

▶ **1. Please provide the following essential information to prepare a proposal and ensure smooth communication. Kindly verify the accuracy of your contact details before submitting the form, as they are vital for our ongoing correspondence.**

Company Name _____	Primary Point of Contact (PPoC) for Proposal _____
Billing Country _____	Title / Role _____
Billing Address _____	PPoC Email Address _____
_____	PPoC Phone Number _____

What is prompting the need for this assessment?

- Periodic Regulatory & Compliance Audits (ISO Audit, PCI DSS Audit etc.)
- Understand overall Security Posture
- Mention any other reason

▶ **2. Please complete this section regarding any personal data present in the system**

As a company committed to GDPR compliance, we prioritise the protection of personal data. If the system to be tested contains any personal data, it is essential that we incorporate this information into the Data Processing Agreement (DPA) attached to the proposal you will receive from us. Accordingly, we kindly request that you carefully answer the questions below.

Important Remark: We strongly recommend that tests be conducted in a controlled testing environment using non-production data, as accessing real data is neither necessary nor aligned with the objectives of the test. This approach is especially crucial for systems containing personal data or any other sensitive data, as it minimises exposure to such data.

Does the system to be tested include any personal data? Yes No

→ Which categories of individuals' personal data are contained in the system to be tested?

Customers Employees Third Parties Others - Please specify _____

→ Please explain what type of personal data is included. Tick all the options that apply and explain what information is stored for each type of personal data you selected.

- Government Identification Numbers (e.g. Social Security numbers, passport numbers, driver's license numbers) _____
- Financial Information (e.g. Bank account details, credit card numbers, payment information) _____
- Health Information (e.g. Medical records, health insurance details, information related to physical or mental health) _____
- Biometric Data (e.g. Fingerprints, facial recognition data, other biometric metrics) _____
- Sensitive Demographic Information (e.g. Race, ethnicity, sexual orientation, religious beliefs) _____
- Other _____

▶ 3. Please answer the Scoping Questions below

G1: How many Thick Client applications are part of the scope? Please list all.

G2: What is the type of Thick Client Application Security Assessment would you like us to perform?

- Black-box Network Infrastructure Assessment (Unauthenticated Scan): This type of assessment does not require any service credentials to be provided.*
- Grey-box Network Infrastructure Assessment (Auspicated Scan as normal user): This type of assessment requires service credentials to be provided before testing.*

G3: What is the total number of modules in the Thick Client application(s)?

(e.g. Core functionality such as for Uber app it is Ride hailing, Adding Payment Method, Ride History etc.)

G4: What is the total number of external Thick Client applications for the scope of the assessment?

G5: What is the total number of web pages per application (approximate number of webpages) of the external application?

G6: What is the total number of roles of the external thick client application?

G7: What is the total number of internal applications for the scope of the assessment?

G8: What is the total number of web pages per application (approximate number of webpages) of the internal application?

G9: What is the total number of roles of the internal application?

G10: What is the thick client application stack and CMS platform on which it is built upon?

G11: Does the application use APIs? If yes, please mention what kind of APIs are used by the application.

G12: How many APIs are used by the application?

▶ 4. If there is any other information you want to add, please provide below