Code of connection standard

# Code of connection standard

Note: This document is Legacy IA Policy. It is under review and likely to be withdrawn or substantially revised soon. Before using this content for a project, contact [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

This standard is designed to help protect MoJ ICT systems by providing a standard for the connection of a 3rd party ICT system to a MoJ ICT system.

## Overview

### Introduction

A Code of Connection (CoCo) is designed to provide a mechanism to record a formal agreement between a 3rd party organisation and the MoJ on the security measures to be applied by that 3rd party prior to and during any electronic connection with a MoJ ICT system, for example, to facilitate the exchange of data between two case management systems.

[HMG Security Policy Framework (SPF)](https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework) mandatory requirements state that:

Departments and Agencies must put in place an appropriate range of technical controls for all ICT systems, proportionate to the value, importance and sensitivity of the information held and the requirements of any interconnected systems.

In order to meet these requirements, the SPF stipulates that ICT systems must:

Comply with the requirements of any codes of connection, multilateral or bilateral international agreements and community or shared services security policies to which they are signatories (e.g. Government Secure Intranet).

Policy statements on connecting 3rd party ICT systems and the requirements for a CoCo are covered in IT Security – Technical Controls Policy, while this document sets out the MoJ standard for its implementation.

### Scope

This guide applies to all MoJ ICT systems including ICT systems hosted by third party suppliers on behalf of the MoJ where there is a valid business requirement to connect to a 3rd party system.

### Demonstration of Compliance

The CESG Information Assurance Maturity Model (IAMM) sets out the minimum maturity level Government departments should attain. Maintaining secure connections is captured as a basic requirement in Level 1 of this model, which the MoJ will need to demonstrate compliance with in their IAMM return to the Cabinet Office.

## Code of Connection

### Context

A Code of Connection (CoCo) is designed to provide evidence to the MoJ that a connecting 3rd party understands the security controls and procedures required to connect to a MoJ ICT system and that those controls and procedures have been implemented. The aim here is to ensure that the risks associated with connecting ICT systems together are sufficiently mitigated in the technical solution and managed on an ongoing basis during live operation.

**Note:** This standard is based on connecting a RESTRICTED-IL3 MoJ ICT system with an Accredited 3rd party RESTRICTED-IL3 ICT system where all electronic communication is over an Accredited RESTRICTED-IL3 network/s and/or RESTRICTED-IL3 communications channel. Where this is not the case, advice must be sort from the IT Security Officer (ITSO) and system Accreditor.

A generic CoCo (based on the note above) is provided in Appendix A; it is split into two sections:

* basic requirement (see section A.1) – The section outlines the base set of CoCo requirement which need to be met by the connecting 3rd party
* supporting compliance statement (see section A.2) – This section contains a series of compliance statements based on ISO 27001 and the [IAS 1&2 Baseline Controls Set (BCS)](https://www.ncsc.gov.uk/guidance/information-risk-management-hmg-ia-standard-numbers-1-2). It is designed to provide a mechanism for a connecting 3rd party to supply compliance evidence to the system Accreditor. Section 3.2 provides details on how this compliance statement should be applied.

**Note:** A signed CoCo between the MoJ and the connecting 3rd party is required before the connection can go into live operation.

### Managing the risk of connectivity

In order to ensure that the connectivity and sharing of electronic data between a MoJ ICT system and a 3rd party ICT system does not cause undue risk from one participating organisation to another, each organisation must reasonably comply with the code of connection to ensure any risks are managed effectively.

The need for a CoCo and its application will be determined by the MoJ system Accreditor who will consider the risks involved, this may require the production of a technical risk assessment and/or RMADS for the connection (further details on RMADS can be found in the [Accreditation Framework](https://intranet.justice.gov.uk/guidance/security/it-computer-security/infrastructure-system-accreditation/) ).

