Schedule 2.4 – Security Management

CHANGE HISTORY

Version	Description	Author	Document Number
5.0	Execution version	TfL	75251114.10

Contents

1 Scope and Purpose

1.1 The purpose of this Schedule is to:

(a) set out the principles of protective security to be applied by the Concessionaire in its delivery of the Services;

(b) set out the Concessionaire's wider security obligations relating to the Services;

(c) require the Concessionaire to test and audit the Services to ensure compliance with the security requirements set out in this Agreement;

(d) require the Concessionaire to deliver the Services in accordance with all applicable security Standards and Good Industry Practice;

(e) set out the Concessionaire's obligations in the event of a Security Incident and/or a potential or attempted breach of security; and

(f) set out the principles for the Concessionaire's relevant design and implementation requirements of the Security Management Plan.

2 Security Principles

2.1 The Concessionaire acknowledges that security, data protection and confidentiality are of fundamental importance in relation to its provision of the Services and TTL's and any member of the TfL Group's ability to retain public confidence. The Concessionaire shall at all times comply with the security Standards and employ Good Industry Practice in its delivery of the Services.

2.2 In recognition of the importance that TTL and any member of the TfL Group places on security, data protection and confidentiality, the Concessionaire shall ensure that:

(a) appropriate members of Concessionaire Personnel and the Concessionaire's management team take responsibility for managing the different levels of security risk and promoting a risk management culture;

(b) security risks are documented in an appropriate manner; and

(c) supporting policies are implemented (to the extent not already in place) to facilitate communication with Concessionaire Personnel, support risk management objectives and to enable the Concessionaire to adopt a lifecycle approach to risk management.

2.3 The Concessionaire shall appoint a security manager with responsibility for the management of the Concessionaire's security obligations set out in this Agreement and who shall be TTL's point of contact in relation to security matters for the purposes of this Agreement (the "**Security Manager**"). The Security Manager shall be the person named as such in Schedule 9.2 (Key Personnel).

2.4 The Concessionaire shall, and procure that its Sub-contractors shall, at all times ensure that:

(a) security threats to the Services are minimised and mitigated to the fullest extent possible; and

(b) the Services shall fully comply at all times with:

(i) the security Standards;

(ii) any security requirements set out in Schedule 2.1 (Services Description);

(iii) an appropriate security risk management process and approach; and

(iv) Good Industry Practice.

2.5 The Concessionaire shall ensure that the Customer Products fully comply at all times with any security provisions set out in Schedule 4.1 (Concessionaire Solution) provided they are no less onerous than:

(a) the security Standards; and

(b) any security requirements set out in Schedule 2.1 (Services Description).

3 Access Controls and Secure Configuration of Systems

3.1 The Concessionaire shall, throughout the Term develop and implement policies to ensure that:

(a) the latest security patches are applied to all relevant Telecommunications Infrastructure and software as required and within a timeframe appropriate to the criticality of each security patch;

(b) account management and configuration control processes are implemented to ensure that access to the Services by Concessionaire Personnel is limited to the extent required for them to fulfil their roles in supporting the delivery of the Services. The Concessionaire shall ensure that the relevant policies address reviews and revocation of such access rights when Concessionaire Personnel change roles or no longer support the delivery of the Services and shall require that authentication mechanisms such as password complexity and additional authentication factors (such as physical tokens) are implemented;

(c) any system administration functionality is strictly controlled and restricted to those Concessionaire Personnel who need to have access to such functionality and that the ability of Concessionaire Personnel to change the configuration of the Services is appropriately limited and fully auditable;

(d) Concessionaire Personnel are informed of what constitutes acceptable use of the Services and the consequences of non-compliance;

(e) any pre-configured passwords delivered with any Telecommunications Infrastructure or software are changed prior to their implementation for use in the Services;

(f) the Services have appropriate boundary controls in place including the use of industry standard firewalls and malicious software protection to ensure that risk of unauthorised access is reduced to an acceptable level;

(g) all wireless devices are secure; and

(h) software upgrades and patching are managed centrally and access to any software shall be granted using the principle of least privilege.

4 Concessionaire Personnel

4.1 The Concessionaire shall:

(a) ensure that all Concessionaire Personnel are security screened in accordance with the Baseline Personnel Security Standard (BPSS); and

(b) provide to TTL within five (5) Working Days of the Effective Date and every six (6) months thereafter, written confirmation that all Concessionaire Personnel are security screened in accordance with the BPSS.

4.2 The Concessionaire shall immediately notify TTL if it becomes aware of any actual or potential security clearance or vetting issues in relation to the Concessionaire Personnel and the Concessionaire shall undertake any action reasonably requested by TTL in relation to mitigating the impact of any such security clearance issues.

5 Training

5.1 The Concessionaire shall ensure that all Concessionaire Personnel have undergone suitable security awareness training prior to their deployment and such security awareness training shall cover, as a minimum:

(a) account usage;

(b) malicious software;

(c) home and mobile working;

(d) use of removable media;

(e) audit and inspection; and

(f) Security Incident reporting,

and the training shall include any specific requirements according to their role.

5.2 The Concessionaire shall implement an up-to-date on-going programme of security awareness training for Concessionaire Personnel throughout the Term.

5.3 The Concessionaire shall provide additional training to Concessionaire Personnel, which may be required following a Security Incident, the application of a patch or update, or any relevant Contract Change or Operational Change.

5.4 The Concessionaire shall ensure that all Concessionaire Personnel are familiar with their responsibilities under applicable Law and policies including, as a minimum, the Data Protection Legislation, the FOIA, the security Standards and policies in relation to the handling of protectively marked materials both during their employment or appointment (as applicable) and following the termination of or change to the terms of their employment or appointment (as applicable).

