SECURITY FRAMEWORKS & CONTROLS ASSESSMENT

KEY SERVICE COMPONENTS

Service Methodology

The security review will be performed through a combination of onsite interviews and assessments of existing policies, procedures and technologies deployed. This is not an evidence based assessment, it is based on the results of the conversations.

Service Scope

The scope of the engagement can only be agreed after meeting with the customer, however the Cyber Essentials Standard provides a suggested scope that can be used initially for discussion purposes.

Service Delivery

SecureData utilises a proven 5-phase approach to produce the key deliverables, including: -

- Agree the Cyber Essentials scope and certification level to attain
  - o SecureData will employ a collaborative approach to concentrate on understanding the business requirements and mapping the systems (including cloud services), business areas and teams to be included.
- Cyber Essentials gap Analysis
  - o Using the Cyber Essentials standard and required questionnaire as a basis, the interview process should include high-level examination of documentation, and may include physical demonstrations of processes and procedures where appropriate.
- Cyber Essentials Report on Compliance, including:-
  - o Executive summary
  - o Description of Scope of Work and Approach Taken
  - o Main conclusions and Information Security maturity
  - o Detailedfindings
  - o Recommendations and suggested improvements
- Remediation plans
  - o SecureData will work with the customer to assist with the creation of remediation steps required for compliance which can be developed into project plans to implement.
- Certification
  - o SecureData will work with our preferred certification providers to complete the required Cyber Essentials security Questionnaire. We will liaise with the customer to clarify any queries to help progress the application to completion. Additional costs for Cyber Essentials certification are required for this phase.

SERVICE DESCRIPTION

There are many security frameworks to choose from. Some look at security from a business perspective using a risk based approach whilst others are designed to address specific issues or risks using a controls-based approach. Both groups deal with common security issues and challenges with common threats or security “domains” appearing in each.

Cyber Essentials (CE) Standard

Organisations can certify to the standard at two different levels, the lower level comprises a self-assessment questionnaire that is independently reviewed followed by an external network vulnerability scan to check the basic security of the perimeter. The next level is the same as the first but includes an onsite audit to scan a selection of internal devices for patch levels and settings.

It is a requirement for organisations that form part of the government supply chain to be certified to at least the lower level of the standard.

ISO27001

ISO27001 is a world-renowned, mature, risk-based security framework designed to cover all aspects of Information Security relating to its Confidentiality, Integrity and Availability (CIA) based around a comprehensive risk assessment of your business and its information assets. Security “controls” are selected from its sister standard ISO27002 or any other standard or framework, or controls of the organisation’s own design, to enable the reduction of risk to data to an acceptable level.

CESG 10 Steps Standard

This standard was the first offering from the Communications and Electronics Security Group (CESG), but proved too difficult for smaller companies to implement and so was replaced by the simplified Cyber Essentials. The 10 steps cover many of the security domains (or subjects) included in the more mature frameworks such as ISO27001. These additional domains include Risk Management and Incident Management.

KEY BENEFITS & DELIVERABLES

- **Draft report:** A draft report will be submitted within 21 days of the site visit which will be discussed with the organisation’s representative to make corrections and/or challenge any assumptions and opinions.
- **Final report:** Containing the assessment of findings against the CE standard control areas presented as both a radar diagram and detailed compliance matrix. The final report includes recommendations and suggested improvements that could be made to assist in achieving an optimally secure and compliant environment.

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com