Incident Readiness Services

SERVICE DEFINITION FOR THE G-CLOUD 14 FRAMEWORK

Overview

Cyberis provide a range of services designed to enhance Incident Readiness. Details of a selection of these are provided below:

Incident Response Planning

Our incident readiness services include helping you put your incident response plan together and reviewing it with your teams to make sure it's fit for purpose.

Discovery Exercise

We'll conduct a discovery exercise with you that will inform the development of the plan:

- Understanding the structure of your business and your key teams – identifying all decision makers, key stakeholders, and contacts.
- Identifying compliance requirements – legal, regulatory, and contractual obligations associated with cyber security incidents.
- Identifying interested parties – customers, suppliers, third parties, cyber security / business interruption insurers, legal advisers, CIRT providers, forensics, and data recovery specialists.
- Understanding IT systems across the organisation.
- Identifying key IT and business processes.

Incident Response Plan Development

Using the information gathered, we will develop a tailored cyber security incident response plan using our experience in incident response management and analysis, as well as proven industry guidance and frameworks provided by CREST, the NCSC and NIST. We will work with key stakeholders to ensure the content of the plan is practical, and works within the framework of your business operations.

We'll prepare a comprehensive and clear incident response plan to guide your stakeholders throughout an incident. This is tailored to your business and your threats, so you know the plan can be effectively applied.

Incident Response Playbook Development

With the structure and content of the plan established, we can discuss and determine the key threats and the most likely incident response scenarios the organisation could encounter, with key stakeholders. Once established, we can develop incident response playbooks that are relevant to, and compatible with, the new incident response plan.

For playbook development, we can work with a plan devised by ourselves, or with plans that have been developed separately. We tailor playbooks to address the suitable and likely scenarios to which you may have to respond. Examples of common incident types covered by playbooks are:

- Network intrusion
- Lost or compromised device
- Website defacement
- Denial of service
- Malware outbreak
- Ransomware

Each playbook is developed to be closely aligned with the newly developed incident response plan or your existing internal plan.

Technical Triage Process Development

Assisting first responders in identifying potential incidents, allowing them to make swift decisions and implementing actions to manage the initial phase of an incident is key to protecting your information and systems. We can help you create technical processes to help first responders analyse suspicious files, emails, websites, and events to identify potential information security incidents and to manage these appropriately.

This will assist first responders with identifying potential incidents, allowing them to make swift decisions and implementing actions to manage the initial phase of an incident, whilst securing potential evidence and protecting information and systems, where possible.

Incident Response Tabletop Exercises

Once your plans are in place, we run bespoke tabletop exercises to prepare stakeholders and train them in your incident response processes.

Our incident response tabletop exercises give you assurance that your plans will work in a real-world situation. As well as providing this important validation, the interactive sessions cover all the applicable roles – from first responders and incident managers to risk owners, communication teams and legal counsel.

Covering the full end-to-end lifecycle of incident response, our tabletop exercises help you iteratively improve your plans, identify gaps in coverage and meet compliance requirements – all in a realistic manner that addresses your key threats.

Service Management

We operate a service management process that is integrated with our ISO 9001 Quality Management System.

All projects are assigned a lead consultant and a project manager throughout delivery of the testing. We operate an escalation procedure in the event of unresolved client dissatisfaction; at the time of G-Cloud 14 submission, this procedure has never been used.

Service Constraints and Levels

We do not have service constraints and levels, other than those specifically tailored and agreed in each 'Statement of Work' within a proposal.

Financial Recompense

We do not have a formal recompense model; as part of our ISO 9001 certification and commitment to customer service, we monitor the quality and delivery of all testing services very carefully.

Training

Training is offered in several of the testing service disciplines we offer; we are happy to discuss training options with our customers.

Ordering and Invoicing Process

Our normal process is to produce a 'Statement of Work' within a commercial proposal and once acceptance is given (through a signed order form or purchase order) we will commence the scheduling process.

Fixed price projects are invoiced on acceptance of the deliverables of each work task. Projects undertaken on a time and materials basis are invoiced monthly in arrears. We are happy to discuss the ordering and invoicing process with our customers.

Termination Terms

Refer to the separate 'Terms and Conditions' document.

Data Restoration / Service Migration

Data restoration and service migration is not included in our price.

Customer Responsibilities

All customer responsibilities will be defined in the 'Statement of Work' for each engagement/project.

Technical Requirements

All technical requirements and service dependencies are discussed with the client during scoping, as in most cases each project has different requirements. Technical requirements and testing pre-requisites will be documented in the 'Statement of Work' within the proposal.