

Cyber Assurance Exercise

Purpose:

To plan for and undertake Cyber Assurance Exercises (CAE) in line with NCSC guidelines and industry best practice on cloud-dependent systems, platforms or business operations in order to ensure appropriate crisis response and recovery planning and inform wider technology and business investments.

Overview:

Under our CAE service, Actica Consulting provides expert resources to plan for and carry out CAEs, providing an extremely thorough, high-assurance capability to respond to cyber incidents relating to systems, platforms and business operations. We ensure clarity of purpose, careful stakeholder management and rigorous analysis throughout.

We work closely with our clients to scope what sort of CAE is required, for example:

- A technology-led event using a technical red team attack method to test or validate processes and procedures in a real or 'near real' simulated environment;
- A socio-technical exercise to test or validate response procedures or policies in a real or 'near real' simulated environment;
- A 'Table top' exercise to test or validate response procedures, processes or policies away from the line of business;
- A 'Boardroom' executive awareness exercise.

We then design a tailored delivery approach, based on our proven, flexible exercising model, that will minimise disruption to 'business as usual' services, maximise the value of time committed by subject matter experts and ensure our clients emerge with a robust body of actionable recommendations to improve their cyber security posture.

Actica is an NCSC Assured Cyber Security Consultancy. Beyond our expertise in CAE methodology and practice, Actica can provide expert security advice on all aspects of information assurance and security, including the HMG Security Policy Framework (SPF), the Government Classification Scheme, the International Standard on Information Security Management (ISO27001), the Network and Information Systems (NIS) Regulations and associated Cyber Assessment Framework (CAF), the Data Protection Act, the Privacy and Electronic Communications Regulations (PECR) and the General Data Protection Regulation (GDPR). Our consultants include a number of UK Cyber Security Council Chartered Cyber Security Professionals (ChCSP), NCSC Certified Cyber Professional (CCP) and CISSP cyber security consultants and are fully conversant with the latest versions of all relevant standards, policy and guidance.

Planning:

- Source information gathering and assessment
- Stakeholder engagement and briefing
- CAE design and validation

Set-up and Migration:

- Scenario modelling
- Threat Assessment
- Exercise Facilitation

Security:

- Proportionate Assurance advisory support
- Socio-technical and physical security analysis and advice on countermeasures, security processes and procedure

Training:

- Formal skills transfer in CAE methodology and good practice

Quality Assurance and Performance Testing:

- Attack Path Analysis
- Table top Exercises
- Full Socio-Technical ('real world') exercises
- Online / Virtual exercises
- Red Teaming
- Buildings / Facilities Security Assessments
- Security Architecture assessments
- Culture and Human Factors assessments
- Risk quantification
- Risk mitigation strategy
- Support to ensure long-term improvement of cloud cyber security awareness and cyber defence practice
- Partnership working and skills transfer to enhance your capability

Information Assurance:

Cyber Defence is important for services of any classification and we have experience of supporting all customers from public-facing online services to sensitive cyber operations. 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. Customers may request clarification of the number of days by SFIA grade for their specific deliverables, which will be confirmed by Actica for contract award.
- 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:

We will expect you to liaise with the Actica lead consultant and ensure timely access to the information and key stakeholders necessary to deliver the service.

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