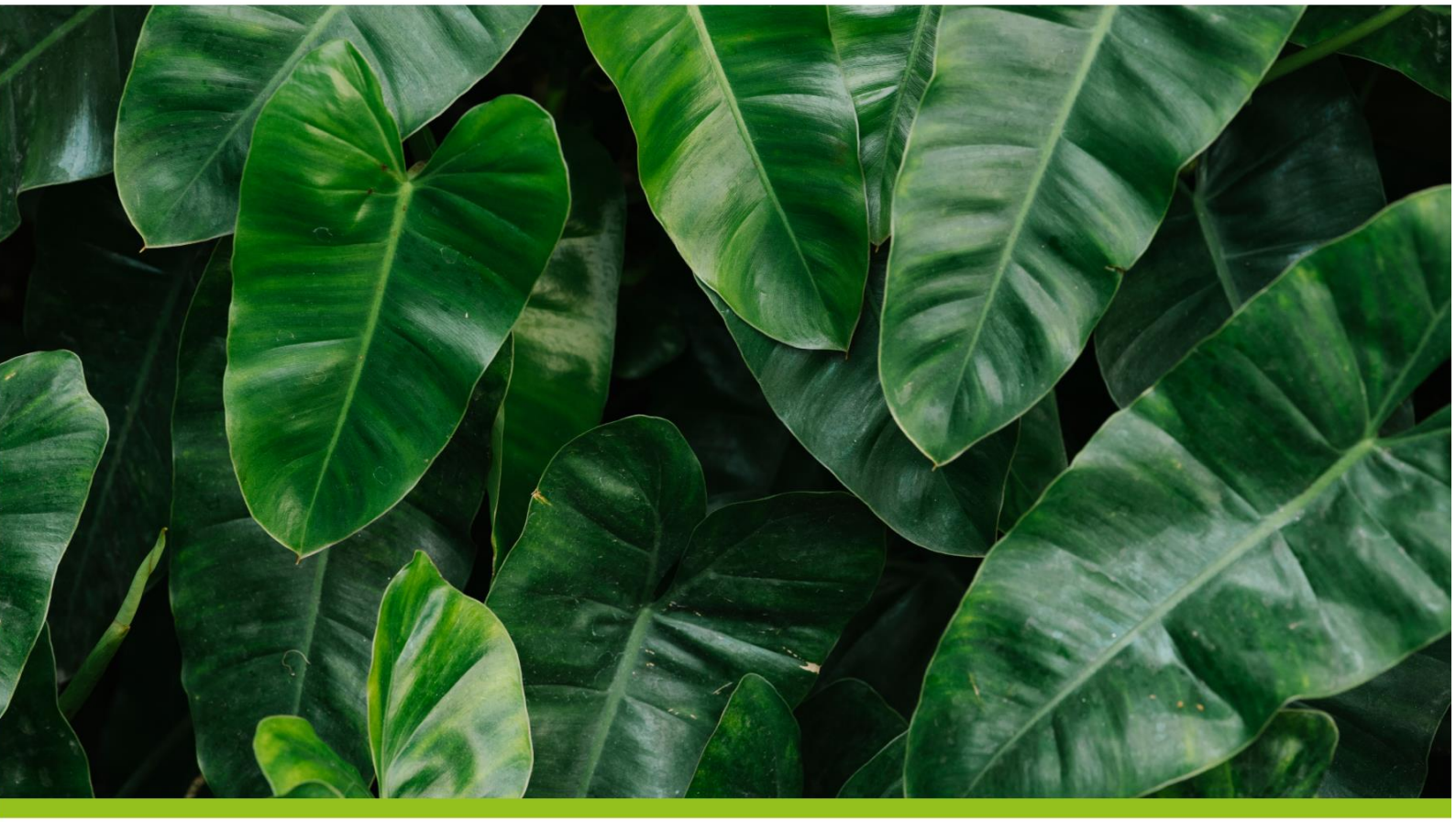
STRATIA CYBER
Security Consultancy



Service Descriptions G-Cloud 14

StratiaCyber.com

1 CONTENTS

1 Information Risk Advisor, Architecture and Assurance Services 3

2 Security Standards Consultancy and Assessment Services 5

3 Security Assessment Services 8

4 Cyber Maturity Services 13

5 Virtual Chief Information Security Officer (vCISO) Service 16

6 Cyber Readiness and Response Service 19

7 Mapping of G-Cloud Services to Stratia Cyber Service Towers 23

www.stratiacyber.com

Telephone 0800 644 0193

Email cyber@stratiacyber.com

1 INFORMATION RISK ADVISOR, ARCHITECTURE AND ASSURANCE SERVICES

1.1 OVERVIEW

Stratia Cyber provides a focal point for resolution of security and information risk matters. This includes:

- Analysis and evaluation information risks by determining the threat sources and potential attach methods attackers may pursue
- Identification of risk through risk assessment using a standards-based methodology
- Reviewing the end-to-end business process to determine if there are any exploitable vulnerabilities
- Explanation of the causes of risk
- Establishing motivation and likelihood and potential impacts of information risks
- Assistance with compliance with applicable regulations, standards and policies.

