

essential services. This includes data, people, and systems, as well as any supporting infrastructure (such as power or cooling).

3.4 Supply Chain Management

The requirement is that effective internal processes shall be implemented for managing internal and external suppliers of systems, components and services for the OT systems which support the delivery of TfL services.

The underlying principle is that TfL understands and manages security risks to networks and information systems supporting the delivery of essential services that arise because of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.

Regardless of the outsourcing model, TfL, as an Operator of Essential Services, remains responsible for the security of the service and therefore all the requirements that come from the NIS Regulations.

3.5 Training and Awareness

The requirement is that effective internal processes shall be implemented for identifying, delivering, and managing awareness and role specific cyber security training to TfL staff and partners to mitigate the risks to the security of network and information systems related to the delivery of essential services.

The underlying principles is that TfL staff and partners have appropriate awareness, knowledge, and skills to carry out their roles effectively in relation to the security of network and information systems supporting the delivery of essential services.

4 Governance

As stated in the policy, security is everybody's responsibility, but effective governance is achieved through a combination of policy and action to ensure that processes are in place and being followed.

Demonstrate the TfL behaviours in everything we do. Security is our shared responsibility, and we all have a part to play. In this way, we can work together to reduce the risk to our services and our people from the continuous and evolving cyber security threat.

The sections below indicate how the responsibilities and accountabilities must develop to deliver the governance requirements.

4.1 Board Direction

TfL and each business unit must display a clear line of sight for OT cyber security governance, set at board level and cascaded down through all levels of the business.

As an integral element of [R1770](#) Operational Technology Cyber Security – Document Framework, there are four policies which articulate TfL's approach to OT cyber security. These are signed at TfL board level and serve as a public statement to TfL's commitment to effective OT cyber security.

- [P006](#) Operational Technology Cyber Security
- [P007](#) Operational Technology Cyber Security - Governance
- [P008](#) Operational Technology Cyber Security - Projects and Upgrades
- [P009](#) Operational Technology Cyber Security - Operations and Maintenance

These policy statements have been written to be a clear and simple direction to all employees and partners of TfL and should be displayed prominently as a reminder of the shared commitment to OT cyber security.

4.2 Roles and Responsibilities

TfL and each business unit must establish clear roles and responsibilities for the security of OT at all levels, with clear and well-understood channels for communicating and escalating risks.

Section 5 explains the set of generic roles which are associated with good practice in OT cyber security and further detail of the accountabilities for each role is contained within [G1770](#) Operational Technology Cyber Security – Governance.

These roles must align with either individual post holders or role types. Each business unit must identify suitable post holders or role types to deliver the associated responsibilities and ensure that the associated accountabilities are incorporated into job descriptions and terms of reference.

4.3 Decision Making and Governance Structure

TfL and each business unit must establish senior-level accountability for OT cyber security, whilst delegating decision-making authority appropriately and effectively whilst retaining oversight.

OT cyber security risks shall form an integral element of any decisions and must be embedded into the change control process. Any risks or changes must be discussed at a level of seniority which is appropriate to the impact of the risk on the business (Section 6 refers).

4.3.1 Governance Structure

A governance structure shall be established to support effective decision making for OT cyber security and this structure must allow for decision making and discussions of OT cyber security risks at the appropriate business level and by the appropriate seniority level within TfL.

- 4.3.1.1 This governance structure should align to business units or development lifecycles so that decision making is appropriate to the business or project that is impacted or affected.
- 4.3.1.2 This structure shall include representatives who are commensurate with the level of risk and business impact under discussion.
- 4.3.1.3 Each business unit shall define cyber security accountabilities and responsibilities against each role that supports the structure of OT cyber security.

Printed copies of this document are uncontrolled.
Page 7 of 32



The business unit cyber security accountabilities and responsibilities should be established as a RACI and is dependent on the function and structure of that business unit. This should be undertaken on a case by case basis and adopted to fit that business unit as a one-size fits all model is not appropriate.

- 4.3.1.4 Appropriate Cyber Security Steering and Working Groups shall be established at the appropriate business level, chaired by an appropriately senior role within the business unit and must meet on a regular basis no less than six per year.

4.3.2 Pan-TfL Cyber and Information Security Steering Group (CISSG)

The Pan-TfL Cyber & Information Security Steering Group (CISSG) shall:

- 4.3.2.1 Exist as a permanent forum to provide leadership and senior management oversight of cyber and information security across the whole of TfL.
- 4.3.2.2 Comprise the key director level stakeholders across TfL who have a principal interest in cyber/information security outcomes.
- 4.3.2.3 Oversee the organisation-wide management of cyber and information security risks to TfL to ensure that the management of cyber security risks to TfL business activities and operational services is consistent, compliant with relevant legislation, and that those operations are cyber-safe, cyber-resilient, cyber-secure, and that they sustain TfL's reputation.
- 4.3.2.4 Determine the overall TfL cyber and information security strategy, target operating model, delivery plans, risk management framework, and assurance agenda.
- 4.3.2.5 Influence senior TfL leaders to improve management of TfL's cyber / information security risks.
- 4.3.2.6 Coordinate the governance of cyber/information security risk management across TfL.
- 4.3.2.7 Oversee the effective and timely management of cyber and information security risks.
- 4.3.2.8 Coordinate activities to enable and facilitate the TfL cyber improvement programme.
- 4.3.2.9 Oversee the effective and timely delivery of the TfL cyber improvement programme.
- 4.3.2.10 Promote sharing of good practice between different business units.
- 4.3.2.11 Liaise with business unit Steering Groups.

4.3.3 Pan-TfL Cyber and Information Security Working Group (CISWG)

The pan-TfL Cyber & Information Security Working Group (CISWG) shall:

- 4.3.3.1 Support the mandate of the CISSG.
- 4.3.3.2 Support and drive the implementation of the broader cyber & information security management agenda set by the pan-TfL CISSG.

Printed copies of this document are uncontrolled.
Page 8 of 32



- 4.3.3.3 Assist the pan-TfL CISSG in the development of security objectives and initiatives, and to support effective cyber and information security management.
- 4.3.3.4 Support and ensure that cyber and information security policies, standards, and procedures are implemented consistently across TfL.
- 4.3.3.5 Be prepared to act as a Major Cyber Incident Response (SILVER) Command, aligned to established incident response procedures.

4.3.4 Business Unit Cyber Steering Group

The Business Unit Cyber Steering Groups (BU SGs) shall:

- 4.3.4.1 Exist as a permanent forum to provide leadership and senior management oversight of cyber and information security across the BU.
- 4.3.4.2 Comprise the key director level stakeholders across the BU who have a principal interest in cyber/information security outcomes.
- 4.3.4.3 Oversee the BU-wide management of cyber and information security risks to safe and reliable operations to ensure that the management of cyber security risks to business activities and operational services is consistent, compliant with relevant legislation, and that those operations are cyber-safe, cyber-resilient, cyber-secure, and that they sustain TfL's reputation.
- 4.3.4.4 Implement the BU cyber and information security strategy, target operating model, delivery plans, risk management framework, and assurance agenda to meet that set by the CISSG.
- 4.3.4.5 Influence senior BU leaders to improve management of the BU's cyber / information security risks.
- 4.3.4.6 Coordinate the governance of cyber/information security risk management across the BU.
- 4.3.4.7 Oversee the effective and timely management of cyber and information security risks.
- 4.3.4.8 Oversee the effective and timely delivery of the BU cyber improvement programme.
- 4.3.4.9 Promote sharing of good practice between different business units.
- 4.3.4.10 Liaise with the CISSG and other BU Steering Groups.

4.3.5 Programme Cyber Security Steering and Working Groups

Cyber Security Steering and Working Groups shall be established at the programme level for major programmes of work, chaired by an appropriately senior role within the programme and must meet on a regular basis no less than six per year.

The Programme Steering Groups (P SGs) shall:



- 4.3.5.1 Exist as a forum to provide leadership and senior management oversight of cyber and information security across the programme.
- 4.3.5.2 Comprise the key senior stakeholders across the programme who have a principal interest in cyber/information security outcomes.
- 4.3.5.3 Oversee the programme-wide management of cyber and information security risks to safe and reliable operations to ensure that the management of cyber security risks to programme activities and operational services is consistent, compliant with relevant legislation, and that those operations are cyber-safe, cyber-resilient, cyber-secure, and that they sustain TfL's reputation.
- 4.3.5.4 Determine the programme cyber and information security strategy, delivery plans, risk management framework, and assurance agenda
- 4.3.5.5 Coordinate the governance of cyber/information security risks and activities across the programme and its contributing projects
- 4.3.5.6 Oversee the effective and timely management of cyber and information security risks.
- 4.3.5.7 Oversee the effective and timely delivery of the programme cyber improvement programme.
- 4.3.5.8 Promote sharing of good practice between different areas of the programme and other programmes.
- 4.3.5.9 Oversee the effective and timely delivery of systems to satisfy the Cyber Security Statement: "The system is acceptably secure at the point of delivery, that organisational arrangements are in place for continuously managing cyber security throughout the operational lifecycle and that residual risks are understood, managed and controlled."
- 4.3.5.10 Liaise with the CISSG and other BU and P SGs

[G1770](#) provides additional guidance on the above governance structure.

4.4 Asset Management

TfL shall implement asset management processes such that the OT assets which support the delivery of TfL services are known and associated with sufficient information to support OT cyber security processes.

IEC 62443 2-1 defines an asset as "a physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization" and notes that in the context of this document, an asset is any item that should be protected by the OT cyber security management system.

Asset Management is also a requirement under the NIS Directive (Objective A3.a).



4.4.1 Asset Register

- 4.4.1.1 Assets shall be recorded in an asset register which shall be maintained for the lifetime of the asset.
- 4.4.1.2 Assets and systems shall be classified to identify which ones may require a higher level of security and to prioritise security activities.
- 4.4.1.3 The following classifications shall be used for OT systems to support prioritising investment in cyber security improvements and identify systems which require additional risk assessment and security controls:
- **Safety critical** – OT system which performs a safety function
 - **Service critical** – OT system which will stop the service immediately if it malfunctions
 - **Service support** – OT system which may cause a degradation of service levels if it malfunctions or stop the service if it malfunctions for an extended period
 - **Non-service** – OT system which will not have an impact on service if it malfunctions.