The CoCo condition and compliance statement contained within the generic CoCo document (see A.1.3) provide a good platform to judge whether the assurance level of the connecting 3rd party ICT system is sufficient rather than just relying on its accreditation status. A risk based approach must be taken to the application of security controls associated with the connection. The generic CoCo (see Appendix A) provides a baseline by which a 3rd party ICT system's connection to a MoJ ICT system will be assessed. The MoJ system Accreditor will provide a steer as to how this should be applied, where the default steer is that the guidance provided in [IAS 1&2 Baseline Controls Set (BCS)](https://www.ncsc.gov.uk/guidance/information-risk-management-hmg-ia-standard-numbers-1-2) at the DETER level should be applied.

It is highly likely that the connection between the two systems will be over the GSi. If so, the 3rd party organisation is likely to have completed the GSi Code of Connection for that system connection. The information requested in the generic CoCo is similar to that required for the GSi CoCo and as such should be readily available.

**Note:** Depending on the protocols being used, the GSi authority may need to be contacted.

### Completing a Code of Connection

The IT System Manager and/or ITSO for the connecting 3rd party organisation must review CoCo and submit the supporting compliance statement to the MoJ system Accreditor along with any supporting documentation.

In completing the CoCo statement, the connecting 3rd party organisation confirms that they have implemented all the controls required, it should be noted that the adoption of these controls will not totally mitigate all the risks involved whether to the 3rd party's own ICT system or to the connecting MoJ ICT system.

Where the connecting 3rd party ICT system does not comply with the controls outlined in the CoCo, the IT System Manager and/or ITSO must provide supporting comments including a high-level plan that outlines the expected timeline to meet them.

An approval from the MoJ system Accreditor is required prior to the connection going into live operation.

## Appendix A - Generic Code of Connection

**NOTE:** *This appendix contains a generic Code of Connection, it is based on connecting a RESTRICTED-IL3 MoJ ICT system with an Accredited 3rd party RESTRICTED-IL3 ICT system where all electronic communication is over an Accredited RESTRICTED-IL3 network/s and/or RESTRICTED-IL3 communication channel. Where this is not the case, advice must be sort from the IT Security Officer (ITSO) and system Accreditor.*

It may need to be customised based on the relevant risk assessment and business context.

### A.1 Code of Connection – Basic requirement

#### A.1.1 Applicable policies

This Code of Connection (CoCo) covers the connection of the “NAME OF MoJ ICT SYSTEM” to “NAME of 3rd PARTY ICT SYSTEM”.

The services to be provided by this connection are defined in section A.1.2.1.

The [MoJ ICT Security Policy](https://intranet.justice.gov.uk/guidance/security/it-computer-security/ict-security-policy-framework/ict-security-policy/) and the IT Security Policy for the “ORGANISATION NAME FOR 3rd PARTY ICT SYSTEM” are the primary polices which apply to this CoCo.

Any 3rd party ICT system connecting to a MoJ ICT system must have a current and relevant IT Security Policy which is accepted by the MoJ ITSO and system Accreditor. If any aspects of the data to be exchanged require special handling measures or are particularly sensitive, the MoJ system Accreditor must be informed an approach to handling that data must be agreed by both connecting parties in advance.

#### A.1.2 Connectivity

##### A.1.2.1 Data flows, service and protocols

This section must contain details on all the data flows and service facilitated by this connection (including the protocols used); where appropriate this information can be contained within a referenced document with a summary contained in the CoCo. It must also contain details on all onward connections from the 3rd party ICT System.

##### A.1.2.2 Connection

The “NAME of 3rd PARTY ICT SYSTEM” must provide a gateway at the edge of their system to facilitate the connection to the “NAME OF MoJ ICT SYSTEM” which is Accredited to RESTRICTED-IL3 and exhibits the following properties:

* Only permit the data traffic flows and protocols identified in A.1.2.1;
* This gateway must be managed by authorised service personnel with SC security clearance as a minimum;
* The gateway must maintain its own audit logs which are included as part of the “ORGANISATION NAME FOR 3rd PARTY ICT SYSTEM” protective monitoring system;
* Have front-end firewall(s) to be a minimum of EAL4 certified or CAPS approved;
* rovide a minimum of EAL4 separation on front-end firewall(s) between the port used for connection to the NAME OF MoJ ICT SYSTEM] and ports used for other connections.