For the on-going management of risk within an organisation, Stratia Cyber offer the following Assurance services:

- Ongoing management of security in an Organisation:
    - presenting options for treating risk
    - which risks can be transferred?
    - impact of accepting risk
- Investigating security incidents
- Options for operational security
- Promoting security awareness

1.2 SERVICE FEATURES

1.3 STRATEGIC APPROACH

Stratia Cyber helps Organisations to determine their cyber strategy and put a road map in place that will enable them to achieve their security objectives.

The first step is to help determine:

- An Organisation's threat profile
- Establish the value of its information assets and business processes, without which the organisation would simply not be able to function!

Once these have been established the next step is to carry out risk assessment, which is usually completed in two parts:

- A holistic view of the Organisation is taken to derive the generic risks to the business.
- Following on, a review of business process is carried out to determine risk. This looks at specific business processes to determine if there are any vulnerabilities that expose the business assets.

These are combined to provide a view of the Organisation's threats and prioritised risk profile before moving to the next stage of mitigating risks. This can help determine and improve the Organisation's Cyber Maturity, see Stratia Cyber's ***Cyber Maturity Assessment Service***.

1.4 Risk Treatment and Mitigation

It is important for any Organisation to understand the nature of risks as well as its tolerance to such risk and levels it can accept. These will be defined in plain English so the Board can have a full understanding of any risk and how to treat it, together with the consequences of accepting risk - a key component of setting the Organisation's risk tolerance.

First, an analysis of the risks is carried out and risks are prioritised in the following way:

- Risks are categorised in terms of severity and damage to the Organisation.
- Then they are evaluated to determine how easy it would be mitigating the risk

Once this has been established, a Mitigation Plan is put in place to address the high priority risks to the Organisation and easy things to do (quick wins), so that the Organisation can see some immediate benefits.

At this point security goals along with a security governance structure will be established for the Organisation and a road map will be developed to address the Organisation's prioritised risks. These will be captured in a Risk Register and reviewed regularly by the Board, which in time will demonstrate how the organisation is improving its cyber security (maturity) profile.

1.5 Ongoing Assurance

Stratia Cyber's Risk and Assurance consultants can provide:

- Support to the ongoing assurance of an organisations IT and applications that process that sensitive business information:
    - into service
    - and through life
- Specialist input to the Organisations CISO and SIRO
- Detailed scope for any penetration testing
- Advice on the remedial action plan

1.6 Outputs

Stratia Cyber will provide the following documentation to support the Organisation's risk profile as defined above:

- Security Strategy and Road Map
- Threat assessment
- Information Asset register and advice on asset classification including HMG and private sector.
- 360-degree assessment of Holistic and Business Risk, including risk tolerance and acceptance statement for the Organisation
- Assurance documentation including;
    - Risk Register
    - Risk mitigation plans.

    - Assurance testing scope and plan
    - Assurance Authority to Operate
- HMG legacy standards RMADS including IS1/2
- Penetration plan document
- Mitigation plan
- Further security support and advice in line with Organisational objectives can be provided.

1.7 SERVICE BENEFITS

The benefits to the Organisation are as follows:

- **Qualified consultants**. CCP qualified consultants lead by Lead CCP and NCSC CCSC Head consultants.
- **Understanding of risks**. Ensures risks are adequately recognised and understood.
- **Cost effective mitigations**. Ensures mitigations are proportionate and cost effective.
- **Documentation.** Produces documentation optimised for both business effectiveness and Accreditation.
- **Scalability**. Resources can be scaled up or down to any requirement.
- **Comprehensive approac**h. This service complements and supports Stratia Cyber's ***vCISO*** and ***Cyber Maturity Assessment Services***

2 SECURITY STANDARDS CONSULTANCY AND ASSESSMENT SERVICES

2.1 OVERVIEW

The two structural security standards that this consultancy service is concentrated on is the Internationally recognised ISO 27001 and the NHS Data Security and Protection Toolkit (DSPT). Both the ISO 27001 and DPST requirements are universal and are intended to be applicable to all organisations, regardless of type, size or nature.

ISO 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks that helps organisations keep information assets secure and manged within the organisation.

The NHS DPST is a self-assessment to the 10 National Data Guardian's (NDG) Data Security Standards. The DPST assessment provides assurance that all organisations that have access to NHS patient data and systems are practising good data security, and that personal information is handled correctly. A categorisation of requirements has been specified into four categories at different detail levels to deliver the assessment and support the varying types of organisations within the health sector.