Note that some systems may be both safety and service critical (e.g., signalling, road tunnel CCTV), in which case they should be classified as safety critical.

- 4.4.1.4 The asset register shall include the following information:

- System Name
- System Classification
- System Function
- System Owner
- System Operator
- System OEM
- Asset Name
- Asset Function
- Asset Owner
- Asset OEM
- Operating System
- Software Version
- Hardware Version
- Firmware Version
- Install Date
- Support Arrangements
- Last review date



4.4.1.5 There shall be a documented asset owner for each asset.

The asset register is an essential source of information for many processes, including risk management and vulnerability management. They should also be accessible across TfL so that common assets can be identified.

4.5 Assurance and Assurance Principles

TfL must complete assurance activities to demonstrate and document that robust and appropriate cyber security management has been undertaken and that an OT system is acceptably secure throughout its entire lifecycle.

4.5.1 Cyber Security Assurance Case

4.5.1.1 The Business Unit shall ensure that an assurance model is established to undertake the assurance of cyber security activities.

4.5.1.2 The Cyber Security Assurance Case (CSAC) shall be the means to demonstrate to internal and external TfL stakeholders including auditors and regulators that cyber security has been appropriately managed and undertaken, that a system has been secured by design throughout the project stage of its lifecycle and that it can operate securely throughout the operational stage of its lifecycle.

4.5.1.3 The CSAC shall provide an auditable trail of effective action. The CSAC is driven by three elements:

- Evidence: This is the evidence being presented in support of the claim or argument.
- Argument: This is the argument and principles to satisfy the claim.
- Claim: This is a statement asserted within the argument that can be assessed to be true or false.

4.5.1.4 The CSAC shall be used to satisfy that the Cyber Security Statement is true:

4.5.1.5 “The system is acceptably secure at the point of delivery, that organisational arrangements are in place for continuously managing cyber security throughout the operational lifecycle and that residual risks are understood, managed and controlled.”

4.5.1.6 For systems that require a safety or assurance case then the CSAC shall become the evidence to demonstrate that the system is acceptably secure.

4.5.1.7 The Cyber Security Statement is to be redetermined to be true or false following any significant change to the system or cyber security risk.

4.5.1.8 Should the Cyber Security Statement be false, then additional treatment activities will have to be undertaken to satisfy the applicable arguments and principles until the Cyber Security Statement is true.

4.5.1.9 The CSAC is comprised of a set of 4 Cyber Security Assurance Arguments and 14 Cyber Security Assurance Principles to satisfy the Cyber Security Statement.

- 4.5.1.10 Evidence must be documented to demonstrate the Cyber Security Assurance Arguments and Principles have been achieved.

The Cyber Security Assurance Arguments and Principles are aligned to the National Cyber Security Centre Cyber Assessment Framework.

- 4.5.1.11 The objective view, assessment and determination of the Cyber Security Statement should be independent of the producer of a CSAC and the delivery streams that contribute to a CSAC.

4.5.2 Argument A: Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the system.

- 4.5.2.1 Principle: Governance - The business area has appropriate management policies and processes in place to govern the approach to the security of the system:

- Ensure that a senior level accountability for cyber security of the system has been appointed and that effective security management is articulated in corresponding policies, standards, processes, and procedures.
- Ensure that a system focus for cyber security has been appointed, that roles and responsibilities for managing cyber security and owning cyber security risk are implemented and that clear channels for communicating and escalating risks and the delegation of decision making are understood.
- Ensure that cyber security risks are considered in the context of other asset and operational risk management.

- 4.5.2.2 Principle: Risk management - The business area has identified, assessed, and understands the security risks and has an established approach to risk management:

- Ensure that a cyber security risk assessment has been carried out and the risks are classified.
- Ensure identified risks are suitably and sufficiently mitigated with appropriate and proportionate countermeasures and reduced to an acceptable level.
- Ensure that risks identified as safety related are reviewed by the appropriate discipline against core hazards to determine if further mitigation is required.
- Ensure that risks identified as RAM/Performance related are reviewed by the appropriate discipline to determine if further mitigation is required.
- Ensure that risk management is performed periodically and as required and that any new or modified risk is sufficiently understood, managed, and controlled.
- Ensure that continuous verification and validation and cyber security assurance structures are in place to validate security measures and their effectiveness and to monitor cyber security risks.

- 4.5.2.3 Principle: Asset management - Everything required to deliver, maintain, or support the system is determined and understood by the business area:

Printed copies of this document are uncontrolled.
Page 13 of 32

- Ensure that assets are identified and inventoried and that cyber security is encompassed into asset management, registers, and reporting.
- Ensure that cyber security risks are managed for software and hardware obsolescence as well as during decommissioning and disposal.

4.5.2.4 Principle: Supply chain - The business area understands and manages security risks to the system because of dependencies on external suppliers:

- Ensure that the supply chain is set security expectations, including the security engineering processes to be followed and applicable security standards, requirements, and contractual obligations.
- Ensure that activities and processes for the periodic assessment and assurance of the supply chain are understood and implemented.

4.5.3 Argument B: Proportionate security measures are in place to protect the system from cyber-attack.

4.5.3.1 Principle: Service protection policies and processes - The business area has implemented, communicated, and enforces appropriate policies and processes that direct the approach to securing the system and data:

- Ensure that all appropriate processes and procedures to manage cyber security are implemented, communicated, and are embedded in normal system operation and maintenance activities and is managed continuously and is updated as appropriate.
- Ensure that change and validation processes to manage changes to cyber security controls as well as the patching, updating and security testing of the system are implemented, communicated, and understood.

4.5.3.2 Principle: Identity and access control - The business area understands, documents, and manages access to the system and users or functions that can access data or the system are appropriately verified, authenticated, and authorised:

- Ensure that controls and processes are implemented so that authorised and privileged users are identified, authenticated, recorded, and managed.

4.5.3.3 Principle: Data security - The business area protects data stored or transmitted from actions such as unauthorised access, modification or deletion that may cause an adverse impact to the system:

- Ensure that controls and processes are implemented so that system data and information about the system is identified, recorded, understood, and appropriately protected.

4.5.3.4 Principle: System security - The business area has protected the system from cyber-attack:

- Ensure that cyber security standards and requirements are included in the system and operational requirements.
- Ensure appropriate cyber security requirements developed in line with cyber security risk tolerability are included in the system requirements.



- Ensure that the system design and operation is reviewed against the cyber security and system requirements.
- Ensure that cyber security requirements are implemented using appropriate techniques and methodologies.
- Ensure that appropriate cyber security testing is undertaken using appropriate techniques and methodologies so to validate security controls and to identify system vulnerabilities.
- Ensure that cyber security requirements are tested using appropriate techniques and methodologies.
- Ensure that organisational physical, cyber and information security standards are complied with.

4.5.3.5 Principle: Resilient networks and systems - The business area builds resilience against cyber-attack and system failure into the design, implementation, operation, and management of the system:

- Ensure that appropriate backup provisions are implemented and tested.
- Ensure that cyber security is considered and incorporated into system disaster recovery and business continuity plans.

4.5.3.6 Principle: Staff awareness and training - The business area staff have appropriate awareness, knowledge, and skills to carry out their organisational roles effectively in relation to the security of the system:

- Ensure that all relevant staff are appropriately cyber security aware, trained and are capable.

4.5.4 Argument C: Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect the system.

4.5.4.1 Principle: Security monitoring - The business area monitors the security status of the system to detect potential security problems and tracks the ongoing effectiveness of the protective security measures:

- Ensure that cyber security detection tools and processes are implemented that identify the occurrence of a cyber security event and that applicable logs and alerts are available.
- Ensure that cyber security monitoring and processes are implemented.

4.5.4.2 Principle: Proactive security event discovery - The business area detects malicious activity affecting or with the potential to affect, the operation of the system:

- Ensure that normal system functions are documented and understood.

4.5.5 Argument D: Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of system functions, including the restoration of those functions where necessary.



- 4.5.5.1 Principle: Response and recovery planning - The business area has well-defined and tested incident management processes in place:
- Ensure that cyber security response and recovery activities are identified, implemented, and periodically tested within appropriate response and recovery plans.
- 4.5.5.2 Principle: Lessons learned - When an incident occurs, the business area has steps to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents:
- Ensure that cyber security lessons learnt processes are implemented and embedded in normal system improvement activities.

4.6 Regulatory Compliance

- 4.6.1 If the system is deemed to be within the scope of the Network and Information Systems Regulations (NIS) 2018, then the NIS Regulations shall apply, in particular the requirements, controls and activities determined by the regulation. The requirements, controls and activities to be applied are outlined by the Indicators of Good Practice and Contributing Outcomes of the current NIS Regulations industry profile, as determined by the DfT.
- 4.6.2 If the system processes personal information or information relating to individuals, then Data Protection Act (DPA) 2018 (The UK implementation of GDPR) shall apply, in particular the requirements, controls and activities determined by the regulation/act.
- 4.6.3 If the system accepts, processes, stores, or transmits financial information, then the Payment Card Industry Data Security Standard (PCI-DSS) shall apply, in particular the requirements, controls and activities of the standard.

Adhering to applicable regulation and legislation may require further assessment and additional requirements to be established.

5 Roles and Responsibilities

TfL and each business unit must identify the individual post holders or role types who fill the following generic good practice OT cyber security roles. In some cases, this may be a single person working in TfL or in others, could be linked to a particular role or function.

In each case, the accountabilities for the role must be included within Terms of Reference and individuals must be trained appropriately to fulfil their responsibilities.

As with any risk at TfL it remains the accountability and responsibility of the Executive until it is formally delegated to an appropriate party be that an individual or governance group.

These roles are generic and reflect good practice and it is acknowledged may not align exactly to different business areas across TfL. The emphasis should be on the business area to identify suitable individual or role to deliver the accountabilities



which support the delivery of OT cyber security in support of the safe and secure operation of TfL services.

