ADVENT IM

G-Cloud 15

Lot 3 – Cloud Support Services

Service Definition:

Red Team Covert Exercise (Red Team Testing/Physical Penetration Test)

connect	visit
@Advent_IM	advent-im.co.uk

1.0 Introduction

Advent IM Limited delivers various Cloud Support Services under Lot 3 of the G-Cloud 15 Framework.

- ✓ Security Consultancy
- ✓ Security Technical Services
- ✓ Security Training

Advent IM has a team of highly experienced and security cleared experts delivering Governance, Risk and Compliance services (GRC) across all areas of security including data, physical and cyber covering information assurance, data protection, business continuity and more. Operating in the public, private and third sectors, Advent IM's team are very highly regarded by clients and are known for their pragmatic approach and superb track record.

Our consultants are NCSC GovAssure trained auditors, ISO27001 Lead Auditors, General Data Protection Regulation (GDPR) Practitioners and include a team of CPNI, Home Office trained, ex-military physical security specialists. Advent IM itself is a Governance, Risk and Compliance Security Supplier to Government and the wider public sector and our services are also available on the Digital Outcomes and Specialists Framework and JOSCAR. In addition, Advent IM is a (UKAS) ISO:9001 and ISO:27001 certified organisation, as well as holding Cyber Essentials and Cyber Essentials Plus. Through our trusted CHECK and CREST accredited partners we can also provide a wide range of testing and digital forensics services.

A full company overview and service portfolio can be found in Section 4.0 Advent IM Company Overview

1.1 Contact Details

The team will be happy to help with enquiries and provide further information on any of our Cloud Support Services.

0121 559 6699

www.advent-im.co.uk

G-Cloud@advent-im.co.uk

Cradley Enterprise Centre
Maypole Fields
Halesowen
West Midlands
B63 2QB

2.0 Service Definition

2.1 Red Team Covert Exercise (Red Team Testing/Physical Penetration Test)

Red Teaming exercise for organisations wanting intelligence-led physical-penetration-testing (PPT). Sometimes labelled 'Black Teaming', Red Team Assessments are designed to penetration test an organisation's physical premises by engineering real-life scenarios that tests physical security measures, policies and procedures against real-world specific threats utilising social engineering and intelligence-led information accessible to hackers.

Features include:

- Remote Project Initiation: Establishing Clear Testing Scope and Boundaries
- Leveraging Open Source Intelligence (OSINT) to Uncover Exploitation Vectors
- Pre-testing Passive Reconnaissance Activities to Identify Actual Vulnerabilities
- Collaborative Team Testing Reducing Risk of Recognition
- Active Covert Reconnaissance to Exploit One-Off Opportunities/ Vulnerabilities
- In-depth Observational Reporting with Risk-Prioritised Mitigation Recommendations
- Enhanced Documentation with Photographic Evidence to Support Findings
- Non-Brute Force Techniques Ensuring Non-Disruptive Testing
- Dual-Phase Assessment: Threat Intelligence (TI-OSINT) and Physical Penetration Test (PT)

Benefits include:

- Real-world hacker scenario testing utilising actual threat intelligence
- Analysis is outcome-driven by genuine weaknesses/ exploited gaps in security
- Strategic, cost-effective cybersecurity recommendations tailored to maximise your ROI
- UK-based, SC-cleared cybersecurity professionals: ensuring high trust and compliance standards
- Enables swift remediation of exploited security practices
- Bespoke cybersecurity solutions: tailored to fit your requirements
- Team-testing increases the success rate of testing outcomes
- Independent, vendor-agnostic security assessments providing objective and unbiased insights
- Extensive experience with public sector security protocols
- NPSA/CPNI certified, home office trained with tactical insights from ex-military

3.0 Service and Contract Management

3.1 Quality of Service

Through Advent IM's (UKAS) certified ISO 9001 Quality Management System, Advent IM can assure clients of consistent delivery of high quality service provision. We ensure all our internal and client side facing business processes are regularly reviewed to maximise benefit for our clients, staff, partners and stakeholders. Our trusted partners also hold ISO 9001 certifications.