Stratia Cyber certified and experienced consultants can provide a pragmatic approach in assisting your organisation to become ISO 27001 certified and/or compliant to the NHS DSPT self-assessment These distinguishable consultancy elements are listed below:

- Analysis
- Implementation
- Risk Management
- Integration

Further details of the activities involved in each of the elements are listed below:

2.2 AUDIT AND ANALYSIS

- ISO 27001 Annex A Control Objectives gap analysis

There is a total of 114 controls within 14 groups or security domains in Annex-A of the ISO 27001 standard. The Statement of Applicability (SOA) is a fundamental part of an ISMS and forms a security footprint of all an organisation applied controls to the ISO 27001 standard. A gap analysis provides a detailed plan to an organisation on compliance or gaps within the security footprint utilised to deliver a SOA.

- NHS DSPT gap analysis

A gap analysis provides a detailed plan on compliance or gaps within the security footprint of the organisation to the NDG 10 security standards. It can also provide a mapping to existing controls when an organisation has implemented another security framework or management system.

- ISMS gap analysis (Pre-Certification)

An ISMS is the implemented management system consisting of processes, procedures and policies that structures the control to protect and manage an organisations information asset. An ISMS gap analysis delivers a review of the current specific company operations, policies and processes or procedures and establishes a detailed implementation plan and recommends actions to satisfy the requirements of the ISO 27001 framework to form an ISMS for successful company certification to the international standard.

- Post management gap analysis (Post-Certification)

A post management gap analysis provides deliverables to a client of a continual improvement plan to maintain an implemented and improve maturity.

- Security Mapping (Control objectives)

Security mapping provides a deliverable of mapping implemented ISMS control objectives to other information security frameworks and standards in relative controls.

- ISO27001 Lead Auditor and Pre-Audit preparation.

Our Lead Auditors will guide you through the process to ensure that the appropriate controls are in place to enable the Organisation to achieve ISO27001 accreditation.

2.3 IMPLEMENTATION

- ISMS implementation

An ISMS implementation deliverables include modification and creation of policies, procedures, clause practices and best practice advice required to implement a comprehensive ISMS to meet all requirements of the clauses and control objectives of the ISO 27001 standard.

- Policy and procedure implementation

Implementation of policy and procedures deliverables include modification and creation of policies, procedures required to meet clauses and control objectives of the ISO 27001 standard.

- Certification Stage 1 & 2 audit assistance

The Stage 1 audit by a Certification Body will review the ISMS to establish whether it complies to the requirements of ISO 27001. The Stage 2 audit is performed to conduct a thorough on-site assessment to determine if an ISMS complies with ISO 27001 standard and should be recommended to the Accreditation Body for certification. This element offers onsite and remote assistance to understand recommendations from the stage 1 audit and leading guidance with the stage 2 audit.

- ISMS Virtual Management

ISMS virtual management delivers managing the implemented ISMS repeated processes such as internal audits, risk assessments and continual improvement of Non-conformance and corrective actions to an organisation on the life cycle of the applied ISMS, usually part time or remotely.

2.4 Risk Management

- ISO 27001 Risk Management implementation

Implementation of risk management delivering policy and procedure utilising Qualitative methodology that complies with best practice, such as the International Standards for Risk Management Principles ISO 3100, Risk Management – Assessment techniques ISO 31010 and Information Security Risk Management ISO 27005.

- ISO 27001 Risk Assessments

Deliverables of risk assessments to identify risks and treatments associated with the loss of confidentiality, integrity and availability for information assets within ISMS scope utilising Qualitative methodology that complies with best practice, such as the International Standards for Risk Management Principles ISO 3100, Risk Management – Assessment techniques ISO 31010 and Information Security Risk Management ISO 27005.

2.5 Integration

- Integration element deliverable to form an Integrated Management System (IMS) that encompasses the ISO 27001 ISMS and ISO 9001 clause and procedures that are related within both standard frameworks.

2.6 Service Benefits

The benefits to your Organisation are as follows:

- CCP qualified consultants lead by Lead CCP and NCSC CCSC Head consultants,
- ISO 27001 Certified Lead and Senior Lead Implementer consultants,
- Experienced Information Assurance Consultants,
- Ensures Information Security risks are adequately recognised and understood,
- Ensures risk mitigations or treatments are proportionate and cost effective,
- Ensure an ISMS is standard compliant,
- Ensure an organisation has good structure for certification assessments,
- Produces documentation optimised for both business assurance and certification,
- Improves Information Assurance for clients,

3 SECURITY ASSESSMENT SERVICES

3.1 OVERVIEW

Stratia Cyber is a CREST member company and is CREST approved for Penetration Testing and achieved certification to the ISO 27001:2013, ISO 9001:2015 standards and Cyber Essentials Plus for licensing as an IASME Consortium Certification body.

Our assessment and analysis methodology and processes have been designed and established through extensive experience of security testing and assessing this domain over several years delivering or supporting technical security assessments for government, defence and industry domains. Our security assessment service is founded on the following principles:

- To provide our services founded on a solid reputation and proven experience;
- To always operate within a legal and ethical manner;
- To provide high quality, value-for-money assessment services;
- Use empirical evidence, research and capability development;
- To only use highly proficient, competent, technically astute testers;
- Incorporate security and use risk management where relevant; and
- To develop and maintain a strong professional accreditation and complaint process.