5.1 Head of OT Cyber Security

The Head of OT Security is the most senior role for managing OT cyber security in TfL. This is usually an individual person, which normally aligns to the Chief Information Security Officer (CISO) role, but it may be considered that a senior level steering group acts across TfL.

5.1.1 Purpose

- 5.1.1.1 Accountability for OT Security Governance across TfL.
- 5.1.1.2 Ensure that there is an OT security strategy for TfL.
- 5.1.1.3 Establish and maintain OT Security governance within TfL.
- 5.1.1.4 To provide senior management guidance and support for OT Security Governance.
- 5.1.1.5 Develop business case for OT Security Governance Programme, if required.
- 5.1.1.6 Consolidate OT Security risk information for reporting to executive management and board.
- 5.1.1.7 Reporting of OT Security Governance to executive management and board level.

5.1.2 Accountabilities and responsibilities

- 5.1.2.1 Communication of OT Security business risk to TfL executive management and board.
- 5.1.2.2 Secure executive management and board support for OT Security Governance Programme.
- 5.1.2.3 Communicate to executive management and board priorities as they affect OT Security.
- 5.1.2.4 Secure budget for centrally funded OT Security activities.
- 5.1.2.5 Ensure TfL OT security standards are in line with local guidance, industry best practice for the sector and meet legal requirements.
- 5.1.2.6 Approval of TfL-wide OT security policies, standards, and procedures.
- 5.1.2.7 Review and approve exceptions from TfL OT Security policies, standards, and procedures, where business approval is not sufficient.
- 5.1.2.8 Support TfL readiness to respond to OT security incidents.
- 5.1.2.9 Ensure OT security incidents are reviewed, and any lessons learnt are shared with key stakeholders.



5.2 Business Unit OT Cyber Security Lead

The Business Unit OT Cyber Security Lead is the most senior role for managing OT security within a BU or similar business function.

This role has yet to be defined or agreed within TfL but is shown here as a future aspiration and to maintain consistent numbering between the standard and the guidance. Responsibilities and accountabilities are held in the guidance document ([G1770](#)) until the role is agreed.

The BU Cyber Steering Group could provide a suitable forum for the delivery of the BU's OT cyber security responsibilities.

5.3 The Guiding Mind

The [Guiding Mind](#) triumvirate is an established concept which brings together functions who discharge the financial/strategy, technical assurance and operating/maintain responsibilities for TfL Assets and is suggested as a suitable mechanism for delivering the BU OT cyber security responsibilities.

5.3.1 Purpose

- 5.3.1.1 Ensure that every system or asset is designed, operated, and maintained in a secure manner to reduce the cyber risk to at least a tolerable level for TfL and provide the governance to ensure that the personnel who are responsible for the system or asset discharge their responsibilities correctly.

5.3.2 Accountabilities and responsibilities

- 5.3.2.1 Ensure each System or Asset has a designated System Owner and that the System Owner has received formal notification of their responsibilities.
- 5.3.2.2 Ensure an OT security risk-reduction programme is in place for the System or Asset.
- 5.3.2.3 Ensure OT security is managed throughout System or Asset lifecycle.
- 5.3.2.4 Ensure management of change covers OT security and monitor adherence to this process.
- 5.3.2.5 Ensure OT designs and modifications are secure and in accordance with TfL security standards.
- 5.3.2.6 Approve third party connectivity to OT systems and that risks associated with this are assessed and mitigated.
- 5.3.2.7 Ensure third party connectivity is secure and aligned with TfL security standards.
- 5.3.2.8 Ensure OT security vulnerability intelligence is reviewed, identify appropriate response, and communicated to stakeholders.
- 5.3.2.9 Ensure OT security Incident Response plans are in place and tested.



5.4 System Owner

The System Owner is the single point of accountability for OT Security Governance for the OT Systems or Assets within their area of accountability. They ensure that system custodians execute their responsibilities.

System Owners should be identified who can act as cyber security champions or ambassadors for their system and who can coordinate further and more specialist cyber security activities throughout the operational lifecycle of their system(s).

Where the System Owner is responsible for a System which falls under the NIS Regulations, the additional accountabilities in Section 5.4.4 shall apply.

5.4.1 Purpose

- 5.4.1.1 To be the single point of accountability for OT Security Governance for the OT within their area of accountability or product portfolio.

5.4.2 Accountabilities

- 5.4.2.1 Ensure systems comply with TfL OT security policies, standards and procedures and any exceptions are documented, justified, and approved.
- 5.4.2.2 Ensure that where systems are supported by IT, all relevant IT processes have been completed in accordance with IT policy.

5.4.3 Responsibilities

- 5.4.3.1 Lead OT security risk assessments, including review of the effectiveness of risk-reduction controls.
- 5.4.3.2 Identify and implement approved risk reduction controls.
- 5.4.3.3 Regularly review and approve operational staff, remote TfL and third-party access accounts and associated permissions.
- 5.4.3.4 Establishing physical and logical access control procedures relating to securing OT systems.
- 5.4.3.5 Obtain approval from Head of OT Cyber Security for third party and remote connectivity to OT systems.
- 5.4.3.6 Business owner of firewall rules for firewalls segregating OT systems in their area and Corporate data networks and firewalls within the OT.
- 5.4.3.7 Manage OT security throughout system lifecycle, including design, build, commissioning, operations, and decommissioning, including Management of Change.
- 5.4.3.8 Review Management of Change impacts on OT security, and approve system changes.
- 5.4.3.9 Secure, repair, decommissioning and disposal of OT equipment.



- 5.4.3.10 Manage security concerns for the maintenance of OT including the relationship with third parties and OT suppliers, firmware, software, and services.
- 5.4.3.11 Maintain OT to the level required by the TfL security standards.
- 5.4.3.12 Monitor security to agreed standards for OT systems and ensure this is reviewed routinely.
- 5.4.3.13 Develop, maintain, and test OT security incident response plans.
- 5.4.3.14 Escalate security incidents, risks, or issues in accordance with the established TfL processes.

5.4.4 NIS Accountabilities and responsibilities

- 5.4.4.1 Own the NIS System Cyber Assessment Framework (CAF) and nominate a NIS System Lead(s) to coordinate and complete regular CAF reviews and related activities, including submission.
- 5.4.4.2 Obtains endorsement of NIS System Improvements with stakeholders for the NIS System.
- 5.4.4.3 Agrees NIS System Improvements with risk owners and Competent Authority (DfT).
- 5.4.4.4 Engages with and seeks appropriate Sponsor and Sponsorship for the NIS System Improvements.
- 5.4.4.5 Monitors the progress of NIS System Improvements and regularly reports the KPIs and progress to the Competent Authority (DfT) and the Pan-TfL Cyber and Information Security Steering Group.
- 5.4.4.6 Ensures that the ongoing operational lifecycle NIS requirements are embedded into the operation and maintenance of the NIS System.
- 5.4.4.7 Maintain cyber security risk assessments and appropriate cyber security controls to ensure continued service delivery.
- 5.4.4.8 Is the Single Point of Contact with the Competent Authority (DfT) and TfL Cyber Security for their NIS System.
- 5.4.4.9 Regularly engages and maintains relationship with and acts upon requests by the Competent Authority (DfT) and the NIS Lead Inspector.
- 5.4.4.10 Maintain an effective NIS incident reporting process.

5.5 Delegation of responsibilities below the System Owner

The System Owner can, if appropriate, delegate responsibilities for their systems and suggested roles to support the system owner are contained within the guidance document ([G1770](#)).



5.6 Programme Roles

Programmes or projects which deliver new or upgraded OT Systems or Assets are required to comply with [S1771](#) Operational Technology – Projects and Upgrades and will be expected to include OT cyber security roles, with suggested roles and responsibilities contained in the guidance document ([G1770](#)).

5.7 TfL Employees and Partners

Security is everyone's responsibility therefore staff and partners shall undertake their roles with cyber security in mind.

6 Risk Management

Risk management is essential to maintain the safety, reliability, availability, maintainability, confidentiality, and integrity of a system and to reduce the likelihood and impact of a cyber security incident.

6.1 Risk Management Process

The risk management process is broken down into the following stages:

6.1.1 Risk Identification and Assessment

- 6.1.1.1 Each system shall be subject to a risk identification and assessment process to determine its cyber security risk and to identify any additional controls required above that of the established minimum-security baseline.
- 6.1.1.2 All Cyber Security Risks shall be identified, assessed, managed, and treated according to TfL's Enterprise Risk Management policy ([P021](#)), TfL's Enterprise Risk Management Framework ([R0651](#)), TfL's Enterprise Risk Assessment Matrix ([R0650](#)) and TfL's Enterprise Risk Management Procedure ([PR0633](#)).
- 6.1.1.3 Cyber security risks shall be considered at all three levels of TfL's Enterprise Risk Management Hierarchy and in particular:
 - L2 Tactical Project risk
 - L2 Tactical Operational / Asset Risk
 - L1 Strategic business area risk

- 6.1.1.4 Risks shall be owned and managed at the business level shown in the table below:

Risk Level	Governance / Ownership
L0 (Board / Enterprise)	TfL Executive
L1 (Operational)	Business Unit
L2 (Tactical)	Project / Product / System / Asset

Table 1 - Aligning Risk Levels to Business Ownership

- 6.1.1.5 A cyber security risk register shall be created and maintained for each system.



- 6.1.1.6 A risk owner shall be designated to own and manage the cyber security risk for the system or asset they are responsible for.
- 6.1.1.7 A risk assessment owner shall be identified and assigned to undertake a cyber security risk assessment. In most cases, whilst the risk owner will be responsible for the risk assessment, it is expected that they will delegate the actual completion of the risk assessment to suitably experienced and qualified personnel.
- 6.1.1.8 Risk owners shall ensure that cyber security risks are identified, reported, and managed.
- 6.1.1.9 A cyber security risk assessment shall be undertaken, or current risks re-assessed:
- upon changes to system configuration
 - upon non-compliances to cyber security standards
 - upon system updates, patching and upgrades
 - upon completion of cyber security testing, such as vulnerability assessments and penetration tests
 - upon notification of arising or modified cyber security threats or vulnerabilities to the systems
 - upon the transition into operation
 - upon the decommissioning of the system
 - upon violation of the Safety Case(s) for the system
 - upon hardware and software obsolescence constraints on the system
 - upon findings or lessons learnt from the continuous operation of cyber security detection tools or cyber security incidents.

Whilst risks should be owned and managed at the appropriate business level, the governance process, through appropriate steering and working groups, must maintain visibility of risks at all levels to assure they are being managed correctly and maintain oversight of common vulnerabilities or aggregated risks.

For example, a technical vulnerability affecting a system component should be identified as a L2 risk by the system owner, but if that component is used across multiple systems, the risk could aggregate to a L1 risk for a business unit and further aggregate to a L0 risk for TfL if that component is used across business units.

6.1.2 Risk analysis

- 6.1.2.1 Each system shall be subject to a risk assessment to determine its cyber security risk and to identify any mitigation controls and actions.
- 6.1.2.2 The risk register shall record the event, cause, classification, likelihood, impact, and consequence of the risk.



6.1.3 Risk Evaluation

6.1.3.1 Cyber security risks shall be evaluated according to the risk tolerability.

TfL's cyber security risk tolerance is: RISK AVERSE

6.1.3.2 Risk adverse indicates a preference to avoid risk or keep it as low as reasonably practicable.

6.1.3.3 The cyber security risk shall be scored from 1-25, with 1 being very low and 25 being very high. The cyber security risk is made up of an Impact score from 1-5 and a likelihood score from 1-5 with 1 being very low and 5 being very high.

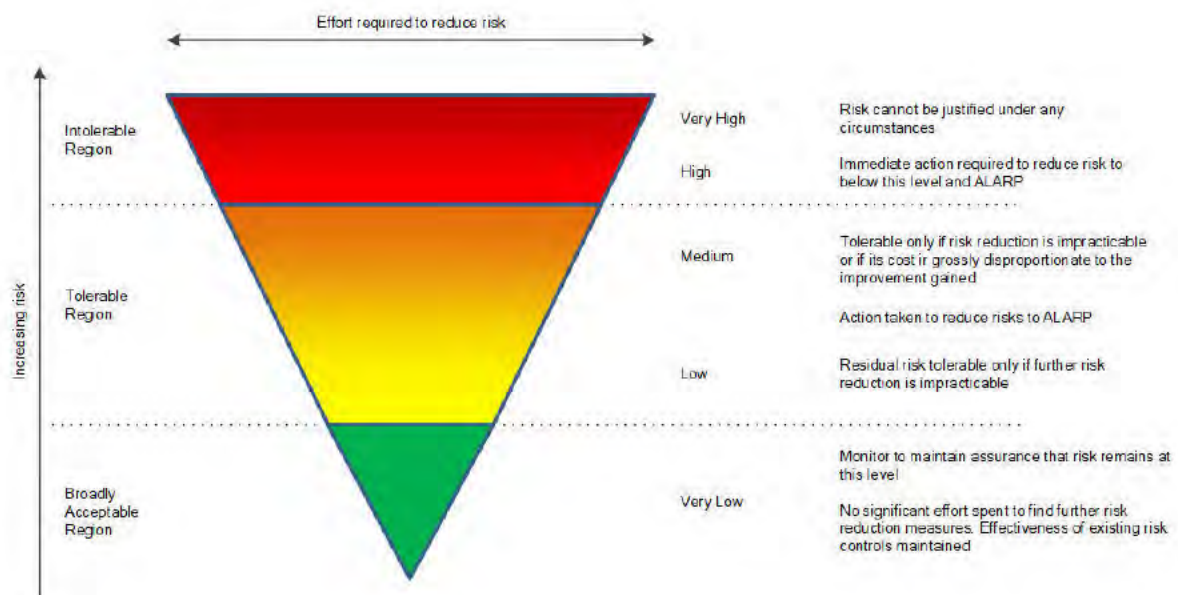
6.1.3.4 The cyber security risk calculation and Probability Impact Diagram is as follows:

Likelihood	VERY HIGH (Frequent)	Medium (11)	Medium (16)	High (20)	Very High (23)	Very High (25)
	HIGH (Probable)	Low (7)	Medium (12)	High (18)	High (21)	Very High (24)
	MEDIUM (Occasional)	Low (4)	Low (8)	Medium (13)	High (19)	High (22)
	LOW (Remote)	Very Low (2)	Low (5)	Low (9)	Medium (14)	Medium (17)
	VERY LOW (Improbable)	Very Low (1)	Very Low (3)	Low (6)	Low (10)	Medium (15)
		VERY LOW (Negligible)	LOW (Lower Marginal)	MEDIUM (Upper Marginal)	HIGH (Critical)	VERY HIGH (Catastrophic)
Impact						

6.1.3.5 Cyber security risks and their tolerability are to be graded as:

Risk	Risk Tolerance	Risk Tolerance Description
Very High	Intolerable	Risk cannot be justified under any circumstances. Immediate action required to reduce risk to below this level and ALARP
High	Intolerable	Risk cannot be justified under any circumstances Immediate action required to reduce risk to below this level and ALARP
Medium	Tolerable	Tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained The risk should be reduced using best practise. Has best practise been met?
Low	Tolerable	Residual risk tolerable only if further risk reduction is impracticable. The risk should be reduced using best practise. Has best practise been met? Action taken to reduce risks to ALARP
Very Low	Broadly Acceptable	Monitor to maintain assurance that risk remains at this level No significant effort spent to find further risk reduction measures. Effectiveness of existing risk controls maintained

6.1.3.6 Broad responses to risks in each tolerability group are indicated in the diagram below.



6.1.4 Risk Treatment

6.1.4.1 Cyber security risks shall be classified and treated by:

- Accept/tolerate
- Avoid
- Reduce/treat
- Share/transfer

6.1.4.2 The risk owner shall ensure that a cyber security risk treatment plan is defined and executed.

6.1.4.3 The cyber security risk treatment plan shall record:

- the identified risks
- parties responsible for managing the risk
- prioritisation of the risk
- the mitigating controls and actions required to manage the risk
- a target date for completing the risk treatment

6.1.4.4 The cyber security risk treatment plan shall drive a set of additional security requirements. These security requirements are to address the risks in which they are to be prioritised, communicated to accountable individuals, and managed to closure.

6.1.4.5 Technical security controls shall be prioritised over non-technical security controls when determining additional security requirements.

6.1.4.6 To achieve defence in depth and to remove a single point of security failure, multi-layered controls should be applied for each risk where practicable.

6.1.4.7 Risk owners shall ensure remediation activities are undertaken, that appropriate security controls are implemented and actions to treat and reduce the residual risk to an acceptable level are completed in accordance with the cyber security risk tolerance.

6.1.4.8 Additional remediation activities and security controls shall not be to the detriment of a safety function.

Cyber security risk management needs to consider the Impact with regards to Safety and Reliability and Maintainability (RAM). A cyber security risk could potentially be the cause of a Safety Hazard or compromise RAM performance targets. Cyber security risks need to be analysed regarding Safety Hazards and RAM performance targets to ensure that Safety and RAM is not affected.

If there is an impact to Safety or RAM, then alternative cyber security controls may be required to mitigate or manage this to appropriate levels. Safety and RAM subject matter experts should be consulted as part of risk management.



6.1.5 Risk Monitoring, Recording and Reporting

- 6.1.5.1 A risk register shall be implemented to record, manage, and maintain cyber security risks. For new or updated systems, this shall be a project responsibility and for existing systems, this shall be a system owner responsibility.
- 6.1.5.2 For systems handed over into operation, project risk registers with residual cyber security risks shall be handed over and accepted by an appropriate risk owner to be managed as operational risks.
- 6.1.5.3 Risk owners shall undertake periodic and regular cyber security risk evaluation, at least on an annual basis, and ensure that cyber security risks are assessed and managed throughout the system lifecycle, from concept to disposal.
- 6.1.5.4 Risk owners shall undertake periodic and regular evaluations of their cyber security risk treatment plans.
- 6.1.5.5 Risk owners shall report cyber security risk as part of normal business risk reporting processes and structures.
- 6.1.5.6 Risk owners shall make cyber security risk assessments and risk treatment plans available to applicable governance and assurance bodies.

6.1.6 Continuous Verification and Validation

- 6.1.6.1 Yearly cyber security technical reviews and assessments assuring the effectiveness of cyber security controls shall be undertaken. This coordination of this for new or updated systems shall be a project responsibility and for existing systems shall be a system owner responsibility.
- 6.1.6.2 The technical reviews and assessments if necessary, shall include any engagement required with independent parties.
- 6.1.6.3 The cyber security periodic technical reviews and assessments shall extend to:
 - Assessment of the operational and maintenance cyber security processes and procedures
 - Configuration review of the technical cyber security controls implemented on the System
 - Tabletop and paper-based assessments of incident response and recovery
 - Vulnerability and penetration testing of external interfaces to the system
 - Vulnerability and penetration testing for internal scenarios which are classified as high-security risk
- 6.1.6.4 Penetration testing shall be undertaken by a competent independent third party.
- 6.1.6.5 Technical reviews and assessments shall be recorded and stored.
- 6.1.6.6 Technical reviews and assessments shall be executed in such a manner that the safety, reliability, functionality, and performance functions of the system is not



compromised (e.g., reference system with the same setup or engineering hours providing that fit for purpose resiliency arrangements are in-place).

7 Supply Chain Management

TfL must ensure that any commercial activity includes appropriate cyber security considerations which are aligned to the level of risk associated with the system or service being procured.

7.1 Third Party Risk

The security of TfL's OT can be put at significant risk by third parties, e.g. vendors, integrators, support organisations and other entities in the supply chain and therefore warrants considerable attention. Technologies that allow greater interconnectivity, such as remote access or internet connectivity, bring new threats from outside TfL. Third parties are often considered a weak link and must therefore be engaged as part of the OT security programme at the earliest stage and steps should be taken to reduce the associated risk.

7.1.1 Procurement Language

- 7.1.1.1 A high-level assessment of the security of potential third parties shall be undertaken using a supplier assessment questionnaire as part of the Selection Questionnaire stage of a procurement.
- 7.1.1.2 A risk-based assessment of the security of potential third parties shall be undertaken using a supplier assessment questionnaire as part of the Invitation to Tender questionnaire stage of a procurement.
- 7.1.1.3 Procurement contracts shall include a Cyber Security Management Schedule that establishes a common set of security obligations on the third party.
- 7.1.1.4 The Cyber Security Management Schedule shall include requirements for:
 - Third parties to incorporate appropriate anti-malware protection within their OT systems.
 - Third parties to establish an effective software patching process.
 - Third parties to undertake hardening procedures for the OT system in operation.
 - Third parties to identify all component technologies (e.g., databases, open-source software) used within the OT system to ensure that all vulnerabilities are managed.
 - Third parties to undertake regular security reviews and audits
 - Third parties to implement incident response and recovery
- 7.1.1.5 Procurement contracts shall include applicable cyber security standards, cyber security requirements and information classification processes as determined by the services procured and the relevant clauses of the Projects and Upgrades, Operations and Maintenance and Governance Cyber Security Standards.



- 7.1.1.6 Procurement contracts shall require third parties to deliver and implement a Cyber Security Management Plan.
- 7.1.1.7 Third parties shall undertake the obligations as determined in the Cyber Security Management Schedule as well as applicable cyber security standards and requirements as determined by relevant clauses of the Projects and Upgrades, Operations and Maintenance and Governance Cyber Security Standards.
- 7.1.1.8 Cyber security obligations shall be implemented throughout the supply chain and includes principal contractors and sub-contractors.
- 7.1.1.9 A full understanding of the supply chain shall inform the assessment of the cyber security risks to the supply chain, which shall be understood, documented, and controlled.
- 7.1.1.10 Shared and transferred cyber security accountabilities and responsibilities between TfL and the supply chain shall be understood and documented.
- 7.1.1.11 The right to review or audit a third party to verify activities related to their cyber security management plan shall be included.

7.1.2 Supply Chain Assurance

- 7.1.2.1 Third parties are to be held to account for their obligations as determined in the Cyber Security Management Schedule as well as applicable cyber security standards and requirements as determined by relevant clauses of the Projects and Upgrades and Operations and Maintenance Cyber Security Standards.
- 7.1.2.2 The delivery of the third party's cyber security obligations are to be assessed on an ongoing regular basis, no less than once a year.
- 7.1.2.3 Supply chain risks shall be understood, managed, and assured.
- 7.1.2.4 A list of third parties that supply and support OT systems shall be maintained. This list can be derived from many sources including procurement and internal knowledge and should, at the very least, contain information on:
 - What the system is
 - The system owner
 - Current versions of hardware and software
 - Criticality
 - Location
 - Inherent Protection (air-gapped, firewalled, IDS/IPS, etc).
- 7.1.2.5 Where third parties are associated with an item in the inventory this shall be determined and recorded.

It may be that an inventory item is associated with several different third parties as outlined below, in which case, the following questions should be asked:



- Who is part of the supply chain and what processes / activities are they involved in?
- Who is the overall system vendor; are they supported by sub-system vendors and which sub-contractors are involved?
- Who is the service provider and what service level agreements exist?

8 Training and Awareness

Security is everyone's responsibility therefore staff and partners require an understanding of basic cyber security principles as well as how to undertake cyber security activities related to their role.

8.1 Training and Awareness Approach

Employees and partners shall undertake core cyber security awareness as well as cyber security awareness and training appropriate to their role and the activities that they undertake.

8.1.1 Cyber Security Training

- 8.1.1.1 Staff and partners that undertake core cyber security activities, are in higher risk or sensitive roles or have direct controlled or uncontrolled management access to assets shall undertake role specific cyber security training.
- 8.1.1.2 The business unit shall identify role specific cyber security training needs and implement training to meet those needs.
- 8.1.1.3 The business unit shall review role specific cyber security training needs on a regular basis, no less than once a year, to ensure that staff and partners receive effective, appropriate, and relevant training.
- 8.1.1.4 The business unit shall update role specific cyber security training as necessary, to account for new changing threats and vulnerabilities.
- 8.1.1.5 System users shall be trained upon the processes and procedures as detailed within the Projects and Upgrades Standard and Operations and Maintenance Standard before first undertaking the activity and refreshed on an ongoing regular basis, no less than once a year.
- 8.1.1.6 Records of employee cyber security training and schedules for training shall be tracked and maintained.

8.1.2 Cyber Security Awareness

- 8.1.2.1 Staff and partners need to know what to do to prevent successful cyber-attacks and what to do in the event of a security event or incident. Everybody must understand their role and the actions they should take to prevent or respond to an incident.
- 8.1.2.2 Core cyber security awareness shall be undertaken by all staff and partners upon joining and on an ongoing regular basis, no less than once a year.



- 8.1.2.3 Staff and partners that undertake core cyber security activities, are in higher risk or sensitive roles or have direct controlled or uncontrolled management access to assets shall undertake role or system specific cyber security awareness.
- 8.1.2.4 Role or system specific cyber security awareness shall be undertaken upon joining and on an ongoing regular basis, no less than once a year.
- 8.1.2.5 Role or system specific cyber security awareness needs shall be identified and undertaken by the business unit.
- 8.1.2.6 Role or system specific cyber security awareness needs shall be validated on a regular basis, no less than once a year, to ensure that staff and partners receive effective, appropriate, and relevant awareness.
- 8.1.2.7 Role or system specific cyber security awareness shall be revised, as necessary, to account for new changing threats and vulnerabilities.
- 8.1.2.8 Records of employee cyber security awareness shall be tracked and maintained.
- 8.1.2.9 Staff and partners shall be made aware of how to report a cyber security incident.
- 8.1.2.10 Staff and partners shall be made aware of local procedures and processes, including information classification, handling, and sharing requirements ([S1782](#)).

9 Supporting Information

9.1 Background

Cyber security should be considered as an integral part of any review for any OT and where possible should be integrated into existing safety, environmental, operational or risk considerations. This should reflect that cyber could be a potential cause of a failure and needs to be captured as part of the response or recovery process, rather than a separate consideration.

9.2 Customer Considerations

Whilst cyber security for OT should not be at the forefront of customer considerations, it should form part of the wider safe, secure, and reliable message.

10 Guidance

For further advice and guidance in support of this Standard, contact the Cyber Security team CyberSecurityGRC@tfl.gov.uk

11 Person accountable for this document

Name	Job title
Paul Richardson	Cyber Security Assurance Manager



12 Definitions

Term	Definition	Source
Operational Technology	A collection of personnel, processes, hardware and software that can affect or influence the safe, secure and reliable operation of a physical process or asset.	Jargon Buster
Business Unit	An identified management unit within TfL operating within an agreed budget, either as a cost or profit centre.	Jargon Buster

13 Abbreviations

Abbreviation	Meaning
ALARP	As low as reasonably possible
BU	Business Unit
CAF	Cyber Assessment Framework
CCTV	Close Circuit Television
CISO	Chief Information Security Officer
CISSG	Cyber and Information Security Steering Group
CISWG	Cyber and Information Security Working Group
CSAC	Cyber Security Assurance Case
HR	Human Resources
IR	Incident Response
IT	Information Technology
NCSC	National Cyber Security Centre
NIS	Network and Information Systems (Regs)
OEM	Original Equipment Manufacturer
OT	Operational Technology
PLC	Programmable Logic Controller
RAM	Reliability and Maintainability
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SG	Steering Group
SIS	Safety-Instrumented System
SSG	Security Steering Group

14 References

Document no.	Title or URL
P006	Operational Technology Cyber Security
P007	Operational Technology Cyber Security - Governance
P008	Operational Technology Cyber Security - Projects and Upgrades
P009	Operational Technology Cyber Security - Operations and Maintenance
R1770	Operational Technology Cyber Security - Framework



Document no.	Title or URL
S1771	Operational Technology Cyber Security – Projects and Upgrades
S1772	Operational Technology Cyber Security – Operations and Maintenance
G1770	Operational Technology Cyber Security – Governance.
S1641	Concessions to standards (LU)
P021	Enterprise Risk Management policy
R0650	Enterprise Risk Assessment Matrix
R0651	TfL's Enterprise Risk Management Framework
PR0633	TfL's Enterprise Risk Management Procedure
S1782	Information Security Classification
	SICS Framework
	CISSG Terms of Reference
	CISWG Terms of Reference
	NCSC CAF
HSE OG86v2	Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2
IEC 62443-2-1	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program
IEC 62443-3-3	Industrial communication networks – Network and system security Part 3-3: System security requirements and security levels
NIST SP800-82	Guide to Industrial Control System (ICS) Security
EN50128	Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems
EN50129	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
EN50159	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

15 Document history

Issue no.	Date	Changes	Author
A1	December 2021	New standard published in accordance with Change Request CR-15283.	Tim Parker



Standard

S1771 A1

Operational Technology Cyber Security - Projects and Upgrades

Contents

1	Purpose	3
2	Scope	3
2.1	Operation Technology (OT) definition	3
2.2	Examples	4
3	Requirements	5
3.1	Protecting against cyber attack	6
3.2	Detecting cyber security events	6
3.3	Minimising the impact of cyber security incidents	7
4	OT Project Lifecycle	7
4.1	OT Project Lifecycle	7
4.2	Good Practice Principles	8
4.3	OT Project Lifecycle Requirements	8
4.4	The Purdue model and Secure OT Design	15
5	Protecting against cyber attack	15
5.1	Identity and access control	15
5.2	Data Security	21
5.3	Personnel Security	24
5.4	Physical Security	26
5.5	Network Security	28
5.6	System Security	32
5.7	Secure Management	41
6	Detecting cyber security events	41
6.1	Security Monitoring	42
7	Minimising the impact of cyber security incidents	46
7.1	Incident response and recovery planning	46
7.2	Backups	48
7.3	Incident lessons learned	48
8	Supporting Information	49
8.1	Background	49
8.2	Customer Considerations	49

Printed copies of this document are uncontrolled.
Page 1 of 51



9 Guidance 49

10 Person accountable for this document 49

11 Definitions 49

12 Abbreviations..... 50

13 References 50

14 Document history 51



1 Purpose

This standard describes the cyber security requirements relating to the design, build, testing, implementation and handover to operations for all new projects and system upgrades comprising or containing Operational Technology (OT) in Transport for London (TfL).

2 Scope

This standard applies to TfL staff and partners with responsibility for designing and implementing OT throughout the lifecycle of any project relating to OT.

2.1 Operation Technology (OT) definition

Operational Technology is a collection of personnel, processes, hardware, and software that can affect or influence the safe, secure, and reliable operation of a physical process or asset.

These include, but are not limited to:

- Signalling for rail, road and marine transport, train management, Supervisory Control and Data Acquisition (SCADA), building management and access control, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), intelligent electronic devices, networked electronic sensing and control, and monitoring and diagnostic systems.

In this context, process control systems include basic process control system and Safety-Instrumented System (SIS) functions, whether they are physically separate or integrated.

- Associated information systems such as advanced control, dedicated equipment monitors, graphical interfaces, process historians, and plant information management systems.
- Associated internal, human, network, or machine interfaces used to provide monitoring, control, and safety operations functionality.

As an owner and operator of physical transport assets, TfL has an extensive estate of OT systems and devices across a wide range of its underground and surface operations.

There are OT systems which are clearly OT such as traction power, tunnel ventilation, fire detection, and systems which are clearly Information Technology (IT) such as Human Resources (HR) and email. However, there are systems where the distinction is not as clear, such as CCTV and ticket barriers.

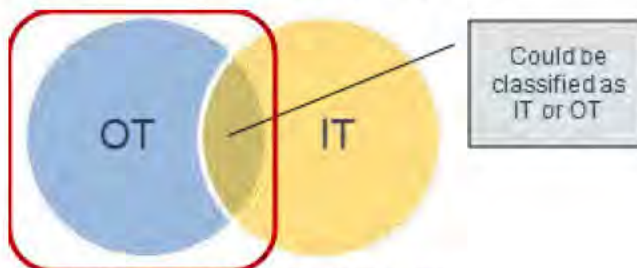


Figure 1 Operational Technology systems scope

2.2 Examples

In this section we provide some examples of systems which may or may not be considered or recognised as OT.

2.2.1 Example OT systems

Examples of OT systems installed in London Underground and Surface Transport that are clearly OT include, but is not limited to:

- Power management systems (traction and general power)
- Energy monitoring
- Signalling systems
- Road traffic signals
- Rolling stock
- Communication networks used by OT (e.g. Surface WAN/Connect/Station LAN)
- Control and information systems
- Track systems
- Station systems (e.g. escalator and elevator control)
- Fire detection and suppression systems
- Civil Systems / Tunnel Systems
- Building management systems and building automation systems
- Heating, ventilation and air conditioning (HVAC) systems
- Security and access control systems (e.g. swipe card or key fob)

2.2.2 Example of systems which can be OT or IT

Some systems may be defined as OT or IT, which is usually dependent on the context. To determine if the system is OT or IT, refer to the definition in section 2.1 above and apply the test of whether the systems “can affect or influence the safe, secure, and reliable operation of a physical process or asset.” If the answer to this is “Yes”, then the system is OT, otherwise it is IT. If the answer is not clear, then refer to the supporting bullet points in the definition to for tests, such as whether the system provides “sensing” or “control”, for example.

Some common edge cases which may be classified as OT or IT are given below:

CCTV and One Person Operation (OPO) CCTV – If the CCTV system (cameras and recorders) are networked then they would come under the definition as “networked electronic sensing” and “monitoring” in the definition above. CCTV which is monitoring an area (e.g. an underground station platform) controlled by other OT (e.g. BMS or signalling) should be classified as OT. CCTV which is not used directly to deliver or support delivering a service (e.g. Head Office CCTV for security monitoring) should be classified as IT.



Lighting controls – Simple manual lighting controls are unlikely to be OT. Automated, remotely controlled or monitored lighting control systems for stations, road and rail tunnels, ferry terminals, are likely to be OT as they can affect the reliable operation of the lighting and of services.

HVAC – Reasonably modern HVAC systems in stations, tunnels and buildings (e.g. Victoria coach station) will have a control system which may be linked into a BMS. They may also have remote access from a facilities management and/or maintenance company.

Ticket barriers – A particular physical access control system which not only has card readers and controllers (OT) but will also link to ticketing systems which will be in the IT network.

Timetabling – Scheduling bus and train services with the timetabling system (IT) may need to interface to other OT systems, such as train management systems. The timetabling system would not be classified as OT because it does “affect or influence the safe, secure, and reliable operation” of services.

2.2.3 Alignment to Purdue Model

A complementary approach to determining if a system should be defined as OT or IT is to refer to the Purdue Model, [G1771](#) Section 4.4.1 refers, where OT systems and services sit in Levels 0 to 3 in the Model and IT systems and services sit in Levels 4 and 5 of the Model.

3 Requirements

This standard details the mandatory requirements for OT cyber security through Projects and Upgrades and is aligned to the Network and Information Systems (NIS) Regulations (2018) and the International Electrotechnical Commission IEC 62443 series of standards for OT cyber security, in particular IEC 62443-3-3 system security requirements and security levels. It forms part of a wider framework of standards and guidance ([R1770](#)) for OT cyber security in TfL. The standard should be read in tandem with the associated guidance ([G1771](#)).

Each system must be subject to a risk assessment to determine its cyber risk and to identify any additional controls required above that of the established minimum-security baseline or concessions which might be necessary where the minimum baseline cannot be met.

Notwithstanding this, the minimum cyber security baseline established within this standard is the set of minimum cyber security requirements for ALL new or upgraded OT which support TfL services.

The baseline is intended to prevent the unauthorised disclosure of information to an entity actively searching for it using simple means with low resources, generic skills, and low motivation. These requirements are applicable to all OT assets including, but not limited to, Intelligent Electronic Devices, RTUs, Microcontrollers, PLCs, Sensors, Actuators, Servers, Workstations, and Network Devices.

Concessions or non-compliance to the requirements established within this standard must have appropriate mitigating controls implemented and follow the formal engineering concession process. Any risks arising from the concession must have



been registered in the project risk register, which is then transferred to the system owner and maintained as the system risk register.

The standard is intended to direct staff and partners working for TfL to understand and adopt the necessary steps to protect against cyber threats, detect a cyber incident and respond to a cyber incident when designing and implementing OT which supports the delivery of TfL services safely and reliably.

Not all elements of the standard are solely the responsibility of the project team responsible for the respective OT system; in some areas, TfL will have to have organisational processes or shared services, such as monitoring, in place to support these requirements and the OT systems will have to have the capabilities to apply the requirements.

For example, if an individual moves role, there needs to be recognition at an organisational level that their access privileges must be reviewed, but the system must have appropriate mechanisms to ensure access controls can be enforced and updated.

It is important to note that this standard closely mirrors Operational Technology Cyber Security – Operations and Maintenance ([S1772](#)) and the two documents have been written in parallel.

The key difference is that for Operations and Maintenance the emphasis is on **operating** and **supporting** the OT securely and according to established process to limit the likelihood and impact of a cyber incident, so the broader guidance remains to give context and build understanding of why the security controls are important. For Projects and Upgrades, the emphasis is more focused on **designing** and **implementing** the OT in a secure way, such that the cyber risk is mitigated as far as practicable and that the controls are appropriate to the risk.

Cyber security considerations or controls are grouped according to the following security principles and the components of each phase are explained in the following sections.

3.1 Protecting against cyber attack

The requirement is that TfL and partners will have proportionate security measures in place to protect TfL services and systems from cyber-attack.

The underlying principle is that TfL defines, implements, communicates, and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of TfL services.

3.2 Detecting cyber security events

The requirement is that TfL and partners will have the capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, TfL services.

The underlying principle is that TfL monitors the security status of the networks and systems supporting the delivery of TfL services to detect potential security problems and to track the ongoing effectiveness of protective security measures.

3.3 Minimising the impact of cyber security incidents

The requirement is that TfL and partners will have the capabilities to minimise the impact of a cyber security incident on TfL services, including the restoration of those services where necessary.

The underlying principle is that TfL has well-defined and tested cyber security incident management processes in place, that aim to ensure continuity of essential services in the event of an incident affecting systems or services.

4 OT Project Lifecycle

All OT projects and operational systems must undertake cyber security activities and implement cyber security controls throughout both the project lifecycle as well as the operational lifecycle. For the purposes of this standard, it is necessary to manage cyber security throughout the entire OT project lifecycle which consists of four key phases: design, build, operation, and decommissioning. This is referred to as a “secure by design” approach.

4.1 OT Project Lifecycle

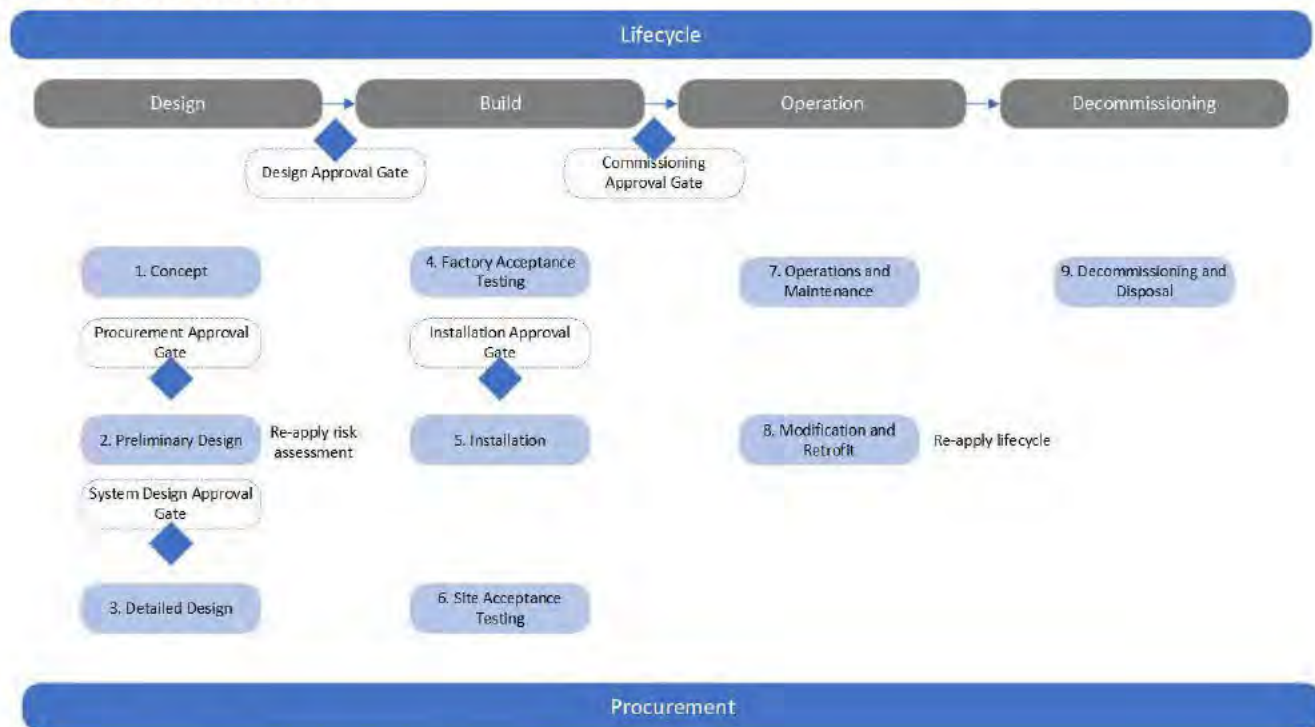


Figure 1 - OT Lifecycle

Implementing security protection measures into OT can be more difficult and costly once systems have been built and deployed. Even more important is that bolting on security measures to either in-service OT, or late in the development cycle of that OT, is often less effective than building them in at the beginning. Dealing with security risks by integrating protection measures into the OT early in its lifecycle is more effective, avoids overruns, is usually less costly and can often be a business enabler.

4.2 Good Practice Principles

To effectively manage the OT lifecycle within the organisation there are five good practice principles which bridge the gap between the lifecycle and cyber security frameworks and bring manageable actions to supporting the lifecycle.

The good practice principles are to:

- Ensure regulatory and security requirements are included in procurement and penalties are flowed down
- Ensure OT systems are secure by design
- Manage security through OT system construction
- Manage operational security
- Managing security risks during decommissioning and disposal.

Further detail for each principle is contained in the supporting guidance document, [G1771](#) Operational Technology Cyber Security – Projects and Upgrades.

4.3 OT Project Lifecycle Requirements

The project must establish and undertake the following activities during the OT project lifecycle:

4.3.1 Concept Phase

Security Awareness Training

- 4.3.1.1 All staff involved in the procurement, development and deployment of OT assets must receive appropriate cyber security awareness training. Staff directly involved in the cyber security engineering of OT assets must be able to demonstrate competency in this domain.

Risk Assessment:

- 4.3.1.2 The project must undertake a cyber security risk assessment to assess the cyber security risk of a system and to determine additional cyber security controls above that of the minimum-security baseline requirements established within this standard.
- 4.3.1.3 Following the risk assessment, the project must develop a cyber security risk treatment plan containing a prioritised list of cyber risks and controls to eliminate, mitigate or contain each risk. This plan must be updated throughout the life of the project and form part of the handover documentation.
- 4.3.1.4 The risk assessment and ongoing management shall be conducted according to [S1770](#) Operational Technology Cyber Security – Governance.

Threat Modelling:

- 4.3.1.5 The project must undertake assessment of cyber threats to inform the cyber security risk of a system.
- 4.3.1.6 This should consider the full range of attacker types, their associated motivations, potential access vectors, attack methodologies and the impacts of any attack on safe operations. MITRE ATT&CK for ICS is a possible tool to support this analysis.



4.3.2 Preliminary Design Phase

Security Requirements:

- 4.3.2.1 The project must incorporate the minimum cyber-security baselines requirements from this standard into the project requirements. This shall form the basis of the cyber security plan for the project.
- 4.3.2.2 The project may have to include additional requirements, such as those arising from the risk assessment or aligned to increased controls for safety critical systems into the project requirements.

Preliminary Design:

- 4.3.2.3 The project must verify and validate that the project cyber security requirements are addressed within the preliminary design.
- 4.3.2.4 As a minimum, the following documentation shall be produced during the preliminary design phase:
 - High Level or Concept Design
 - Draft Network specifications and proposed configurations
 - Draft interface specifications
 - Draft cyber security plan
 - High Level Security Architecture.
- 4.3.2.5 The project shall expect the level of detail in the design and architecture to include all the security controls to be implemented along with an inventory of all the communication flows and interfaces of the OT assets and the system segmentation, in the form of a Security Zones proposal, to demonstrate a planned intent to satisfy all the cyber security requirements.
- 4.3.2.6 The preliminary design must also demonstrate that functional and operational objectives of the system are capable of being met.

4.3.3 Detailed Design Phase

Detailed Design

- 4.3.3.1 The project must verify and validate that the project cyber security requirements are addressed within the detailed design.
- 4.3.3.2 The project must use the preliminary design to undertake the development of a detailed design able to satisfy all the cyber security requirements.
- 4.3.3.3 The project must adopt appropriate secure coding practices, including, but not limited to OWASP and Top 20 PLC Secure Coding Practices.
- 4.3.3.4 As a minimum, the following documentation shall be produced:
 - Low Level or Detailed Design
 - Network specifications and configurations
 - Network traffic profile and expected communication paths
 - Interface specifications



- Cyber security plan
- Security Architecture, including Zone and Conduit model.

4.3.3.5 The detailed design process must:

- Define, develop, document, and validate the required cyber security design
- Justify interfaces between OT assets assigned to different security Zones and domains of trust
- Confirm that any interfaces within a security Zone do not result in a reduction of the cyber security for assets within the Zone
- Confirm that any interfaces between security Zones do not result in a reduction of the overall cyber security of the Zones
- Confirm that any interfaces between OT assets and external domains of trust do not result in a reduction of the cyber security for the asset or system.

4.3.3.6 Once the detailed design has been established, verification must be performed to ensure that all the cyber security requirements have been met.

4.3.3.7 The verification process must include a review of:

- Any deficiencies in the design that might allow inadvertent, unintended, or unauthorised access or modifications to OT assets that might degrade the safety, reliability, integrity, or functionality during operation.
- Ineffectiveness of safety functions relating to OT assets in the presence of undesired cyber behaviour from connected systems.

4.3.3.8 Any observed deficiencies from the verification process must be corrected by revising either the cyber security requirements or the design to resolve the deficiency. The results of the verifications shall be documented in a design output document, such as the design review report.

Incident Management

4.3.3.9 There must a defined process to effectively manage cyber security events during the project lifecycle with the objective of minimising impacts on the project and maintaining or restoring normal operations.

4.3.3.10 Formal event reporting and escalation procedures must be established.

4.3.3.11 There must be procedures in place to identify cyber security events and respond to them.

Secure Development and Testing Environments

4.3.3.12 The project must review details of development and testing processes including policies, procedures, practices, and technical environments to ensure they are cyber-secure (see 4.3.3.13).

4.3.3.13 The project must confirm the acquisition and handover of secure OT assets which are free of malware, vulnerabilities or weaknesses resulting from insecure product development and/or testing processes.

4.3.3.14 There must be a secure development and testing framework which must:

- Ensure that secure development and testing environments (including tools and development facilities) are established.
- Ensure that secure development and testing processes are established and applied.
- Ensure that all the applicable controls defined in this standard are implemented, providing evidence of their implementation.
- Document standards, coding practices, technical details of the development and testing environments, maintenance plans, secure development and testing methodologies, and product benchmarking against well-defined standards and frameworks.
- Identify countries of origin of the products used and where their assembly, development and testing are undertaken
- Demonstrate quality assurance
- Demonstrate contingency planning for assets during product development and testing
- Ensure that software maintenance plans, including software recovery information, are available during the contract lifecycle and afterwards for maintenance.

Continuous Verification and Validation

- 4.3.3.15 Each security control of the OT assets must be regularly validated by test or demonstration during development and commissioning to ensure that it does not degrade the following to an unacceptable level:
- Safety
 - Functionality
 - Performance.

4.3.3.16 Testing of OT assets must be conducted fully and in multiple stages to ensure correctness in the final environment.

4.3.3.17 All verification and validation tests must be documented.

4.3.4 Factory Acceptance Testing Phase

Factory Acceptance Testing

4.3.4.1 The project must ensure that functional testing of the cyber security controls is completed on the system within the constraints of a factory setting.

4.3.4.2 The project must ensure that penetration testing is completed on the system during Factory Acceptance Testing (FAT).

Factory and Site Acceptance Testing Requirements

The following requirements must be met at both the FAT and Site Acceptance Testing (SAT) stages of delivery:

4.3.4.3 The project must receive documentation to confirm that all applicable manufacturer updates and patches have been installed prior to testing.



- 4.3.4.4 The project must receive documentation to confirm that all applicable requirements have been met prior to testing.
- 4.3.4.5 The project must receive documentation to confirm the absence of vulnerabilities, or the effectiveness of implemented mitigation and containment controls.
- 4.3.4.6 The project must receive documentation to confirm the absence of malware prior to testing.
- 4.3.4.7 The project must confirm that the testing is conducted across a fully representative sample of all types of OT assets present in the system throughout the testing period.
- 4.3.4.8 The project must confirm that the system remains free of malware throughout the testing process.
- 4.3.4.9 The project must confirm that the system performs as expected in terms of safety, function, and performance under cyber-attack scenarios.
- 4.3.4.10 The project must specify that penetration tests are conducted and reported according to NIST Special Publication 800-115 (SP 800-115). Furthermore, the penetration tests must be conducted by an independent specialist testing company.
- 4.3.4.11 The project must receive updated cyber security risk assessments based on the findings of the completed penetration test and implement or update risk treatment plans where necessary.
- 4.3.4.12 The penetration test scenarios must be defined by the independent specialist testing company, with input from the project, and agreed with the project in advance. Suppliers may be involved in the development of test scenarios.

