

## **(ITT2B) Cyber Security Engineering**

### **Question**

#### **1. Background**

- 1.1 Following the recent government spending review, TfL continues to increase passenger capacity to meet ever increasing demand, and improve customer service across all modes.
- 1.2 Our service is now more reliant on computer, communication, and software systems and the interconnectivity between electronic systems is increasing unabated. This includes the connectivity between systems within our organisation and interfaces to external networks (such as the internet and COTS-based wireless communication systems). To improve the delivery of transport services and enhance the customer experience there is a desire to obtain, communicate and utilise the information that is generated and used by our systems.
- 1.3 To protect against safety threats, deliver services reliability and consistently, reduce costs through unnecessary reactive controls, mitigations and recoveries, and to restrict the reputational damage to TfL from undesirable actions or threats, the electronic security of systems and information is critically important to us.
- 1.4 We also have a duty of care to protect sensitive customer data and other private information that may reside on our systems and to comply with existing and future legislation.
- 1.5 A whole-system approach is needed to ensure that people (including staff, suppliers, customers and attackers) are appropriately considered, including the dependency and vulnerabilities posed by them.

#### **2. The Requirement**

- 2.1 TfL is seeking specialist support to ensure that the systems and information on our estate is protected and remains secure from accidental or intentional unauthorised access or interference.
- 2.2 There is a need to develop appropriate system and information security strategies and policies that deliver quantifiable benefits in an efficient and effective way whilst minimising the impact on services, customers and staff.
- 2.3 Support is needed to assess the security risks and threats, based on an understanding of current trends, including how systems may develop and interact in the future.
- 2.4 There is a need to develop system security requirements from best practice and analyses of system functions.
- 2.5 There is a need to prescribe integrated security solutions that are consistent with the design intent of the system assets, procedures, and people interactions to which they apply.

2.6 Support is additionally required to review and audit the specification, design, development, migration and operational use of the security solutions across multiple systems and environments.

### **3. Key Accountabilities**

3.1 Oversee system security delivery, ensuring adequate assurance is provided to the client for them to authorise solutions into use, and characterise the risks, dependencies and mitigations of residual vulnerability or threats.

3.2 Establish and maintain effective relationships with suppliers and programme team discipline engineers, end user representatives and any other stakeholders.

3.3 Ensure dependencies are understood and appropriately managed, both within and across Projects and Programmes, and coordinated with other business units in TfL. Ensure risks and issues are actively managed in accordance with TfL procedures and escalated in a timely manner where necessary.

3.4 Recommend appropriate approaches to implement security policy in line with TfL's business needs. Develop and manage a comprehensive plan of activities to support delivery of security change, including risk and impact assessments.

### **4. Scenario Description**

4.1 TfL are procuring a large transport infrastructure upgrade that involves many systems and assets across the business. Some of these assets are business critical, and some provide safety functions.

4.2 The robust delivery of safe customer services is a business priority, but cost must be managed.

4.3 The upgrade incorporates new technologies that are able to gather, communicate and transmit information across the systems whilst interfacing to a number of legacy systems that are not part of the intended upgrade works.

4.4 It is intended that information gathered from the system is available to business management systems for improved customer service management. Additionally, some of this information has been promised to be made publically available to facilitate 3<sup>rd</sup> party use (via publicly available APIs).

4.5 The new technologies involve wireless communication systems, and high-speed IP communications services such as video. Existing legacy systems include electrical, electronic and traditional telephony systems.

4.6 To reduce maintenance costs, the suppliers are requesting remote access to systems and data.

- 4.7 Through the European directives of open procurement, suppliers may originate from EU member states. A number of these suppliers have partnership organisations for development and maintenance resident in other non-European countries (India, China, South Korea, Brazil, Philippines etc).
- 4.8 A core principle for reducing costs and leveraging supplier development is to adopt existing ("COTS") products.
- 4.9 A significant amount of product development is necessary (specifically software and telecommunications products, real-time controllers, data storage and forward devices, user interfaces) in some of the products. Other products require little modification for the upgrade, but considerations of their impact (including security) are required.
- 4.10 The upgraded system necessarily interfaces with important business systems and options for commercial opportunities (tracking of customers, payment methods, advertising) are longer-term aspirations.

## **5. Response Content**

In no more than 1500 words contained in a maximum of 4 sides of A4 (pictures, diagrams etc. may be included in the sides of A4 limit) using the above scenario, demonstrate:

- Your overall approach to system security and information management, including evaluating business benefit and cost.
- Explain how you would manage the trade-off between the cost of procuring, developing, and maintaining security against the increasing pressure for efficiency saving and reducing costs. Specifically, outline the issues and approaches you would take to ensure adequate security provision is in place whilst managing the cost and impacts on their implementation.
- Briefly outline appropriate procurement strategies that would help protect TfL's interests, and any key security-oriented requirements that may be needed.
- The principles of good practice that you adopt, including reference to international standards and guidance where appropriate.
- The proposed approach to establishment of the security architecture, and how it combines and impacts the system (design) architecture.
- The working and governance structures that you would propose and approaches to tracking and reporting.