Stratia Cyber provides experienced and qualified Security Assessors and Penetration Testers who have extensive experience of managing and delivering the complete security assessment process.

Additionally, we can provide assessments for:

- Infrastructure vulnerability and penetration testing
- Web applications vulnerability and penetration testing inc. OWASP domains.
- Mobile device and applications penetration testing

- ICS and SCADA systems assessments
- Physical assessments
- Cyber incident analysis
- Technical analysis of systems
- Active Threat Inference and Threat Intelligence
- RF and Wireless based testing
- Red Team and enterprise-wide assessments
- NCSC Cyber Essential scheme standard and audited assessments.

3.2 SERVICE FEATURES

3.2.1 Our Approach

Our assessment service activities follow and implement a repeatable and documented assessment methodology that aligns with industry best practice, and which evolves on the basis of continuous improvement through ensuring that lessons learnt during the process are captured and used to enhance or correct the service and/or the deliverables as we develop our offerings.

This provides consistency and structure to assessments, expedites the transition of new assessment staff and addresses resource constraints associated with assessments.

Using this methodology also enables us to maximize the value of assessments for clients while minimizing risks introduced by certain technical assessment techniques.

All assessment and testing conducted by Stratia Consulting shall always be within the bounds and adherent to the Computer Misuse Act, the Regulatory Investigative Powers Act, the Wireless Telegraphy Act and other such acts of law which are relevant (this list is subject to change).

Relevant UK law related to personal privacy includes the Data Protection Act and the Human Rights Act article 8, specifically "*The right to respect for private and family life"* and actions required to prevent a breach of either of the acts shall be considered and include on a per-test basis.

The implications of computer crime are varied and far reaching. Computer crime is a relatively new, but exponentially increasing, problem across the globe and in our society; it is therefore vital that companies that offer security assessment services understand and work within frameworks that comprehend computer crime, such as those crimes conducted with the help of a computer, a network, or even a small computing device like mobile phone, and the part that the Internet plays due to its ubiquitous availability and ease of access.

3.2.2 Assessment Services

Security assessments and penetration testing are always tailored dependant to the requirements of the client, and offered using a blend of appropriate approaches, tools and techniques, each bespoke for the test at hand and each constructed and planned to assess the defences and configuration of differing assets, for example:

- Technical assessments; manual and automated vulnerability and penetration testing;
- Remote Vulnerability and Pen Testing Services;
- Business Processes Evaluation;
- Physical testing; buildings, boundaries;
- Personnel testing aka “Social Engineering”; and/or
- A combination of any or all the above.

Each aspect can be further evaluated, for example technical assessments may be targeted at all or part of an organisation’s IT estate and related assets, for example:

- External and boundary systems;
- Internal networks, systems and associated “infrastructure”;
- Applications including web applications;
- User systems, workstations and user access devices (UADs);
- RF and Wireless based systems;
- Telephony systems including VoIP and Public Switched Telephone Networks (PSTN);
- Mobile devices; and/or
- A combination of any or all the above.

The key to successful outcomes is rigorous testing and reporting key findings and mitigation recommendations; and security testing is conducted only when appropriate authorisations and legal aspects have been considered and addressed. Therefore, value for the client is realised and the optimum approach and expected outcome is agreed.

A Cyber Essential (CE) scheme assessment is compliant to the cyber control framework defined by the National Cyber Security Centre (NCSC) scheme standard and IASME certification body requirements. The self-assessment and independent audit checks and tests an organisations defences to ensure they reach with full compliance the CE Standard. The CE scheme focusses on five key areas to ensure adequate defences are in place. These are: Boundary Firewall and Gateways, Secure Configuration, User Access Control, Malware protection and Patching. An audited assessment is performed on a representative sample of the infrastructure for common vulnerabilities across the above five areas.

3.2.3 Outputs

Stratia Cyber shall provide contextual reporting which is critical to ensuring the vulnerabilities and findings are fully explained and assist remediation. Findings shall always be considered within the context of the organisation; context can significantly change the risk scoring.

To prioritize remediation of the penetration test findings, it is a common practice during the reporting phase for a severity or risk ranking to be assigned for each detected security issue. The written report shall clearly document how the severity/risk ranking is derived.

The Common Vulnerability Scoring System (CVSS) is an example of an open framework that may be referenced for assigning a baseline risk rating. In most cases, severity or risk ranking may be applied because of evaluating an industry-standard score (e.g. CVSS) against a threshold or value that indicates risk (i.e. high, medium, and low). However, it should be noted that it is possible for a vulnerability to exist that is inherent to an environment; therefore, a standardized score is not available.

When custom scoring is part of the risk-ranking process, the report should reflect a traceable set of

reasoning for the modification of industry-standard scores or, where applicable, for the creation of a score for a vulnerability that does not have an industry-standard score defined.