4.3.5 Installation Phase

Training

- 4.3.5.1 The project must ensure that cyber security training is undertaken by operational and maintenance staff relating to the cyber security requirements, controls, and deliverables of the system.

Installation

- 4.3.5.2 The installation must be planned and conducted in accordance with the overall project cyber security plan.
- 4.3.5.3 The project must ensure that OT assets are protected during installation activities and that the Installation Work Plan highlights specific cyber security risks of the installation process, with the actions taken to reduce them to acceptable levels.
- 4.3.5.4 The project must ensure there is a plan which identifies the actions required to return OT assets to a state within the tolerable cyber security risks levels, should they be exposed to unplanned risk during the installation process.
- 4.3.5.5 Before installation, the project must ensure that the security of any tools has been assessed and confirmed as secure, free from malware and containing only essential software to support the installation.



- 4.3.5.6 After installation, the project must ensure that the tools have been assessed and confirmed clean to prevent the leak of the confidential data relating TfL or the installed system.

4.3.6 Site Acceptance Testing Phase

Site Acceptance Testing

- 4.3.6.1 The project must ensure that functional testing of the cyber security controls is completed on the system within the constraints of a non-operational site setting.
- 4.3.6.2 The project must undertake penetration testing of the system at SAT.
- 4.3.6.3 The project must undertake necessary remediation activities as a result of SAT.

4.3.7 Operations and Maintenance Phase

Documentation

- 4.3.7.1 The project must receive documentation covering the design of the cyber security controls and their ongoing operation and maintenance.
- 4.3.7.2 As a minimum, the following documentation is to be provided for handover:
- Operational manuals, processes and procedures
 - Network specifications and configurations
 - Baseline network traffic plan
 - Cyber security plans
 - Asset Register
 - High Level Design (HLD) or Concept Design document
 - Low Level Design (LLD) or Detailed Design Document.

Handover into Operation

- 4.3.7.3 The project must receive documentation to confirm that all the cyber security controls have been verified and validated as functional at handover.
- 4.3.7.4 The project must receive documentation to confirm that, where possible, identified risks and remediations have been closed out and that appropriate mitigating controls have been implemented where this has not been possible.

Training

- 4.3.7.5 The System Owner and Lead Maintainer must receive a comprehensive training plan encompassing the entire cyber security scope, developed security plans as well as the technical features and implementation details of the solutions developed/deployed during the project lifecycle.

4.3.8 Modifications and Retrofit Phase

Operation and Maintenance

Prior to any modification of an OT asset, a cyber security risk assessment must be conducted to confirm that any temporarily disabled security features will not significantly impact the overall security posture of the OT asset during modification.



- 4.3.8.1 For any OT asset modification, the overall security posture of the current cyber security plan should be considered to ensure that the maintenance of the system provides assurance that implemented controls remain in place, and continue to operate correctly, and that the plan itself continues to remain effective.

Secure Supply Chain

- 4.3.8.2 The project must ensure that secure supply chain requirements apply to both hardware and software assets.
- 4.3.8.3 There must be an ongoing process to protect the supply chain for OT assets. This process must contain adequate plans, policies, procedures, and registers to continually demonstrate to the project and system owner that the supply chain remains secure.
- 4.3.8.4 The secure supply chain must be used throughout the project lifecycle.
- 4.3.8.5 There must be controls in place to protect the systems during their physical or logical transport ensuring that the assets are not vulnerable to subversion, including malicious code insertion, counterfeit insertion, and tampering.
- 4.3.8.6 The secure supply chain process must be extended to third party products which are incorporated into the system.
- 4.3.8.7 The secure supply chain process must address and continually demonstrate the following during the project or contract lifecycle:
- Chain of custody practises and updated documentation.
 - Inventory management including the location and protection of physical and logical assets including spare parts.
 - Information protection
 - Secure digital products delivery
 - Trusted channels and controls to ship assets including tamper-proof packaging
 - Controls to detect unauthorised access and/or alteration throughout the delivery process
 - Cascading of these cyber security requirements to the entire supply chain
 - Collection and preservation of evidence demonstrating security of the supply chain.

4.3.9 Decommissioning and Disposal Phase

Disposal and Decommissioning

The project must have procedures in place to address decommissioning and secure disposal of OT assets (including media) in a controlled manner, to avoid disruption to interfacing OT assets and disclosure of sensitive information.

The project must assess and document the effect of replacing or removing an existing OT asset and/or security function. The scope of this assessment must include interfacing OT assets.



4.4 The Purdue model and Secure OT Design

Sections 4.4 to 4.8 of the guidance document ([G1771](#)) provide knowledge and understanding which support the good practice principles in Section 4.2 and the OT Project lifecycle requirements in Section 4.3.

5 Protecting against cyber attack

The following controls will contribute to protecting TfL's OT against cyber-attack and establish the minimum baseline of cyber security measures for all new projects and upgrades to existing systems. Safety critical and service critical systems must also be risk assessed and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

5.1 Identity and access control

TfL must assure good management and maintenance of identity and access control for the networks and information systems supporting TfL services.

The requirement is that the project will have to develop a list of all users (humans, software processes and devices) and to determine for each control system component the required level of Identity and Access Control (IAC) protection.

Access control is the method of controlling who or what entities can access premises and systems, as well as the type and level of access that is permitted. There are three key aspects associated with access control:

- account administration
- authentication
- authorisation.

All three aspects shall work together to establish a sound and secure access control strategy. Account administration is the method associated with granting and revoking access accounts and maintaining the permissions and privileges provided under these accounts to access specific resources and functions on the physical premises, network, or system. Access accounts should be function or role-based and may be defined for individuals, groups of individuals functioning as a crew or for devices providing a function.

The detailed requirements are aligned to the headings below to group requirements under common functions and to support traceability to the NIS regulations where required.

5.1.1 Account administration

As an organisation, TfL must ensure, on an ongoing basis, that only appropriate individuals or entities have accounts that allow access and that these accounts provide appropriate access privileges.

The project must ensure that any system can support the following minimum baseline requirements:

- 5.1.1.1 Access shall be granted, changed, or terminated on the authority of an appropriate manager or system owner.



- 5.1.1.2 A record shall be maintained of all access accounts, including details of the individual(s) and devices authorised to use the account, their permissions, and the authorising manager.
- 5.1.1.3 Access accounts shall be suspended or removed as soon as they are no longer needed, for example in the event of a job change. 3rd parties engaged on the support and maintenance of systems are required to notify TfL of Joiners, Movers and Leavers.
- 5.1.1.4 All established access accounts shall be reviewed three-monthly to ensure that the accounts only provide the minimum required permissions.
- 5.1.1.5 The use of default accounts and passwords is forbidden.
- 5.1.1.6 Passwords for access accounts shall be changed from default or test credentials before the system is handed into operation.
- 5.1.1.7 Periodic reviews of compliance, minimum six-monthly, to the account administration policy and process should be performed.

Note: For safety critical and service critical systems the following additional requirements shall apply:

- 5.1.1.8 Unified account management (for example, an Active Directory service supporting multiple systems within a security Zone)

5.1.2 Authentication

As an organisation, TfL must positively identify network users, hosts, applications, services, and resources for computerised transaction so that they can be given the rights and responsibilities associated with the accounts they have been granted under account administration.

The project must ensure that any system can support the following minimum baseline requirements:

- 5.1.2.1 All users must be authenticated before using an application or system.
- 5.1.2.2 Anonymous authentication shall not be permitted.
- 5.1.2.3 There shall be no hard-coded credentials in the system.
- 5.1.2.4 Root accounts shall not be used as main credentials.
- 5.1.2.5 All default credentials must have been changed by FAT.
- 5.1.2.6 All system administrator access accounts and application configuration access accounts shall have strong authentication practices (such as requiring strong passwords or Multi Factor Authentication (MFA)).
- 5.1.2.7 There shall be no use of SMS for MFA (alternatives are one-time passcodes from an app like Google Authenticator or hardware MFA).

Where this is not technologically achievable, possible compensating controls could include separate physical or electronic entrance control technologies or administrative practices, such as a two-person rule.

In large scale or distributed systems, the use of a centralised access control system, such as LDAP or Radius, should be considered.



- 5.1.2.8 After 3 failed login attempts by a local or remote user, the system should disable the associated access account for 3 hours. There may need to be exceptions for local accounts on systems where constant access is required, such as Human Machine Interfaces (HMIs) in control rooms.
- 5.1.2.9 After 30 minutes of inactivity, a local or remote user should be required to re-authenticate before the user can re-access the system. There may need to be exceptions for local accounts on systems where constant access is required, such as HMIs in control rooms.
- 5.1.2.10 The system shall not allow multiple concurrent logins.
- 5.1.2.11 The system shall not allow applications to retain authentication data between sessions.
- 5.1.2.12 All access attempts to critical systems should be recorded and retained in a log file for a minimum period of three months.
- 5.1.2.13 Log Files should be reviewed for successful and failed access attempts as well as unusual or unexpected activity such as out of hours access or attempts to access the system by unauthorised users.
- 5.1.2.14 Systems should employ an authentication scheme (such as X.509) for task-to-task communication between applications and devices.

Note: For safety critical and service critical systems the following additional requirements shall apply:

- 5.1.2.15 Multifactor authentication for untrusted networks.
- 5.1.2.16 Multifactor authentication for all networks.

5.1.3 Authorisation

As an organisation, TfL must grant access privileges to resources after successful authentication of the user and identification of their associated access account. The privileges granted are determined by the account configuration set up during the account administration step in the business process.

The project must ensure that any system can support the following minimum baseline requirements:

- 5.1.3.1 There must be clearly documented rules that define the privileges authorised for access accounts which are aligned to the job roles for the system. These rules must follow the principles of least privilege.
- 5.1.3.2 The system must apply these rules to all users upon authentication.
- 5.1.3.3 Access accounts must be role based to manage access to appropriate information or systems for that user's role.
- 5.1.3.4 Safety implications shall be considered when defining roles.

Note: For safety critical and service critical systems the following additional requirements shall apply:

- 5.1.3.5 Unique identification and authorisation.

