of disruption – assessing the impact of a disruption on operations, client service, reputation, regulatory compliance, finance and staff.
- Recovery needs – identifying and prioritising the recovery needs for critical functions in terms of resources, assets and technology support.

The resultant BIA report will provide the essential information to enable the customer to determine the recovery requirements for the various functions across its business and formulate an approach that defines what must be recovered, the recovery timelines, the resources needed for recovery and any associated key dependencies.

We will conduct a series of interviews and workshops with the departments in scope, to refresh the content (as outlined above) to identify where there are any significant relevant changes. Critical activities may have changed, priorities might be different post-pandemic, there may be different critical applications and services now in use.

5.3. Business Continuity Plan Development

BC Plans provide an organisation with a documented framework for responding to an incident or disruption and managing the resumption of time-critical activities within acceptable timescales. Redcentric will use information derived from the updated BIA to update existing Word-based plan documents relevant to the needs of the organisation (ideally in a common format). These will include:

- Incident Management
  - Incident Response
  - Assessment and escalation protocols
- Business Continuity and Continuity Support
  - Continuity activity management
  - Team recovery documents
  - Recovery tasks aligned to re-instatement of critical activities within required timescales
  - Appendices relevant to the needs of the organisation.

Content developed may cover:

- Roles and responsibilities
  - Defined roles

    - Team structures
    - Guidelines and framework for activities
- Response process and procedures
    - Activity management
    - Invocation procedures
    - “Standing down” procedures
    - Meeting and recovery locations
    - Recovery tasks of critical activities and required timescales
- Incident Management
    - Structure, command and control
    - Resource requirements
    - Information recording
- Communications
    - Internal communications
    - External communications
    - Contact records (internal and external)
    - Cascade structures and processes

The deliverable is a series of updated Word-based BC Plan documents that cover the in-scope departments, including the overall organisational BC Plan, and that reflect the current approach to incident management. In line with industry good practice we will ensure that the updated plans are action-oriented, easy to reference and in a format and layout that is functional and practical.

5.4. Business Continuity and Disaster Recovery Testing

Business Continuity Exercises are recommended to ensure the documents and processes are fit for purpose and to ensure staff fully understand the roles assigned to them.

The exercise will involve a tailored scenario. Following the exercise, Redcentric will make recommendations on how to further develop the customer’s response capabilities, providing a report with observations and recommendations.

Deliverables will be:

- Scenario development, establishing a suitable crisis scenario and gaining approval for the desired outcomes and objectives.
- Exercise development, including injects, slides and logs.
- Delivery of a scenario exercise focused on helping the IT Team to learn, reflect and improve.
- Exercise report and recommendations for improvement.

Without performing IT DR testing, no organisation can be sure it can successfully recover its priority IT resources. It is important to manage the risks associated with such testing activities. This can be achieved by carrying out component tests (e.g. application tests, simulated failover or “bubble” tests for High Availability environments) prior to undertaking a full system DR Test. These application tests will also help direct the likely timeline required to undertake a larger DR Test, ie a full data centre failover.

For each DR test managed by Redcentric, the Consultant will:

- Hold a pre-test meeting (via conference call) to define the scope, personnel involved, identify risks, likely timescales for the test, begin to define any element that needs business approval/access arrangements etc)
- Arrange progress meetings as necessary (usually weekly starting at least 4-6 weeks prior to the test) to develop the test plan and ensure all identified risks are managed
- Work with technical staff to document a test plan and finalise the runbook
- Attend the test – document progress of the test including issues, recovery times and ensure test plan is being followed
- Produce a post-test report
- Hold post-test meeting(s) (via conference call) to ensure all actions identified are assigned for completion
- Ensure the runbook is updated by Redcentric staff

5.5. Information Security Management Consultancy

Organisations are required to maintain and demonstrate compliance with a range of information security frameworks and standards to conduct their business, such as ISO 27001, 27002, Cyber Essentials / Cyber Essentials Plus, PCI DSS, GDPR, SOC 2, and so on.