#### A.1.3 Conditions

|  |  |
| --- | --- |
| Condition | Description |
| CoCo-1 | The minimum standards applicable to the “NAME of 3rd PARTY ICT SYSTEM” shall be the equivalent to application of the IAS 1&2 Baseline Controls Set (BCS) at the DETER level and ISO27001. The supporting compliance statement (see A.2) has been derived from IAS 1&2 Baseline Controls Set (BCS) and ISO27001 and provides a check list that “ORGANISATION NAME FOR 3rd PARTY ICT SYSTEM” should use to document their compliance to this CoCo. The completed compliance statement will allow the MoJ to determine whether the “NAME of 3rd PARTY ICT SYSTEM”'s level of compliance is sufficient to meet the requirements outlined in this CoCo. |
| CoCo-2 | The MoJ system Accreditor must be advised of any proposed changes (including configuration changes) to be made to the “NAME of 3rd PARTY ICT SYSTEM” which will have an effect on its connection to the “NAME OF MoJ ICT SYSTEM”. |
| CoCo-3 | All existing and planned onward connections to or from the “NAME of 3rd PARTY ICT SYSTEM” must be brought to the attention of the MoJ system Accreditor prior to any live connection to the “NAME of 3rd PARTY ICT SYSTEM” as this may represent a risk to the “NAME OF MoJ ICT SYSTEM” and its onward connections. All such connections must be identified in this document (see A.1.2.1). The information provided will be kept confidential and only used for the purpose of assuring the security of this connection. |
| CoCo-4 | No data Protectively Marked above RESTRICTED should be exchanged over this connection. |
| CoCo-5 | All points of connection to the “NAME OF MoJ ICT SYSTEM” shall be within a secure IL3 environment. |
| CoCo-6 | All users (including administrative users) who connect to the “NAME of 3rd PARTY ICT SYSTEM” have been subject to a formal user registration process (section A.11.2.1 in the compliance statement, see A.2) and all have individual unique user accounts. |
| CoCo-7 | All security incidents concerning the “NAME of 3rd PARTY ICT SYSTEM” which have (or may have in the future) involve the connection between the “NAME of 3rd PARTY ICT SYSTEM” and “NAME OF MoJ ICT SYSTEM” must be reported to MoJ ITSO and system Accreditor. |
| CoCo-8 | Data may only be exchanged over this connection using the permitted types of business connection defined in relevant Interchange Sharing Agreement and/or Risk Management & Accreditation Document Set (RMADS) and is limited to the protocols defined in this document (see A.1.2.1). |
| CoCo-9 | The “NAME of 3rd PARTY ICT SYSTEM” is protected by either a hardware Firewall or software Firewall which is either EAL 4 certified or CAPS approved. |
| CoCo-10 | The “NAME of 3rd PARTY ICT SYSTEM” has an anti-virus application installed and it is subject to regular anti-virus signature updates, with the maximum period between updates being 4 hours. |
| CoCo-11 | The “NAME of 3rd PARTY ICT SYSTEM” is subject to an operating system and hosted application security patch regime. |
| CoCo-12 | The “NAME of 3rd PARTY ICT SYSTEM” is administered by dedicated and trained IT staff to a recognised standard such as ISO2000 (ITIL) and/or recognised professional IT qualifications such as MCSE. |
| CoCo-13 | The “NAME of 3rd PARTY ICT SYSTEM” must be hosted, operated and supported from within the UK. |

#### A.1.4 Assumptions

The connecting 3rd party ICT system may make the following assumptions about the security provided by the “NAME OF MoJ ICT SYSTEM”:

* The “NAME OF MoJ ICT SYSTEM” is Accredited by the MoJ to process data up to and including RESTRICTED-IL3 for Confidentiality, Integrity and Availability;
* The security regime within the “NAME OF MoJ ICT SYSTEM” ensures the confidentiality and integrity of data originating from the “NAME of 3rd PARTY ICT SYSTEM” once it enters the boundary of the “NAME OF MoJ ICT SYSTEM”.