5.5 The Concessionaire shall monitor the effectiveness of any training given to Concessionaire Personnel during the Term and shall take appropriate action if any such training is identified as being ineffective.

6 Testing and Audit

6.1 The Concessionaire shall conduct security testing in accordance with the Security Management Plan including security penetration testing of the Services.

6.2 The Concessionaire shall conduct regular automated security tests of the Services in accordance with Good Industry Practice, including vulnerability scans and ethical hacking and penetration tests of the Services, and ensure that any identified vulnerabilities are remedied within a reasonable period of time, taking into consideration the risk posed to TTL, any member of the TfL Group and the Services.

6.3 The Concessionaire shall procure services from a Certified Cyber Security Consultancy to conduct security tests on the Services, including ethical hacking and penetration tests, to assure that the Services comply with the security obligations set out within this Agreement, including:

(a) the security Standards;

(b) the Security Incident Management Process;

(c) the Security Management Plan; and

(d) the provisions in this Schedule.

6.4 In addition to complying with the requirements of PCI DSS and other relevant industry standards and Good Industry Practice, the Concessionaire shall at least once during each Contract Year, engage an appropriately skilled third party to conduct a formal audit of the Services against the then-current versions of the following:

(a) the security controls, processes, procedures and security Standards required pursuant to this Agreement;

(b) the Data Protection Legislation (using BS10012 or another standard as agreed with TTL), where applicable; and

(c) the Security Management Plan.

6.5 Without prejudice to any other right of audit or access granted to TTL pursuant to this Agreement or at Law, TTL and/or its representatives may carry out such audits in relation to security matters in accordance with Part B of Schedule 7.5 (Financial Transparency and Audit Rights) as are reasonably required to assess the Concessionaire's compliance with the security obligations set out within this Agreement.

6.6 The Concessionaire shall within ten (10) Working Days after completion of the audit or security tests carried out in accordance with this Paragraph 6 produce a report setting out:

(a) the outcome of such audit or security tests including:

(i) any non-compliance with the security obligations set out within this Agreement; and

(ii) all identified vulnerabilities; and

(b) the Concessionaire's plans to remedy each such identified vulnerability as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement including the Change Control Procedure.

6.7 The Concessionaire shall implement its plans to remedy each identified vulnerability in accordance with the report pursuant to Paragraph 6.6.

7 Security Incident Management Process

7.1 The Concessionaire shall, and shall procure that its Sub-contractors shall:

(a) establish and document a process to identify and respond to Security Incidents and mitigate the impact of such Security Incidents on the Services, including in relation to assigning clearly defined roles and responsibilities to specific Concessionaire Personnel;

(b) promptly identify all Security Incidents; and

(c) record each Security Incident and corresponding severity level in the Information Security Management System.

7.2 If a Security Incident occurs, the Concessionaire shall, within the framework of the Security Incident Management Process:

(a) immediately take steps to assess the scope of the data (including TTL Data) compromised or affected including the amount of data affected;

(b) immediately take the steps necessary to remedy or protect the integrity of the Services against any such Security Incident;

(c) securely collect and preserve evidence, including logs, to support the Security Incident Management Process;

(d) handle any information pertaining to the Security Incident according to the handling requirements for information designated as “Official” in accordance with the Government Security Classifications policy;

(e) promptly escalate the Security Incident to a person or Governance Meeting with an appropriate level of seniority within the Concessionaire’s organisation;

(f) as soon as reasonably practicable develop a remediation plan for the Security Incident which sets out full details of the steps taken and to be taken by the Concessionaire to:

(i) correct, make good, reinstate, replace and remediate all deficiencies and vulnerabilities, loss and/or damage to the Services in connection with the Security Incident; and

(ii) perform or re-perform any security tests or alternative tests relating to the security of the Services as appropriate to ensure that the Security Incident has been addressed and its effects mitigated.

7.3 The Concessionaire shall produce a detailed report within two (2) Working Days of the resolution of the Security Incident, such report to detail:

(a) the nature of the Security Incident;

(b) the causes and consequences of the Security Incident;

(c) the actions undertaken and length of time taken by the Concessionaire to resolve the Security Incident; and

(d) the actions undertaken by the Concessionaire to prevent a recurrence of the Security Incident.

7.4 If:

(a) a Security Incident relates to the loss of material designated as “classified” in accordance with the Government Security Classifications policy, or the suspicion of unauthorised access to such classified material; and/or

(b) a Security Incident relates to ESN Service Management Services (if called off in accordance with Clause 6.34 (ESN Service Management Services)),

the Concessionaire shall immediately report the Security Incident to the TTL Representative.

7.5 If a security event occurs in relation to an aspect of TTL's or any member of the TfL Group's operations which is not a Security Incident, the Concessionaire shall to the extent requested by TTL:

(a) provide such information as is requested by TTL in relation to the Services which is relevant to the security event (including, if necessary, by collating information from the Concessionaire IT System, its Sub-contractors' systems and Concessionaire Personnel);

(b) provide relevant TTL Personnel with supervised access (or, if the Parties agree, direct access) to any relevant systems, Concessionaire Assets and Concessionaire Personnel in order to investigate the security event; and

(c) follow TTL's directions in relation to the steps necessary or desirable to remedy or protect the integrity of the Services,

and TTL shall reimburse the Concessionaire’s reasonable, demonstrable costs and expenses in relation to the Concessionaire’s compliance with such request.

8 Security Logging and Monitoring

8.1 The Concessionaire shall ensure that the Security Management Plan sets out the Security Monitoring Strategy to monitor its own performance of its obligations under this Schedule. The Concessionaire shall update the Security Monitoring Strategy as necessary throughout the Term in response to:

(a) changes to applicable Laws, regulations and standards;

(b) changes to Good Industry Practice;

(c) any relevant Contract Changes or Operational Changes and/or associated processes;

(d) any perceived or changed security threats;

(e) any Security Incident; and

(f) any reasonable request by TTL.

8.2 The Security Monitoring Strategy shall include, as a minimum, processes for monitoring and logging (as appropriate):

(a) networks and host systems to detect attacks originating both on an internal private network or from public networks (e.g. internet);

(b) instances of or attempts at unauthorised or accidental:

(i) input or misuse of the Services and the Concessionaire IT System; and

(ii) access to TTL Data,

by Customers, End Users, TTL Personnel and Concessionaire Personnel;

(c) Malicious Software on the Concessionaire IT System;

(d) access to and movement of TTL Data, including internal Concessionaire access to such TTL Data; and

(e) traffic for unusual or malicious incoming and outgoing activity that could be indicative of an attempted or actual attack.

8.3 The Concessionaire shall ensure that access to system logs and monitoring information is strictly restricted to those Concessionaire Personnel who need to access these items to ensure the delivery and integrity of the Services.

8.4 The Concessionaire shall ensure that any monitoring process complies with the Security Monitoring Strategy and all of its legal and regulatory obligations pursuant to applicable Law.

8.5 The Concessionaire shall maintain a log of:

(a) all instances of Concessionaire Personnel accessing Personal Data;

(b) all Customers, TTL Personnel and Concessionaire Personnel logon attempts, successful and failed, to the Services or any elements of the Concessionaire Solution requiring authentication;

(c) all actions taken by Customers, TTL Personnel or Concessionaire Personnel with administrative privileges;

(d) all instances of accounts being created for Customers, TTL Personnel or Concessionaire Personnel and their relevant privileges;

(e) all records of formal staff induction or certification required by Concessionaire Personnel to operate systems and handle TTL Data (where required);

(f) all instances of accounts for Customers, TTL Personnel, or Concessionaire Personnel being deleted;

(g) changes to Concessionaire Personnel membership of access groups for system resources that comprise the Concessionaire Solution;

(h) group privilege changes against each of the system resources that comprise the Concessionaire Solution;

(i) unauthorised use of input and output devices and removable media; and

(j) all access to log files and audit systems.

8.6 The Concessionaire shall implement recording mechanisms to identify Customer, TTL Personnel and Concessionaire Personnel and their actions when cases of misuse and fraud are being investigated and shall ensure that any such recording mechanisms are protected against manipulation and disruption.

8.7 The Concessionaire shall retain the logs maintained pursuant to Paragraph 8.5 in accordance with the provisions of Schedule 8.4 (Document Management) and Schedule 2.3 (Standards).

8.8 The Concessionaire shall regularly review logs to identify any:

(a) anomalies;

(b) suspicious activity; and

(c) Security Incidents.

9 Malicious Software

9.1 The Concessionaire shall comply with its obligations in relation to Malicious Software set out in this Agreement including those set out in Clauses 21.10 and 21.11 (Malicious Software).

10 Removable Media

10.1 The Concessionaire shall implement appropriate controls to ensure that the use of removable media is restricted strictly to that needed to supply and support delivery of the Services.

10.2 The Concessionaire shall ensure that all Concessionaire Personnel with access to removable media are subject to acceptable use policies, on-going risk management procedures and appropriate training. Such policies and procedures shall be designed to discourage the use of removable media and protect the integrity of removable media.

10.3 If removable media is used, the Concessionaire shall ensure that it deploys suitable anti-virus and anti-malware checking solutions to actively scan for the introduction of malware onto systems and networks through all data imports and exports from removable media and that the removable media is encrypted to a suitable standard.

11 Mobile and Home Working

11.1 The Concessionaire shall have a home and mobile working policy in relation to the Concessionaire Personnel.

11.2 The Concessionaire shall ensure through this policy that:

(a) all data, including TTL Data, is protected and suitably encrypted when stored outside of TTL Assets and Concessionaire Assets;

(b) all data, including TTL Data, is protected when accessed, imported or exported through a connection other than one which is accessed at TTL Assets; and

(c) Security Incident management plans and processes acknowledge the increased risk posed by home and mobile working such as theft or loss of data, including TTL Data and/or devices.

12 Disposals

12.1 The Concessionaire shall not reuse any elements of the Concessionaire IT System, Telecommunications Infrastructure or software or removable media used in the performance of the Services unless such items have been wiped securely in accordance with a standard agreed with TTL in writing. The Concessionaire shall securely dispose of the Concessionaire IT System, Telecommunications Infrastructure and software used exclusively for the delivery of the Services to a standard agreed with TTL in writing upon the termination or expiry of this Agreement or when such elements of the Concessionaire IT System, Telecommunications Infrastructure or software are no longer required for the delivery of the Services, whichever is sooner, and documented accordingly.

12.2 The Concessionaire shall ensure that the disposal of any relevant Telecommunications Infrastructure or software is accurately reflected in the Infrastructure Register and the CMDB.

13 Security Management Plan

13.1 The Outline Security Management Plan as at the Effective Date is set out at Annex 1 (Outline Security Management Plan).

13.2 The Concessionaire shall within one hundred (100) Working Days of the Effective Date submit to TTL for Assurance a draft detailed Security Management Plan which shall be consistent with the Outline Security Management Plan and as a minimum shall:

(a) set out the security measures to be implemented and maintained by the Concessionaire in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure the Services comply with this Schedule;

(b) set out the responsibility and security measures relevant to the storage, processing or management of Personal Data and, where applicable, TTL Personal Data in accordance with Clause 24 (Protection of Personal Data);

(c) set out the Security Monitoring Strategy;

(d) reference and comply with any security requirements set out in Schedule 2.1 (Services Description);

(e) in relation to Customer Products, reference and comply with any security provisions set out in Schedule 4.1 (Concessionaire Solution);

(f) reference and comply with any applicable Standards or TTL or any member of the TfL Group's polices set out in Schedule 2.3 (Standards);

(g) state any other cyber security industry standards over and above those set out in Schedule 2.3 (Standards) which are applicable to the Services;

(h) state all applicable Law which relates to the security of the Services; and

(i) comply with any other security requirements TTL may reasonably request from time to time.

13.3 When Assured such detailed plan shall replace the Outline Security Management Plan and become the "**Security Management Plan**".

13.4 The Concessionaire shall review and update the Security Management Plan at least once every Contract Year and as required in response to:

(a) changes to the Standards;

(b) emerging changes in Good Industry Practice;

(c) any relevant Contract Change or Operational Change and/or associated processes;

(d) any new perceived or changed security threats; and

(e) any reasonable request by TTL.

13.5 The Concessionaire shall submit any amendments to the Security Management Plan for Assurance by TTL.

14 Information Security Management System (ISMS)

14.1 The Concessionaire shall within thirty (30) Working Days of the Effective Date develop, implement and operate the ISMS relevant to the Services.

14.2 The Concessionaire shall ensure that the ISMS includes sufficient cyber security governance, policy, process and procedures to manage information security risks.

14.3 The ISMS shall be designed to protect all aspects of:

(a) the Services;

(b) all processes associated with the delivery of the Services;

(c) the Telecommunications Infrastructure:

(d) the Concessionaire Solution; and

(e) any information and data (including Confidential Information and TTL Data) to the extent used by TTL, any member of the TfL Group or the Concessionaire in connection with this Agreement.

14.4 If the investigation of a Security Incident reveals weaknesses or flaws in the ISMS the Concessionaire shall as soon as reasonably practicable develop a remediation plan for the ISMS which sets out full details of the steps to be taken by the Concessionaire to remedy the weakness or flaw.

14.5 The Concessionaire shall implement its plans to remedy each identified weakness or flaw in accordance with the remediation plan pursuant to Paragraph 14.4.

14.6 The Concessionaire shall maintain and regularly improve the ISMS and shall fully review the ISMS in accordance with ISO/IEC 27001 at least once every Contract Year, or from time to time in response to:

(a) changes to the Services;

(b) changes to Good Industry Practice;

(c) any relevant Operational Changes or proposed Operational Changes to the Services and/or associated processes;

(d) any new perceived or changed security threats; and

(e) any reasonable request by TTL.

14.7 The Concessionaire shall provide the results of such reviews to TTL (together with such related information as TTL may reasonably request) as soon as reasonably practicable after their completion. The results of the review should include:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

(c) proposed modifications to the procedures and controls that affect the ability to respond to events that may impact on the ISMS; and

(d) suggested improvements in measuring the effectiveness of controls.

15 Compliance with ISO/IEC 27001

15.1 The Concessionaire shall obtain, from a UKAS-registered organisation, certification of the Information Security Management System to ISO/IEC 27001 for the aspects of the Concessionaire's business involved in or supporting delivery of the Services. The Concessionaire shall obtain such certification within twelve (12) months of the Effective Date and shall maintain such certification throughout the Term.

15.2 If certain parts of the Information Security Management System do not conform to Good Industry Practice or controls as described in ISO/IEC 27001 and Schedule 2.3 (Standards), the Concessionaire shall promptly notify TTL of this.

15.3 TTL may, in accordance with Part B of Schedule 7.5 (Financial Transparency and Audit Rights), carry out, or appoint an independent auditor to carry out, such regular security audits as may be required in accordance with Good Industry Practice in order to ensure that the Information Security Management System maintains compliance with the principles and practices of ISO/IEC27001.

15.4 If on the basis of evidence provided by such audits, TTL, acting reasonably, considers that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Concessionaire, then TTL shall notify the Concessionaire of the same and the Concessionaire shall, as soon as reasonably practicable, provide TTL with a written plan to

remedy each such non-compliance as soon as possible, provided that any such remediation must be implemented in accordance with this Agreement.

16 Approved Products

16.1 The Concessionaire shall ensure that all Telecommunications Infrastructure and software providing security enforcing functionality are certified under the NCSC Commercial Product Assurance (CPA) scheme to the appropriate grade, as determined by the security policy documents referred to in Schedule 2.3 (Standards), provided that relevant certified products are available in the market.

16.2 If a product provides cryptographic functionality but has no assurance under the CPA scheme, then the product should be assured under the NCSC Certified Assisted Products Service (CAPS) to a level commensurate with the assurance requirements set out in IAS1&2 Supplement.

16.3 If a product is not assured under either the CPA or CAPS schemes, TTL will consider another recognised assurance, such as Common Criteria certification, to a level commensurate with the assurance requirements set out in IS1 and IS2.

16.4 If a product has no formal assurance, TTL reserves the right to require bespoke assurance of that product under a recognised scheme such as NCSC Tailored Assurance Service (CTAS).

Annex 1 - Outline Security Management Plan

1 Purpose

1.1 The purpose of this document (the OSMP) is as follows:

(a) define the scope and boundaries of the Security Management Policy, Security Management Plan, and Information Security Management System - collectively the BAI Information Security Framework;

(b) document roles and responsibilities within the BAI Information Security Framework;

(c) outline the principles of, and approach to, Security Management which will be applied in relation to the Services;

(d) outline approach to compliance with provisions of Schedule 2.4 (Security Management); and

(e) document the commitment from BAI to managing Information Security according to leading industry practice across the key phases of the project - implementation and operations.

2 Context and Scope

Context

2.1 The OSMP is not intended to define or document the operational processes, procedures, or associated work instructions or documentation records to be delivered as part of the Services offered. It is an outline of the contents of the Security Management Plan (SMP), which in turn outline where, within the BAI Information Security Framework, these detailed artefacts are to be delivered. As the OSMP is an outline of the SMP, which in turn is the top-level document, it refers out to other documents rather than reproducing their content.

2.2 The position of the OSMP within the BAI Information Security Framework is below:

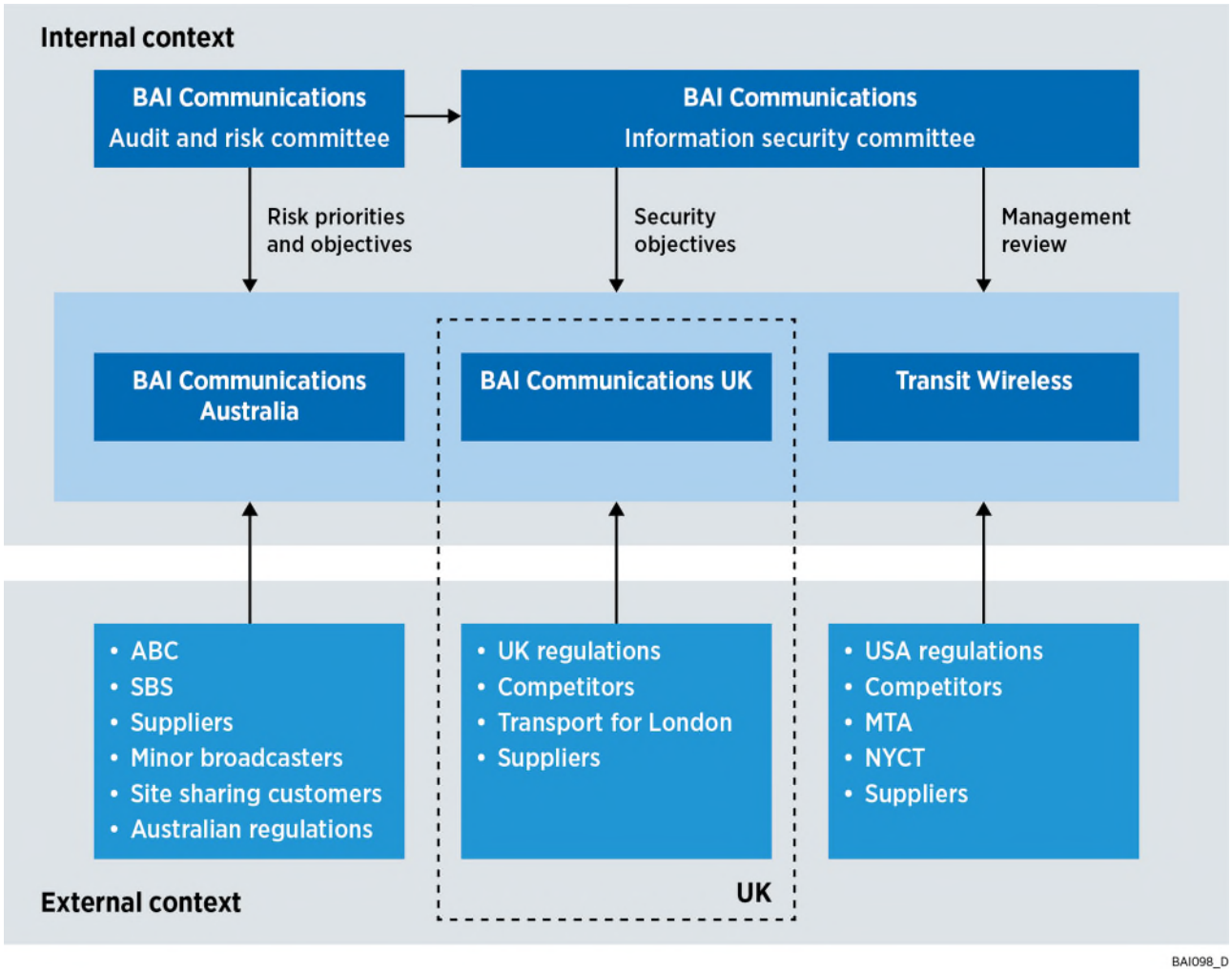

Figure 1: BAI Information Security Framework

2.3 BAI determines external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcomes of the BAI Information Security Framework. As part of this process, BAI has determined the interested parties that are relevant to this framework and will work to understand the requirements of these interested parties relevant to information security.

2.4 The following factors have been considered:

External	Internal
Legal and regulatory (including TfL Standards)	Contractual relationships
Technological	Business objectives
Environmental	Culture, competencies and structure
Supply Chain	Systems and infrastructure

Scope

2.5 This OSMP applies to all Services envisaged within the Concession:

(a) all products and services provided to our customers;

(b) all data and information created, received and managed in the course of the concession;

(c) all permanent and temporary BAI staff who manage and support BAI, TfL and customers' systems and information; and

(d) all third parties, contractors and suppliers accessing or handling BAI, TfL, or customer information, equipment, network or systems as part of BAI's delivery of the Concession.

3 BAI Information Security Framework

Information Security Policy

3.1 The Information Security Policy (ISP) provides the formal policy basis for information security activities within BAI, available in a documented form to all persons within the scope of the ISMS via the BAI Policy Portal. The ISP provides the basis for information security activities, and is supported by a framework of standards, guidelines, processes, and procedures. Each Security Service established and operated by the ISMS has a basis in policy. The ISP is available to all persons affected by the policy and is supported by an Information Security Policy Statement, available publicly via our website, outlining BAI's commitment to information security.

Outline Security Management Plan

3.2 The OSMP defines the scope and boundaries of the Security Management Policy, Security Management Plan, and Information Security Management System - collectively the BAI Information Security Framework. It also documents roles and responsibilities within the BAI Information Security Framework, outline the principles of, and approach to, Security Management which will be applied in relation to the Services, outline approach to compliance with provisions of Schedule 2.4 (Security Management), and document the commitment from BAI to managing Information Security according to leading industry practice across the key phases of the project - implementation and operations.

Security Management Plan

3.3 The SMP, aligned with the OSMP, describes how BAI manages information security in a manner that can be classified as leading industry practice, and specifies any additional or different application of controls, specifically required due to the nature of Services offered throughout the Concession period.

Information Security Management System

3.4 The overall scope of the ISMS has been formed with consideration of the need, expectations and requirements of the organisational context, namely the design, build and operation of highly available broadcast, cellular, Wi-Fi, and fixed line digital communications networks on behalf of our customers. The scope of the ISMS is reviewed in response to significant changes in organisational structure, objectives or operations.

3.5 The scope and boundaries for the ISMS are documented and maintained in the Eramba system under the following hierarchy:

(a) locations;

(b) systems;

(c) departments;

(d) business processes;

(e) networks;

(f) facilities;

(g) hardware types; and

(h) information assets.

3.6 The ISMS design process assesses both the external and internal contexts for BAI UK as part of determining the issues that are relevant to the design, operation, monitoring, and continual improvement of the ISMS. It also takes into consideration internal best practice based on BAI's operation of similar networks in North America and Australasia.

Customers

3.7 Customers with requirements and/or expectations for BAI regarding information security, or who have access to BAI information, equipment or facilities are represented within the ISMS. These customers and their requirements are registered within the Third Parties module of the Eramba information system with a type of ‘Customer’.

Regulators

3.8 Regulators which produce applicable standards and regulations are formally registered within the ISMS within the Third Parties module of the Eramba information system with a type of ‘Regulator’.

4 Roles and Responsibilities

Overview

4.1 Roles and responsibilities for Security Management have been designed such that the operational importance placed on Security is in line with the commitments made throughout BAI's Information Security Framework. Ultimate accountability resides with the CEO, supported by a full time Risk and Compliance Manager, who in turn is supported via internal and external resources based in the UK and throughout BAI Group.

4.2 Roles and Responsibilities Matrix

Role	Responsibility	Methods / Metrics
BAI UK CEO	Ensuring the resources required for implementation, maintenance and continual improvement of the Information Security Framework are provided	Engagement with Risk and Compliance Manager to define organisational and financial resources required
	Ensures persons associated with the ISMS are competent based on appropriate education, training and experience	Engagement with People Department with regards to Baseline Personnel Security Standard (BPSS) clearance checks and competency-based interviews
	Actively reviewing the performance of the ISMS	
Risk and Compliance Manager	Highlight resource needs and deficiencies	Develop cost projections that align to normal budget cycles
	Overall ISMS performance	ISMS objective status Number of information security incidents Number of security alerts processed Percentage of users with Multi-Factor Authentication (MFA) required Percentage of users possessing legacy workstation Percentage of systems with local authentication Percentage of systems with local logging
	Security Services / Controls	Control reviews completed Associated asset risks for each control Related security incidents for each control Effectiveness metrics defined for each control
	Risk Assessment / Review	Completed on time

Role	Responsibility	Methods / Metrics
		Risks documented correctly Treatment plans reviewed by risk owners
	ISMS documentation	Reviews completed on time Compliance with ISO requirements Plans for address compliance gaps reviewed Communication plan followed
	Security awareness	Percentage of staff up to date with training Composition of training reviewed Staff know their responsibilities (assessed via internal audit interview)
	Corrective action tracking	SHIELD system
	Reviewing internal audit findings and corrective actions	Post audit reviews
	Maintenance of information security policies	Updating of documentation
	Defining and monitoring information security objectives	Updating of documentation Reporting
	Ensuring information security activities support the objectives of BAI UK	Engagement with business to align business objectives
	Reviewing information security risks and the associated controls	Internal and External support
	Maintaining compliance with ISO/IEC 27001:2013	Internal and External Audits
Manager, Information Security and IT Compliance	Ensuring information security activities support the objectives of BAI Group	Flow down of information

Role	Responsibility	Methods / Metrics
	Support Risk and Compliance Manager in their Role and Responsibilities	Flow down of information
People Department UK	Retain evidence of competence and security clearance for all employees	BPSS clearance checks Competency based interview records Training records All records retained in soft copy in employee files
BAI Information Security Committee (ISC)	Governing the ISMS including review of performance and setting of priorities	
Audit and Risk Committee (ARC)	Tracks organisational risks, including a summarised representation of information security risk	
	Conduct internal audits	Refer to the ISO/IEC 27001:2013 Internal Audit Plan for further details.

5 Principles of Security Management

Importance of Security Management to TfL

5.1 BAI acknowledges and affirms that security, data protection and confidentiality are of fundamental importance in relation to the provision of Services and TfL's ability to retain public confidence. BAI will comply with the security Standards outlined in Schedule 2.4 (Security Management) and employ Good Industry Practice in its delivery of the Services.

Importance of Security Management to Customers

5.2 BAI acknowledges that our customers place significant emphasis on the confidentiality, integrity and availability of the data carried by their networks. Consequently, BAI is committed to ensuring the highest practicable security standards are maintained as part of the technical solutions we deliver on their behalf, and the physical environments in which they are deployed.

BAI Security Obligations

5.3 BAI will be responsible for the security of:

(a) any sites located beyond TfL's estate;

(b) all personnel, including sub-contractors; and

(c) all systems, solutions, and services, including those of sub-contractors, in respect of their involvement in the provision of Services.

5.4 BAI will also be responsible for:

(a) BAI Information Security Framework; and

(b) security architecture.

5.5 Throughout the concession, BAI will ensure that it shall:

(a) appropriately manage security threats to Services, including to the extent to which it is possible, threats that arise as a result of external failures in security such as those relating to transmission equipment or unauthorised access to the TfL estate; and

(b) comply with the Security Standards and TTL Requirements.

TfL Security Obligations

5.6 TfL shall, at all times during the Concession Period, ensure that the physical security environment which houses BAI's technical solution, specifically the London Underground where BAI will deploy the Commercial Mobile Service (CMS), Emergency Services Network (ESN), and components of the Fibre and Streetscape Services (including but not limited to Points of Presence) is of a level of security which:

(a) is in accordance with security standards and good industry practice including any applicable Guidance; and

(b) complies with all applicable Laws.

6 Approach to Security Management

Overview

6.1 BAI's overall approach to Security Management is to utilise an adapted version of our Group-wide Three Lines of Defence Risk Management Framework. Our approach is as follows:

(a) first line is the responsibility of operations and business units to identify and manage risks directly, including the design and operation of controls;

(b) BAI’s Risk Management Team leads the second line of defence, responsible for reporting enterprise risks to the Executive Team, Audit and Risk Committee and the Board; and

(c) third line is our Internal and External Audit functions that are responsible for independent assurance of the effectiveness of the internal controls in place to manage risk to within an accepted level of risk tolerance.

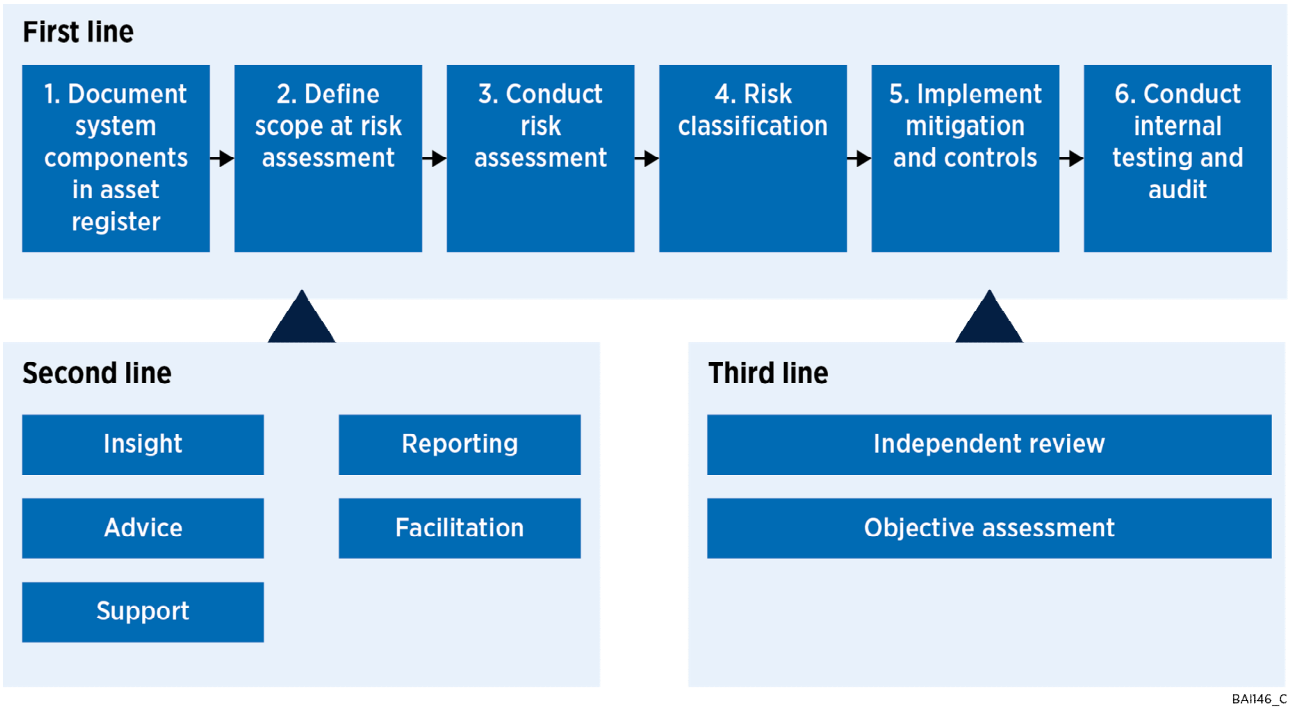

Figure 2 Approach to Security Management

First Line

6.2 Focusing on the Operational Technology (OT) Environment within the UK operating business, i.e. the scope of the assessment are the services we are providing our customers related to the Concession. BAI's First Line utilises a component-driven approach to security management. This approach requires an assessment of the threat that each component within the overall system faces, their vulnerabilities, and the business impact that a compromise would cause.

6.3 Once identified, specific risks faced by specific components within the system are classified according to the severity of the risk's impact and the ease with which the vulnerability could be exploited by a threat. This allows for prioritisation of risks, with the highest priority risks in terms of impact and likelihood are mitigated first.

6.4 The system components assessed in this way are:

(a) hardware (including but not limited to low power radio nodes, high power radios, DWDM filters etc.);

(b) software (including but not limited to software required to operate Services, as well as managing the Services such as Operational Support Systems, Business Support Systems etc.);

(c) data (e.g. traffic carried by the DAS);

(d) services (e.g. Wi-Fi, Fibre Services);

(e) information (e.g. login details required to access a service); and

(f) staff (BAI and supply chain).

6.5 From there, BAI compiles an asset register which defines the full list of components being assessed, including those items (e.g. low power radio nodes) which BAI does not control. These components are then assessed based on the following criteria:

(a) vulnerability: a weakness in any component that, if exploited, would mean an impact is realised; and

(b) impact: the consequences if a risk is realised:

(i) at a macro level these are assessed in terms of impact to BAI's financial performance, reputation, compliance with laws and regulations, health and safety, operational performance (i.e. maintenance of service) and flow-on to customers, and impact to the environment and community; and

(ii) looking at information specifically, impact is assessed in terms of confidentiality, integrity and availability, of information.

6.6 Once the various threats, vulnerabilities and impacts have been assessed, they are combined to create a list of risks which are prioritised according to likelihood of the risk materialising and the impact on BAI – utilising BAI's Risk Rating Matrix.

6.7 The next step in our approach to Security Management is Risk Mitigation and Acceptance:

(a) mitigation: steps taken by BAI to reduce the likelihood of risks materialising, and the impacts caused if they do occur:

(i) this can be done by transferring risk to a third party;

(b) acceptance: those risks that cannot be completely mitigated (comparable to avoided), are then accepted:

(i) accepted risks are minimised to a level as low as reasonably practical, documented, and then subject to ongoing monitoring and control.

6.8 Throughout the lifetime of the service this assessment is repeated considering evolution of known risks and new risks being identified. New risks can either arise of components initially identified in the asset register, or new components implemented as part of any change process (which in turn are added to the asset register).

6.9 Lastly, First Line carries out internal penetration testing and audits on system components on a scheduled basis, as well as impromptu / unscheduled basis to test the risk controls implemented and performance with regards to response management / protocols.

6.10 Responsibility for the First Line resides with the Engineering and Operations Teams at BAI UK, supported by counterparts in other operating businesses to leverage international best practice and learnings from businesses which have been in operation for several years.

Second Line

6.11 The Second Line facilitate and monitor the implementation and effectiveness of risk management; providing risk advice and support (in contrast to management of the risks), design risk policies, frameworks and procedures, and provide insights and assist the Board and management in defining the organisation's risk appetite.

6.12 Second Line is responsible for enabling functions which support the First Line, for example:

Function	Example of Activities
People	Implement employee and workplace related policies, control, and training programmes
Legal	Support in drafting of legal documentation ensuring contractual controls are implemented where necessary, and drafting of agreements
Finance	Decision support and financial planning for implementation of risk control processes

Third Line

6.13 BAI's Group Level internal audit capability conduct independent reviews of the Risk Management Framework, as well as provide assessments of the control design and its effectiveness. This clean-team function (i.e. not part of any operating business) provide an objective assessment of the operation of the First and Second Lines, and can call on external resources, for example external specialist penetration testing, and audit capabilities to conduct detailed functional audits.

7 Information Security Management

Overview

7.1 Information Security sits both within and outside the scope of the OT environment in that information might be gathered or created throughout the Concession term pending the evolution of Services over the Term.

Risk Assessment

7.2 The Risk and Compliance department maintains Risk Management documentation which defines risk acceptance criteria and the process for performing risk assessments. The implementation of a risk assessment methodology ensures repeated risk assessments produce consistent, valid and comparable results. The Risk and Compliance Manager, supported by the Manager, Information Security working with the BAI Group Risk and Compliance department, undertakes information security risk assessment exercises in accord with the ISMS calendar. The Risk and Compliance Manager maintains an information security risk register which is available to members of the ISC for review and summarised for the ARC.

7.3 Each risk has an assigned owner. If the information security risk register for an organisation contains one or more risks classified as high or extreme, there is a representative security risk created in Shield for the organisation. Each risk is classified in terms of likelihood and consequence resulting in a risk rating. This rating is used as part of risk treatment prioritisation.

7.4 Information security risks identified outside of scheduled risk assessment exercises are recorded within the information security risk register and managed in accordance with the agreed risk management process.

7.5 BAI undertakes information security risk assessments at planned intervals. Each assessment is indicated on the ISMS calendar.

Activity	Tracking	Schedule
Detailed information security risk assessment	Eramba GRC	February – March
Corporate risk assessment	Shield	Every 6 months
Presentation of risks to ISC	ISC records	June, December
Presentation of summarised risks to ARC	ARC records	February, May, August, October

7.6 Each individual information security risk is reviewed as part of the annual information security risk assessment in consultation with the risk owner.

Documentation

7.7 The ISMS maintains the documentation required by the ISO/IEC 27001:2013 standard. This documentation exists as policies, standards, guidelines, processes, and procedures, which are managed according to BAI's Records Management Policy and Processes.

Monitoring, Measurement, Analysis, Evaluation and Communications

7.8 BAI plans and implements processes to meet information security requirements and objectives. We measure the success of these controls and remedial actions to address risks and opportunities. This monitoring is done via a combination of internal and external penetration testing and audits, as well as continuous vulnerability scans conducted automatically. Monitoring is also done via Group-level audit functions which ensures overall alignment with business objectives. When a non-conformity is identified, whether via internal or external audit, it is reported to the ISC. Appropriate actions are taken to control and correct non-conformities and are tracked in order to ensure the non-conformity is addressed within agreed timeframes. Where a non-conformity is identified as part of an internal audit, the finding, along with any corrective actions, is tracked in the SHIELD system.

7.9 Channels through which communication of updates to policies, processes, procedures are issued include:

(a) ISO 27001 Program Team Site (ISO Team / SharePoint);

(b) BAI Information Security Team Site (ISO Team / SharePoint);

(c) BAI Policy Portal;

(d) Eramba GRC system (Eramba);

(e) Confluence Wiki system (Confluence); and

(f) Critical Register of Important Documents (CRID) (SharePoint).

7.10 Channels through which to maintain awareness of key principles associated with Information Security include:

(a) BAI global intranet and policy portal;

(b) Microsoft Teams;

(c) lunch and learn sessions;

(d) email advisory and support service; and

(e) face-to-face training sessions.

Continuous Improvement

7.11 Continuous improvement is a core focus of the ISMS. This includes genuine assessment of effectiveness and pro-active efforts to improve in accordance with the ISMS calendar.