We help organisations to:

- Achieve and maintain compliance to grow your business by demonstrating your credibility as a supplier, making you an attractive partner for your customers and stakeholders.
- Balance compliance with security to ensure that your information security policies, processes, and procedures result in a practical uplift to your security posture, not just ticking a box.
- Identify compliance gaps and access specialist knowledge and expertise to quickly address them ahead of a planned third-party audit.

Our InfoSec consultants offer advice and guidance on the protection of strategic information and other assets which are essential for an organisation and enable them to meet organisational goals. We provide assessments based on industry best practices and aligned with various standardised control frameworks and industry standards, including ISO 27001, 27701, Cyber Essentials / Cyber Essentials Plus, PCI DSS, GDPR, SOC 2, the NIST Cyber Security Framework, CIS Control Framework and so on.

Although the approach will vary depending on the security and compliance goals of the organisation, we typically follow a repeatable high-level approach:

- Step 1 – Identify business goals
- Step 2 – Identify essential information and assets
- Step 3 – Mitigate risk – people, processes, tools
- Step 4 – Monitor and report
- Step 5 – Review controls at regular intervals

Effective cyber security operations rely on a combination of preventive and detective controls. Therefore we consider the following areas when analysing an organisations capabilities (and gaps) to determine an appropriate treatment and improvement plan.

Preventative controls

Create security awareness by educating leadership and employees for example:

- Define who has access to what data

- Ensure employees understand phishing risks
- Ensure important data is not left out on desks

Put in place processes, for example:

- Prevent unauthorised access to your network with authentication
- Ensure patch management is up to date

Put in place policies for example:

- Define how to access data safely when travelling
- Ensure staff know what to do when plugging in a USB stick

Detective controls

- Monitor who has accessed what data
- Monitor devices on the network
- Ensure you have a digital audit trail which provides logs to help detect intrusions

5.6. Call-off Consulting

Redcentric provides flexible “call-off” Cyber Security knowledge from our experienced Cyber Security, Business Continuity (BC), operational resilience, and information security (IS) consultants. Equally, the call-off consulting can be used to conduct Penetration Testing if required.

The service allocates several “call off” days defined within the contract. The flexibility means that days can be used when needed to meet objectives and commitments in relation to business resilience, information availability and recoverability.

Examples of how call-off consulting can be employed include:

- Support to Operational Resilience programme implementation and ongoing operation
- Cyber Security Awareness training
- Development of Cyber Incident Response Plans
- SecOps and InfoSec support
- Penetration Testing
- Review and update Cyber Security policy, strategy, and programme documentation
- Crisis Management training and awareness (group and individual)
- Refresh Business Impact Analysis and Risk Assessments (BIRA)
- Update and extend BC Plans
- IT DR review, plan development and testing
- Cloud Infrastructure Security Hardening Review
- Guidance on IS risk treatment plans
- Reporting and audit
- Ad-hoc support, advice, and guidance

Document Control

Service Category	Cyber Security
Title	Cyber Security Professional Services Service Definition
Reviewer	Tom Holloway
Business Area	CSG
Review Cycle	Annual

Version and Change Control

Version	Date	Change
1.0	19/02/2024	Released

Ownership

Redcentric's Cyber Security Management Team is the collective owner of this document and responsible for ensuring that this definition is reviewed in line with the requirements of Redcentric's ISO 9001 Quality Management System.

Disclaimer

This information is subject to formal contract and is an indicative and unqualified invitation to treat not capable of acceptance. No contractual relationship shall exist until formal contract documentation has been negotiated and executed by both parties.

Redcentric does not warrant the completeness or accuracy of the information contained herein and shall not be responsible for technical or editorial errors or omissions. Other than as stated elsewhere in this document, Redcentric hereby excludes any express or implied warranties that may be contained in this document and further disclaims all liabilities which may arise due to, and/or as a consequence of, reliance on the information contained herein.

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED