

## **Service Definition**

### **Information Security Consultancy**

#### **Introduction**

NTA Monitor has supplied independent information assurance consultancy services to the public sector since 1997, and is able to offer a range of tailored services to meet your IA requirements, including:

- Information Security Gap Analysis
- Information Security Audit
- ISO 27001
- Third Party Supplier Security Assessments
- Review/Creation of Information Security Policy & Procedure Documentation
- Security Incident Readiness

#### **Scoping**

A scoping meeting will be held at the outset of the engagement to fully understand your organisation's aims, goals and expectations relating to information security. A detailed proposal will then be prepared outlining the stages involved, milestones and the level of both NTA and your organisation's input required to meet requirements.

#### **Service Overview**

These services may be purchased either individually or as a collection of services offered by NTA Monitor.

By their very nature these services are bespoke and tailored appropriately against the individual organisation and their existing security posture. The following is a broad outline of the elements involved with each service:

- Information Security Gap Analysis
  - Understand context of the organisation (what information needs protecting, responsibilities, priorities and objectives)
  - Current information security situation (existing controls, what testing/auditing has already taken place)
  - Work through policies, procedures and technical controls/implementation
  - Produce report highlighting gaps and areas for improvement
- Information Security Audit
  - Analysis of IT and information security
  - NTA involvement with the Information Security Management System (ISMS)
  - Interviews with key stakeholders and senior staff (e.g. COO)
  - Review existing policy and procedure documentation and highlight where these are not being followed
  - Report on findings with recommendations for improvement
- ISO 27001
  - Implementation – formal certification or simply conforming with the standard
  - Upgrades from 2005 to 2013

## **Service Definition**

### **Information Security Consultancy**

- Third Party Supplier Security Assessments
  - Distribution and review of security questionnaires to understand third party suppliers' approach to information security and handling of your data, with report of findings
  - Third party supplier network (internal and external) and application vulnerability assessments
- Review/Creation of Information Security Policy & Procedure Documentation
  - Aimed at organisations' working towards compliance standards such as ISO 27001 or implementing an ISMS as part of governance and best practice
  - Identify both minor and major defects
  - Report with recommendations for improvement
  - Rewriting of policies and procedures based on agreed changes
  - Creation of policies and procedures from scratch
- Security Incident Readiness
  - Preparation and planning for an information security incident
  - Staff awareness and training
  - Implementing suitable technical controls for detection and response to an incident
  - Table-top exercises based on expertly constructed scenarios to test readiness

## **Service Management**

You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling onsite delivery, ensuring reports are sent out in a timely manner, scheduling follow up activities and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

## **Ordering and Invoicing Process**

Once the scope of work and number of units/days required has been agreed between the customer and NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

## **Customer Responsibilities**

The customer is responsible for providing relevant access, contact details and documentation as required, with a commitment from key stakeholders to engage with NTA to ensure the most successful outcome from the service required.