We align and use well-known, industry-standard references, which include:

- National Vulnerability Database (NVD);
- Common Vulnerability Scoring System (CVSS);
- Common Vulnerabilities and Exposure (CVE);
- Common Weakness Enumeration (CWE);
- Bugtraq ID (BID); and
- Open-Source Vulnerability Database (OSVDB).

The CVSS is the required scoring system for our methodology to use for ranking vulnerabilities detected during vulnerability scans. Using this system, a standardized vulnerability score can be adjusted through the evaluation of the traits of vulnerability within the context of a specific environment.

The report shall contain both the inherent 'base' CVSS score, for instance those generated by automated tools, and for critical findings or those with significance, the residual temporal and environmental scores from the CVSS shall be reviewed by the Task Lead so that the Client can make informed decisions about how the vulnerability remediation will best be prioritised and managed.

Additionally, analysing and verifying raw data to ensure that the test has been thorough and comprehensive shall be performed; depending upon the environment and findings, Task Leads may conduct additional manual tests.

Final analysis, such as the development of overall conclusions, usually takes place after all testing activities have been completed and involves the development of mitigation recommendations. While identifying and categorizing vulnerabilities is important, a security test is much more valuable if it also results in a mitigation strategy being developed and implemented. Mitigation recommendations, including the outcome of the root cause analysis and may be developed for each finding. There may be both technical recommendations (e.g. applying a particular patch) and nontechnical recommendations that address the organization's processes (e.g. updating the patch management process).

The testing phase concludes with a final review of the testing activities (aka “wash-up” meeting) and occurs as soon as possible/immediately following the end of the test, often at the end of the final day, and is the first formal opportunity to report initial findings to the customer.

The final review meeting shall include identifying the anomalies identified during testing such that all stakeholders understanding the findings and the relevance and a summary overview of the findings from the most severe to lower ratings. Lower rating shall not be dismissed as unimportant as a combination of low ratings may be exploited together to produce a combined higher rating. The final on-site Client meeting shall also cover whether the scope has been fully delivered. In the event the scope has not been fully met, agreement on further outcomes shall be discussed and agreed with the Client.

Prior to finalisation of all reporting artefacts and documentation, our written reports shall be:

- Peer-reviewed by Task members;
- Authorised and approved for release by the Head of Assessment Service;
- Only disseminated to relevant stakeholders;
- Disseminated only via secure means, usually using encrypted files;
- Supported by debriefing sessions; and
- Acted upon where agreed with the Client.
- CE reports conform to the CE scheme standard and certification body requirements.

Our reports shall contain:

- Key dates; dates of testing, dates of reporting, dates of report distribution;
- The names, roles and qualifications of the test team;
- The type of tests performed;
- Highlight any issues affecting the validity of testing or the results; and
- Any other unknown or anomalies encountered during testing.

3.3 SERVICE BENEFITS

Research in the field of security assessments has demonstrated that there are significant benefits to an organisation through effective security assessments and penetration testing, which can include:

- A reduction in ICT costs over the long term;
- Improvements in the technical environment e.g. reducing support calls;
- Greater levels of confidence in the security of your IT environments;
- No need to be onsite for certain services;
- Increased awareness of the need for appropriate technical controls;
- Preparedness for when a breach occurs;

- Competitive advantage;
- International standards and compliance; and
- Consistency in approach

A CE assessment is designed to reduce the risks from phishing and other low level hacking attacks, by implementing a set of sensible and pragmatic security measures that can be put in place by any size organisation. Benefits can include:

- Government and Public sector buyers increasingly require their suppliers to have achieved the Cyber Essentials certification.
- Shows an organisation takes cyber security seriously.
- and that they have taken sensible security measures to protect from the most common threats
- Independently verified self-assessment.
- A technical audit of your systems.
- Cyber Essentials certification includes automatic cyber liability insurance.

4 CYBER MATURITY SERVICES

4.1 OVERVIEW

Stratia Cyber provides experienced and qualified Security Consultants and Architects with extensive experience implementing good cyber practice and infrastructure design. We provide a review of an Organisation's cyber profile or an Organisation's Third-Party or Supply Chain suppliers with two levels of assessment:

- Cyber Maturity Evaluation:
    - Assessment of the Organisation's Cyber awareness to threats and risk.
    - Assessment against good practices, staff skills and infrastructure
    - An assessment is made against a standard set of cyber capability to assess maturity rating the Organisation from non-existent, through intuitive, to optimised, and
    - A strategy and plan will be established with the Organisation to enable them to improve their cyber maturity level.
- Cyber Gap Analysis Review:
    - Organisation's Cyber awareness of threats, risks and important business assets
    - How the Organisation's organisational responsibilities address security governance.
    - Review technology and controls protecting the Organisation's assets.
    - A recommendations report will be provided detailing the next steps the Organisation should take.

4.2 SERVICE FEATURES

4.2.1 Maturity Assessment

The scope of a Maturity assessment is to determine the existing level of cyber maturity for an organisation when measured against a set of standard controls and industry good practice, this is done for an Organisation's staff, processes and technology.

