

Cyber Defence Strategy and Capability Development

Purpose:

To help you to protect your valuable information against cyber threats.

Overview:

The National Cyber Security Centre has assessed cyber attacks and cyber crime as among the highest priority risks to national security, the economy and critical national infrastructure. Large public sector organisations are, complex, high risk enterprises which depend on information systems for most of their business activities. They have unique risks and vulnerabilities associated with an extensive and evolving array of inter-connected systems and services, including recent migration to cloud services.

This service provides those tasked with protecting their organisation's information assets with independent advice and technical support to analyse current cyber defence capability, identify gaps, develop a compelling and enduring case for investment and support the implementation of new cyber defence capability, enabling the mitigation of the potential political, economic and reputational impact of the continually evolving cyber threat. Improving cyber security awareness and cyber defence practice and capability is essential. We can help you to invest appropriately in cyber defence capability to protect your vital strategic, operational and tactical information and its secure and timely transfer and exploitation.

The appropriate outputs from this service will depend on your organisation's current capability, scope of services, threat profile and lead stakeholder motivation. We can apply our extensive experience to your business to develop cyber defence strategy, develop detailed requirements for appropriate cyber defence capability, develop options to meet these requirements and assess their costs and benefits, produce a compelling business case and assist its progress through the assurance, scrutiny and approvals processes.

Planning:

- Help your business to develop an effective cyber defence strategy
- Gap analysis against cyber defence best practice and legal requirements
- Develop detailed requirements for appropriate cyber defence capability
- Develop options, assess their costs and benefits and perform appraisals
- Develop and review business case
- Assessment against Cyber Essentials Plus, NIST, ATT&CK and advanced attacks
- Covers corporate, line-of-business and industrial control systems

Set-up and Migration:

- Develop and implement programme plans and roadmaps
- Transition planning and support to assist transition
- Ensure business case progress through assurance, scrutiny and review process
- Conduct benchmarking to identify potential areas for improvement
- Development, guidance and review of implementation plan

Ongoing Support:

- Support ongoing security assurance and protection of vital information assets
- Support to ensure long-term improvement of cloud cyber security awareness and cyber defence practice
- Partnership working and skills transfer to enhance your capability

Related Security Services:

- Security Strategy
- Security Risk Management
- Security Design
- Cyber Security Consultancy

- Security Audit Services

Enhancing your organisation's security posture or maintaining current levels of Information Assurance in terms of cloud-dependent services is usually a critical consideration when developing a Cyber Defence strategy and associated capabilities. Our related security services can provide specialist security related input to defining and managing these aspects.

Information Assurance:

We can provide relevant data protection and privacy advice for services of any classification. We employ security cleared personnel who operate with information at all levels of the Government Security Classification Policy (GSCP). Our systems are approved to hold classified information.

Pricing:

This service is priced based on anticipated resource requirement. Resources will be charged in accordance with the agreed SFIA day rates. Two pricing options are available:

- Firm price. The firm price will be based on the anticipated resource requirements including provision for risk. Provision for travel and subsistence cost will be made. Payment will be required against achievement of agreed milestones. Details will be specified in a price quotation provided and agreed before service commencement.
- Limit of liability. The limit of liability will be agreed based on an anticipated resource requirement. Charges will then be made monthly in arrears against resource effort expended. A limit of liability will also be agreed to cover travel and subsistence. Travel and subsistence costs will be charged at cost monthly in arrears against cost incurred.

Service management details and constraints:

Our service is subject to ISO9001 certified quality controls. A lead consultant shall be appointed who will have responsibility for liaising with the client and managing the Actica team providing the required services. In addition a Project Authority will be appointed who is normally a Director within the Company who will act as the point of escalation. We support our clients on-site, via email or by telephone, during standard office hours and with a 1 business day response time to acknowledge support requests.

Data backup and recovery:

Where our staff use infrastructure and information provided by our clients, it is the clients' policies and procedures that prevail. Ordinarily, our consultants are supported by our own infrastructure up to, and including OFFICIAL, and we have facilities for higher classification information to be received, stored and transmitted. Our consultants' laptops and our corporate systems are backed up regularly and our corporate Disaster Recovery Strategy and Plan ensures that we are able to continue to provide services to our clients in any event.

On-boarding/off-boarding:

For all of our assignments we operate our standard on-boarding/mobilisation activities. At assignment closure, we undertake a review and ensure that skills have been transferred to client staff where appropriate.

Ordering and invoicing process:

Specific details of the clients requirement should be sent to cloud@actica.co.uk. Following discussions about your requirement Actica will send a fully priced proposal detailing the services to be provided. Once approved a valid purchase order should be sent to finance@actica.co.uk for processing. Once the work is completed and accepted by the client Actica will invoice the client for the work. Payment is expected within 30 days. We are able to use a range of electronic purchase and payment systems (e.g. CP&F).

Consumer responsibilities:

The Consumer should appoint a single point of contact for reporting purposes.

Contact Details

Actica Consulting Limited
4 Stirling House
Stirling Road
Surrey Research Park
Guildford
Surrey, GU2 7RF

Telephone: 01483 484090
Email: info@actica.co.uk
Website: www.actica.co.uk

Registered Office in England as above
Company Number 03396854