3.2 Security of Service

As Information Security is Advent IM's core business, we take Information Security seriously and we have integrated our (UKAS) ISO:27001 Information Security Management System into our Quality Management System, to produce a (UKAS) audited Business Management System that can not only assure delivery of a consistent quality service but also one which has security in mind. We also hold Cyber Essentials and Cyber Essentials Plus. Our trusted partners also hold ISO 27001, Cyber Essentials and Cyber Essentials Plus certifications.

3.3 Service Team Members

In the first month of any contract being awarded, principal members of staff are allocated to the contract including (but not limited to):

- **Dedicated Client Manager -** This will be a senior member of the Client Engagement team who will be the initial point of contact for the Contracting Body for all non-project specific related matters. This ensures the Contracting Body will benefit from a single point of contact simplifying and streamlining service delivery; and
- **Lead/Principal Consultant -** This will be one of the most senior members of the consultancy team with the most skills and relevant market and sector experience for the project or engagement. This ensures the Contracting Body will benefit from the right consultant being selected to lead the contract and will maintain consultant relationship continuity.
- **Project Co-ordinator** – To ensure a smooth delivery process.

3.4 Project Management

Advent IM employs Project Management in line with PRINCE2 for each new project, as applicable. This includes (but is not limited to):

- Project Initiation Meeting (PIM), to confirm the scope, objectives, contacts, deliverables, timelines and assumptions of the project
- Project Initiation Document (PID), to capture and document the PIM discussions for agreement between the parties
- Project and Critical Path Planning, using such project management tools to provide the Contracting Body with a visual picture of the project timelines and dependencies
- Project Management Meetings and Checkpoint Project Reporting, to provide the Contracting Body with regular updates on the progress, issues/resolution of and timings (completed and forward booked)
- Project Closure Meeting/Process to formally close off each project and ensure that all deliverables captured in the PID have completed successfully and to the Contracting Body's satisfaction

3.5 Program and Project Initiation

At the point of a contract being awarded, a Project Initiation Meeting (PIM) will be arranged to agree/confirm the scope for the project, this will include discussions to agree and document (but not limited to) the following:

- Communications structures
- Lines and methods of reporting
- Escalation including those procedures for reporting urgent incidents and issues
- Ensure the Client has Director level support and contact when required
- Issue management and resolution
- Contract and project management processes
- Quality metrics and reporting mechanisms
- Roles and responsibilities of all staff involved in future projects, including but not limited to Advent IM's: Project Coordinator; Client Manager; and Lead/Principle Consultant
- Processes not documented for initiating an individual project, commercially and operationally
- Service Level Targets (SLTs) and Service Level Objectives (SLOs) not contained within the contract documentation

The meeting ensures the Contracting Body benefits from a streamlined delivery service, as important processes are defined at the outset to facilitate a smooth and more consistent contract delivery. It also reduces risk for the Contracting Body of issues arising. Introducing the persons involved in delivering the contract helps both organisations to get to know each other culturally in order to build and maintain trust and effective working relationships. It is also expected that non-operational areas will be discussed such as sensitive issues and political sensitivities that may exist that Advent IM should be aware of in order to deliver the best quality of service possible.

In order for Advent IM to engage with the Contracting Body at a strategic level, this meeting shall be attended by:

- Advent IM's Delivery Director (when required); Project Coordinator (when required); Client Manager; and Lead/Principal Consultant
- Similar counterparts and other senior stakeholders from the Contracting body

4.0 Advent IM - Company Overview

We are a different kind of security consultancy. Whilst offering the highest degree of experience and skill from our consultants, Advent IM has a supportive, collaborative and highly integrated approach. We work *with* our clients rather than delivering consultancy *at* them. Our clients find this to be a more effective approach, adding value and delivering a high return on investment.

How working with us will benefit you:

- **You will benefit from us employing our own consultants on a full time permanent basis to deliver our core consultancy services ensuring the highest levels of service consistency and quality and the ability to build strong, long term working relationships**
- **You will benefit from us only employing the best. We don't use graduates or juniors. All our consultants have a minimum of 10 years direct security experience and a number of years of senior consulting experience. Our staff are at the forefront of our industry and are actively engaged in Policy formation and development at the highest level**
- **You will benefit from our unique, collaborative approach of facilitating and mentoring, leaving you and your individual personnel fully prepared following project close out**
- **You will benefit from us building long term partnerships with you based on trust and integrity that add value to your organisation. We know how valuable it is to deal with the same people regularly**
- **You will benefit from our integrated approach to risk management which reduces duplication, costs and bureaucracy and results in an embedded, enabling, organisation-wide culture where everyone owns and manages risk to information assets**
- **You benefit from our open and ethical approach. Our advice is completely vendor independent and unbiased. We don't sell anything or have any agenda to promote any vendor products**
- **Our unique service delivery methodology ensures you will get a high Return on Investment (ROI) and Value for Money (VFM)**

OUR CONSULTANCY COVERS:

INFORMATION SECURITY MANAGEMENT (ISO 27001:2022)

- Gap Analysis
- Risk Assessment
- Risk Treatment
- Statement of Applicability
- Policy Development
- ISMS implementation
- Internal Auditing
- Pre-Certification Audit

ARTIFICIAL INTELLIGENCE (ISO 42001)

- Gap Analysis
- Risk Assessment
- Risk Treatment
- Policy Development
- Management System Implementation
- Internal Auditing
- Pre-Certification Audit
- Awareness Training

BUSINESS CONTINUITY

- Gap Analysis
- Business Impact Analysis
- Risk Assessment & Risk Treatment Plan
- Business Continuity Strategy
- Business Continuity Planning
- Training
- Testing
- Pre-Certification Audit

HMG TECHNOLOGY & INFORMATION RISK MANAGEMENT AND ASSURANCE

- Continuous assurance following Secure By Design principles (SbD)
- Application of current and legacy IA Assurance Methodologies
- Risk Management, Risk Assessment & Risk Treatment following guidance including ISO 27005, ISO 31000, ISO 27002 and NIST
- Security Architecture System Designs and Reviews
- Digital and Cloud Security Services
- IA Audits and Reviews including GovAssure and GovS007 Compliance

- IA Incident Management
- IA Policy & Standards Advice and Guidance, including policy development and reviews
- Advice on Off-shoring Data
- System Decommissioning Services
- Codes of Connection Reviews e.g. PSN
- Privacy Impact Assessments

PCI-DSS COMPLIANCE

- Prioritised Assessment of compliance, identifying any gaps and remediation requirements
- Physical Security Review to comply with Requirement 9 – a major non-IT related part of the standard
- Identification and documentation of Compensating Controls
- Ad hoc help and guidance on remediation implementation including a one-off PCI Audit
- Re-assessment of compliance after you have implemented all remediation requirements
- A regular PCI-DSS assessment against the Self-Assessment Questionnaire (SAQ) to meet ongoing compliance requirements
- Completion of the Annual Attestation of Compliance (AoC) (you may need this to demonstrate compliance to prospective customers)

PHYSICAL SECURITY: REVIEW, AUDIT & TEST

- Holistic Threat Assessments
- Security Reviews and Audits including PASF and TPAP
- Security Design Solutions and Design Reviews
- Testing and Commissioning of Security Components
- Education Physical Security Reviews

MY SECURITY MANAGER

- Access to a Dedicated Security Manager and a Pool of Experts Across our Services Portfolio
- Packaged Solutions with Scheduled and Ad-hoc on Site Presence
- Email Enquiry Service

RED TEAMING

- A test of your physical security measures
- Testing How Staff Adhere to the Policies and Procedures Implemented by your Organisation
- What Information can be Gathered via Social Engineering

- How Effective your Physical Security Controls Work in Practice

PENETRATION TESTING THROUGH TRUSTED CHECK/CREST PARTNERS

- Internal and External Penetration Testing
- Cyber Essentials Testing
- PSN Initial and Ongoing Compliance Testing
- Website and Web Application Testing
- Application and Mobile App Testing
- Server Build and Infrastructure Testing
- Network Fabric and Firewall Testing
- Wireless Testing
- Desktop and Mobile Device Testing
- What Information can be Gathered via Social Engineering
- How Effective your Physical Security Controls Work in Practice

SURVEILLANCE CAMERA CONSULTING

- Unique Reviews Suited to Your Business
- Determine if Planned Upgrade / New Systems are Actually Required
- Cover Multiple or Single Systems / Components