The outcome will determine what level of maturity is required and achievable for the Organisation and what steps it needs to go through to get there.

4.2.2 Organisational Culture

To determine the general awareness and understanding of cyber security in an Organisation the following steps are carried out:

- Ascertain the extent to which the Organisation fully understands the value of its:
    - Asset, and
    - Business processes
- Threat awareness:
    - Does the organisation understand its threats?
    - Does the organisation understand how threats will manifest themselves?
- Risk awareness, does the Organisation:
    - Have a method to assess risk?
    - Understand what level of risk it can tolerance, and
    - Understand the consequences of accepting risks when considering impact to the Organisation against cost, and resource required to mitigate these risks.

This step is key to the Organisation understanding the value of its key business assets and processes without which it could cease to operate.

4.2.3 Cyber Control groups

The following groups are used as a framework to establish a measurable standard set of controls, as part of this exercise the applicability of control groups will be reviewed as not all will suit all organisations:

- Access control – who can access and what they are authorised to see within job role.
- Crypto and key management – secure comms and data at rest
- Security Information and Event Management – Situational Awareness
- Business resilience – DR and BC
- Network and trust management – Boundaries, gateways and remote access.

- Threat and Vulnerability Management – TVM

4.2.4 Metrics

As a means of capturing and measuring an organisation's maturity level, staff will be interviewed to establish maturity against the following areas of operation in the above control groups:

- Staff – Suitability Qualified and Experienced Professional
- ICT – Tools and technologies
- BAU – Operational readiness level
- Documentation – Processes and procedures
- Policy and standards, and
- Governance and Assurance

This uses a spectrum of criteria to determine the maturity level ranging from non-existent, ad-hoc, repeatable but intuitive, through to defined, managed, measurable and optimised.

4.2.5 Reports

The final report will determine the following:

- Maturity level for each control group;
- Overall maturity;
- Determines the maturity level where the organisation needs to be; and
- A six, twelve, eighteen-month plan to determine how to get there.

4.3 GAP ANALYSIS

Stratia can help Organisations to take the first step by performing a high-level review of their cyber security profile. This can be regarded as a pre-qualifying step to performing a Cyber Maturity assessment.

In its simplest terms the review will carry out the following:

- Review assets and key business processes.
- Understanding of threat, risk and governance
- Review of policy
- Review the organisation's ICT infrastructure.

This is intended to highlight, via a report, major identified gaps in an Organisation and recommendations to mitigate these.

4.3.1 Service benefits

The benefits to the Organisation are as follows:

- **Accredited Consultants**. CCP qualified consultants led by Lead CCP and NCSC CCSC Head consultants.

- **Assurance of advice**. Lead architect level of advice on corporate infrastructure.
- **Value for Money.** A proportionate and cost-effective approach
- **Relevant Experience**. Ability to leverage on experience having dealt with other similar Organisations.
- **Standards Based.** Consistency through a Standards-based approach.

5 VIRTUAL CHIEF INFORMATION SECURITY OFFICER (VCISO) SERVICE

5.1 OVERVIEW

Stratia Cyber provides experienced and qualified virtual Chief Information Security Officers (vCISO). This includes:

- Board level current and qualified cyber security expertise.
- Cyber strategy creation and delivery
- Analysis and evaluation of current organisation to identify information and business risks.
- Identification of risk through risk assessment using a standards-based methodology
- Reviewing the end-to-end business process to determine if there are any exploitable vulnerabilities.
- Managing security incidents
- Promoting security awareness
- Ensuring organisations remain compliant with applicable regulations, standards and policies.

5.2 SERVICE FEATURES

5.2.1 Strategic Approach

The vCISO service is a cost-effective method for Organisations to determine their cyber strategy and put a road map in place that will enable them to achieve their security objectives.

The first steps are to understand the Organisation to determine:

- A vision for the Information Security Programme
- The Organisation's threat profile
- The value of its information assets and business processes, without which the organisation would simply not be able to function.

Once these have been established the next step is to carry out risk assessment, which is usually completed in two parts:

- A holistic view of the Organisation is taken to derive the generic risks to the business.

- Following on, a review of business process is carried out to determine risk. This looks at specific business processes to determine if there are any vulnerabilities that expose the business assets.

These are combined to provide a view of the Organisation's threats and prioritised risk profile before moving to the next stage of developing an Information Security Programme. This can help determine and improve the Organisation's Cyber Maturity, see Stratia Cyber's ***Cyber Maturity Assessment Service***.

5.3 INFORMATION SECURITY PROGRAMME

This programme will be pivotal to driving good information security practice in the organisation. It will be defined in plain English so the Board can have a full understanding of any action and how to treat it, together with the consequences of accepting risk - a key component of setting the Organisation's risk tolerance.

