Service Map

Assessments we offer and follow up services aligned to our assessment

ASSESS PORTFOLIO

The assessment delivered is selected during the pre-engagement stage based on external pressure, regulatory or customer, and complexity, depth and breadth of the client organisation – the customer may add elements if necessary – A DORA aligned assessment is not listed below but is available.

Assessment 1 – UK National Cyber Security Centre – Cyber Assessment Framework (Full assessment)

This assessment is primarily for UK based clients and would suit a client who works solely in the UK and either works with or is part of UK government, CNI or the National Health Service.

Assessment 1a – UK National Cyber Security Centre – Cyber Assessment Framework (lite assessment)

This assessment is best suited for small to medium businesses to gauge their alignment to the cyber assessment framework. This assessment is quicker and less in-depth than the full version.

Assessment 2 – National Institute of Standards and Technology (NIST) Cyber Security Framework Alignment Assessment (2.0)

This assessment will consist of reviewing the client's alignment with the 6 Functions 21 Categories and the 106 subcategories of the NIST framework.

Assessment 3 – ISO27001:2022 Alignment Assessment

This assessment is primarily for organisations that are looking towards ISO27001 certification or are looking to check their alignment to ISO27001. This is for any type of organisation of any size.

Assessment 4 – International Electrotechnical Commission (IEC) 62443 for Operational Technology Control Systems alignment assessment.

This is for organisations with manufacturing capability who wish to review their alignment to IEC62443 standard for OT security in manufacturing. This assessment will also review the IT capability and the boundary that exists between the IT and OT layer of the network.

ADDRESS PORTFOLIO

The address portfolio is engaged under the title of Cyber Maturity as a Service (CMaaS). This service is procured as a subscription, any individual element can be consumed during the subscription period as needed. The subscription is priced based on the depth & complexity of the engagement (time consumed) and is delivered by an experienced CISO - Elements are listed below:

CYBER MATURITY AS A SERVICE

CYBER SECURITY STRATEGY

Hands-on guidance to define and document a proportionate strategy to meet agreed business-aligned cyber outcomes.

STRATEGIC PLANNING AND ROADMAPPING

Assistance and advice to build a cyber programme based on the cyber strategy with benefits and outcomes mapped

INCIDENT & CRISIS MANAGEMENT

Management intervention during and after an incident – not incident response, this service manages the response and stakeholder team

TECHNOLOGY EVALUATION & IMPLEMENTATION

Support solution and vendor evaluations, production of requirements to drive the procurement task and vendor proposal evaluation

SUPPLIER RISK MANAGEMENT

Supplier assessment service that defines the supplier benchmark and delivers key supplier assessments providing a supplier risk profile

SECURITY CULTURAL AWARENESS

Service that provides exposure to the cyber security landscape, its alignment to business risk and drives best practice behaviours to reduce incidents

RISK MANAGEMENT & COMPLIANCE

Hands-on guidance to manage risk & regulatory compliance organically or during change, includes continuous assessment of business risk improvement

PROGRAMME MONITORING & OPTIMISATION

Programme management oversight and programme efficiency improvement designed to ensure that outcomes are met in the timescales set out

thirty
nine

cyber
39