DATA PROTECTION

- Data Protection, UK General Data Protection Regulation (GDPR) and Data Use & Access Act (DUAA) Consultancy
- Full Outsourced Data Protection Advisory Service
- Writing, reviewing and updating of Data Protection Policy
- Data Compliance Checks and Audits against the Act and associated Codes of Practice such as UK GDPR and PIRM (formerly MOPI)
- Data Protection, UK GDPR, DUAA Staff Awareness Training
- Identification of Data Protection responsibilities when offshoring data
- Ad hoc assistance with implementing new and emerging directives from the Information Commissioner's Office (ICO) such as UK GDPR
- Support in Data Breach Crisis Management, ICO undertakings and Monetary Penalty situations
- Cyber Attack Crisis Management

CYBER ESSENTIALS AND CYBER ESSENTIALS PLUS CONSULTING

- Review of existing documented processes
- One to one interviews to collect required information
- Assisted 'live' self-completion of questionnaire
- This consultancy is needs driven and will be dependent upon client security management maturity levels

- Cyber Essentials Plus testing through trusted partners

MY DATA PROTECTION OFFICER

- Outsourced security management
- Scalable, flexible bespoke solution
- Onsite presence
- Project management
- Fixed price solutions
- Available nationwide

THIRD PARTY AUDIT and SUPPLY CHAIN ASSURANCE

- Evaluate risks and recommend the best and most appropriate responses
- Draft the right standards that a supplier should have in place
- Audit suppliers
- Penetration testing and red teaming is also available

POLICE CYBER SECURITY

- Information Governance Reviews covering strategy, roles, responsibilities and policy
- Application of IA Assurance Methodologies including Secure By Design (SbD)
- End to end system and Network Accreditation & Information Risk Management following PDS guidance including Risk Assessments & Risk Treatment
- Third Party Assurance for Police (TPAP) Consultancy and Training
- Security Architecture System Designs and Reviews
- IA Audits and Reviews including PASF
- IA Incident Management Analysis
- IA Policy & Standards Advice and Guidance
- IA Governance and Strategy Review and Development
- Codes of Connections Reviews

MOD SUPPLIER SECURITY

- Assurance services using MoD SbD Process mandated in JSP 440 Leaflet 5C
- Continual Assurance of information-based capability in line with JSP440 and NIST
- NIST adoption including NIST CSF, NIST SP800-37, NIST SP800-53
- Physical Security Reviews
- Risk Management, Risk Assessment & Risk Treatment
- Digital and Cloud Security Services
- Technology Risk Assessment
- Defence Cyber Certification (DCC) Consultancy Support
- Training

- Outsourced Specialist Individuals or Teams on an ad-hoc or contractual basis

ADVENT IM OUTSOURCED SERVICES

- Advent IM excellence, at scale
- Wide range of individual roles or whole project teams
- Complete people and project management
- Recruitment, Interviews, including a Senior Advent IM Security Consultant
- Vetting
- Onboarding/offboarding
- Timesheet management
- Issue escalation
- One contract, one contact for whole project team
- Wraparound Advent IM project management, if required

OUR TRAINING COVERS:

DATA PROTECTION TRAINING

- Data Protection / UK GDPR / DUAA Awareness Training
- Public Sector Data Protection Training for Non DPOs Intermediate
- Public Sector Data Protection Training for Non DPOs Advanced
- Public Sector Data Protection Practitioner Training
- Police Data Protection Training for Non DPOs Intermediate
- Police Data Protection Training for Non DPOs Advanced
- Police Data Protection Practitioner Training

INFORMATION ASSET OWNER

- Preparing for Information Asset Owner (IAO)
- Public Sector The Essentials Information Asset Owner (IAO) Training
- Public Sector Intermediate Information Asset Owner (IAO) Training
- Public Sector Advanced Information Asset Owner (IAO) Training
- Police The Essentials Information Asset Owner (IAO) Training
- Police Intermediate Information Asset Owner (IAO) Training
- Police Advanced Information Asset Owner (IAO) Training

SENIOR INFORMATION RISK OWNER TRAINING

- Police Senior Information Risk Owner (SIRO) Training
- Public Sector Senior Information Risk Owner (SIRO) Training

OTHER TRAINING

- Third Party Assurance for Police (TPAP)
- Technology & Information Risk (TIRM) Management Training

- Bespoke Training – tailored training courses related to our security consultancy services portfolio
- AI Security Awareness Training
- Data Use & Access Act Training
- Secure by Design Training for MOD, Police & Central Government
- Secure by Design Awareness Training for Security Engineers
- Security Aspects Letter (SAL) Training