First, an analysis of the risks is carried out and risks are prioritised in the following way:

- Risks are categorised in terms of severity and damage to the Organisation.
- Then they are evaluated to determine how easy it would be mitigating the risk

Once this has been established, an Information Security Programme is put in place to address the high priority risks to the Organisation and easy things to do (quick wins), so that the Organisation can see some immediate benefits.

This programme will include:

- Communications plan
- Internal Risk programme
- Third Party Risk programme

At this point security goals along with a security governance structure will be established for the Organisation and a road map will be developed to address the Organisation's prioritised risks. These will be captured in a Risk Register and reviewed regularly by the Board, which in time will demonstrate how the organisation is improving its cyber security (maturity) profile.

5.3.1 Ongoing Assurance

Stratia Cyber's vCISO consultants can provide:

- Support to the ongoing assurance of an organisations IT and applications that process sensitive business information:
    - into service
    - and through life
- Specialist input to the Organisations Board and SIRO
- Detailed scope for any penetration testing

- Advice on the remedial action plan

5.3.2 Outputs

Stratia Cyber may provide the following documents and activities as part of the vCISO service to support the Organisation:

- Information Security Strategy and Road Map
- Board Meeting attendance.
- Threat assessment
- Information Asset register and advice on asset classification including HMG and private sector.
- 360-degree assessment of Holistic and Business Risk, including risk tolerance and acceptance statement for the Organisation
- HMG legacy standards RMADS advice including IS1/2
- Penetration plan document
- Mitigation plan

5.3.3 Service benefits

The benefits to the Organisation are as follows:

- **Qualified consultants**. CCP qualified consultants lead by Lead CCP and NCSC CCSC Head consultants
- **Clear concise advice**. Delivery of complex cyber security issues in clear concise non-technical language
- **Understanding of risks**. Ensures risks are adequately recognised and understood
- **Cost effective**. Access to assured security advice without the need to build an expensive in-house team.
- **Documentation.** Produces documentation optimised for both business effectiveness and Accreditation
- **Scalability**. Service can be scaled up or down to any requirement
- **Comprehensive approach**. This service complements and supports Stratia Cyber's ***Information Risk Management*** and ***Cyber Maturity Assessment Services***

6 CYBER SECURITY INCIDENT RESPONSE

6.1 OVERVIEW

Our Cyber Readiness and Response service and process has been designed and established through many years' experience of delivering and supporting technical and cyber security response for government, defence and industry in general.

Our cyber response service is founded on the following principles:

- To provide our services founded on a solid reputation and proven experience;
- To always operate within a legal and ethical manner;
- To operate a timely and coordinated approach in-line with client requirements;
- To provide high quality, value-for-money readiness and response services;
- Use empirical evidence, and active threat inference as required;
- To only use highly proficient, competent, technically astute staff or associates;
- Incorporate security and use risk management where relevant; and
- To develop and maintain professional accreditation and complaint processes.

Stratia Cyber provides experienced and qualified staff who have extensive experience of managing and delivering the complete cyber readiness and response process.

7 CYBER READINESS AND RESPONSE SERVICE

7.1 SERVICE FEATURES

7.1.1 Our Approach

Our Cyber Readiness and Response service activities follow and implement a repeatable and documented methodology that aligns with industry best practice, and which evolves through continuous improvement by ensuring that lessons learnt during the process are captured and used to enhance or correct the service and/or the deliverables.

This provides consistency and structure to this service and enables us to maximize its value to clients whilst minimizing risks inherent in employing certain technical techniques.

All activities conducted by Stratia Cyber will always be legal. Relevant UK law related to personal privacy includes the Data Protection Act 2018 and the Human Rights Act article 8, specifically "*The right to respect for private and family life"* and actions required to prevent a breach of either of the acts shall be considered and included on a per-test basis.

Cyber criminals are exploiting the latest technology to further their needs. Cyber readiness and response activities should be continually adapted to counter this kind of activity.

The implications of computer crime are varied and far reaching. Whilst computer crime is a new problem across the globe and in our society, it is exponentially increasing. It is therefore vital that companies comprehend and respond to computer crime, such as those crimes conducted using a computer, a network, or even a small computing device like mobile phone, and the part that the Internet plays due to its ubiquitous availability and ease of access.

7.2 Cyber Readiness and Response Services

Our cyber readiness and response services align with the NIST Cyber Security Framework for each of the Identify, Protect, detect, Respond and Recover segments and follow the industry widely used 6-step process to cyber readiness and response.

Preparation

The Preparation Phase is about ensuring the appropriate Policies, Processes, Plans (including staff identification, call trees, appropriate documents exist, and these are effectively disseminated) are in place and that your organisation has identified the members of your Incident Response Team including external entities.

Identification and Analysis

During the Identification and Analysis Phase we will work with you to clarify if your organisation is dealing with a discrete incident or one that is part of a wider threat. This is where fully understanding your organisation's infrastructure and operations is critical to identifying significant deviations from normal traffic baselines and suspected malicious activity. Various methodologies can be applied, for example, Open-Source Intelligence (OSINT) to identify Indicators of Compromise (IOC), configuration assessments, onsite or remote network data streams capture, mobile device forensics and wireless client assessments. These types of identification methodology lead to deep analysis and threat hunting to establish any threats of malicious activity present.

Containment

During Containment, we will work with you to limit the damage caused to business activity and systems and to minimise or prevent any further damage from occurring. If required, we will collect all the necessary information as evidence.

Eradication

During the Eradication Phase the emphasis is on ensuring your organisation has a "clean" infrastructure and associated systems. This may be a complete reimage of a system, or a restore from a known good backup, and include application of patches and fixes to vulnerabilities, correction of any improper configuration in the systems and networks, removal of malicious code or a computer virus from all infected systems, stop or kill all active processes of a threat actor to terminate the threat, apply access controls and change passwords.

Recovery

During the Recovery Phase, the analysis and prior activities will help to determine when to bring the systems back into production; and whether to or how long to monitor the system for any new or remnant signs of abnormal activity. Examples of tasks can include performing a damage assessment, ensuring that the compromised system and its related components are secured, and ensure the systems meets company standards or baselines. Before returning it to service we would bring up function/service by stages in a controlled manner and verify that the restoring operation was successful. All related parties would receive prior notification on resumption of system operation e.g. operators, administrators, senior management, and other parties involved and keep a record of all actions performed.

Lessons Learned

As the business moves back into normal operations it is most important to review and assess any lessons learned. This will allow your organisation to consider which activities and knowledge to improve your business processes. This could include additional technical defences or otherwise preparedness for future events, improving security measures to protect the system against future attacks, prosecution of those who have breached the law, education for parties involved about the experience learnt, producing a learning knowledge base from past incidents to allow referral in the future to reduce the likelihood, and enacting continual improvement to an implemented ISMS – Preventive & Corrective management.

7.3 OUTPUTS

Stratia Cyber will provide contextual reporting which is critical to ensuring all findings are fully explained and fully assist respond-recover remediation objectives. Findings shall always be considered within the context of the organisation as each operating context can differ from one organisation to another and potentially significantly change risk scorings.

Final analysis, such as the development of overall conclusions, usually takes place after all response activities have been completed and involves the development of mitigation recommendations. While identifying and categorizing findings is important, these activities are much more valuable if they also result in a mitigation strategy being developed, and subsequently implemented. Mitigation recommendations, including the outcome of the root cause analysis, may be developed for each finding. There may be both technical recommendations and nontechnical recommendations that address the organisation's processes (e.g. updating the patch management process).

The final review will include identification of the anomalies found during our response, written in a way that all stakeholders can understand the findings and their relevance, and a summary overview of the findings rated from the most severe downwards.

Prior to finalisation of all reporting artefacts and documentation, our written reports shall be:

- Peer-reviewed by Response Task members;

- Authorised and approved for release by the Head of Service;
- Only disseminated to relevant stakeholders;
- Disseminated only via secure means, usually using encrypted files;
- Supported by debriefing sessions; and
- Acted upon where agreed with the Client.

Our reports shall contain:

- Key dates: dates of activities, dates of reporting, dates of report distribution;
- The names, roles and qualifications of the cyber response team;
- The type of activities performed;
- Highlight of any issues affecting the validity of findings or the results; and
- Any other unknown or anomalies encountered during our activities.

7.4 SERVICE BENEFITS

Research in the field of security assessments has demonstrated that there are significant benefits to an organisation through effective security assessments and penetration testing, which can include:

- **Cost reduction**. A reduction in ICT costs over the long term;
- **Technical improvements**. Improvements in the technical environment e.g. reducing support calls;
- **Improved security**. Greater levels of confidence in the security of your IT environments;
- **Increased awareness**. Increased awareness of the need for appropriate technical controls;
- **Better preparedness**. Preparedness for when a breach occurs;
- **Advantage**. Competitive advantage;
- **Compliance**. International standards and compliance; and
- **Consistency**. Consistency in approach

8 MAPPING OF G-CLOUD SERVICES TO STRATIA CYBER SERVICE TOWERS

	Risk Advisor, Architecture and Assurance Services	Standards Consultancy and Assessment Services	Security Assessment Services	Cyber Maturity Services	Virtual Chief Information Security Officer
Cloud Security Architecture	X				
Cloud Security Risk Management	X				
CREST Penetration Testing			X		
Cyber Essentials			X		
Cyber Essentials Plus			X		
Cyber Security Consultancy	X	X	X	X	X
ISO27001 Consultancy		X			
IT Health Check		X	X		
NCSC Certified Risk Management Service	X				
NHS DSPT Consultancy		X	X		
NHS DSPT Internal Audit		X			
PSN Code of Connection (CoCo) Check		X	X	X	
PSN Compliance		X		X	
Security Analyst as a Service	X				
Security Architecture	X				

Security Auditing				X	
Supplier Assurance				X	
Third Party Assurance				X	
Virtual Information Security Officer			X		X
Vulnerability Scanning			X