#### A.1.5 Administration

This document must be reviewed annually or following a major change to the “NAME of 3rd PARTY ICT SYSTEM” or the “NAME OF MoJ ICT SYSTEM” to ensure no additional security measures are required.

**Note:** A major change is defined as:

* Software – A significant change in the functionality of any software used to support the connection;
* Hardware - A significant change to the physical hardware supporting the connection;
* Design/Architecture - A change in the connectivity of the “NAME of 3rd PARTY ICT SYSTEM” to the “NAME OF MoJ ICT SYSTEM” or any other ICT system it connects to, the security controls protecting those connections or the re-configuration of any services used to support the connection.

#### A.1.6 Authorisation for connection

On the basis of the information made available to them, and to the best of their knowledge, the undersigned confirms that the connecting “NAME of 3rd PARTY ICT SYSTEM” complies with the requirements outlined in this CoCo and that the information provided in the supporting compliance statement is accurate.

**Note:** Any major change (as defined in A.1.5) to the connecting “NAME of 3rd PARTY ICT SYSTEM” may invalidate this CoCo and a new submission may be required.

|  |  |  |
| --- | --- | --- |
| NAME | Signature |  |
| JOB TITLE |  |  |
| NAME OF 3rd PARTY CONNECTING ORGANISATION | Date |  |
| NAME OF MOJ INFORMATION ASSET OWNER | Signature |  |
| MoJ Information Asset Owner |  |  |
|  | Date |  |
| NAME OF MOJ SYSTEM ACCREDITOR | Signature |  |
| MoJ System Accreditor | Date |  |

### A.2 Supporting compliance statement

This compliance statement provides a check list which will enable the MoJ to assess the “NAME of 3rd PARTY ICT SYSTEM” compliance against this CoCo and the pertinent security controls from HMG IAS 1&2 Baseline Controls Set (BCS) at the DETER level and ISO27001. The system Accreditor will determine whether or not the “NAME of 3rd PARTY ICT SYSTEM” presents an unacceptable risk to the “NAME OF MoJ ICT SYSTEM”.

Guidance on completion:

* Under the 'Control' column are a number of security controls which should be read and responded to in subsequent columns;
* Under the 'Compliance' column, answer **Yes**, if the control is fully met, **No**, if it is not fully met, **Partial**, if part of the control has been implemented or **N/A** if the control does not apply;
* Under the 'Process Owner/References' column, the name of an individual or group who is responsible for managing that control must be entered and any associated documents referenced;
* Under the 'Solution/Comments' column, enter a brief statement outlining how that control is met, why it is not met, only partially met or why it does not apply.

**Note:** The notes (in blue and italics) under the “Solution/Comments” column are for guidance only. These notes must be removed upon completion.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref. | Control | Compliance (Applicability) Y/N/P/N/A | Process Owner/ Reference | Solution/Comments |
| **A.5** | **Security Policy** |  |  |  |
| **A.5.1** | **Information Security Policy (ISMS Policy)** |  |  |  |
| **A.5.1.1** | **Information Security Policy document** - Does the “ORGANISATION NAME FOR 3rd PARTY” have an Information Security policy document, approved by management, and published and communicated to all employees and relevant external parties? |  |  | *State clearly what the document title is. Describe how/when this document is communicated to all staff and contractors. Provide a copy of the policy with this statement if possible.* |
| **A.6** | **Security Organisation** |  |  |  |
| **A.6.1** | **Information Security Infrastructure** |  |  |  |
| **A.6.1.1** | **Management commitment to Information Security** - Does “ORGANISATION NAME FOR 3rd PARTY” management actively support security within the organisation through the establishment of a forum where security issues are discussed and security responsibilities are acknowledged? |  |  | *Is information security a standing agenda item at a regular management meeting and/or has a separate working group been set-up to discuss and address security concerns? Who attends this meeting and what is the frequency. Provide terms of reference for the meeting/group where possible.* |
| **A.6.1.3** | **Allocation of Information Security Responsibilities** - Are “ORGANISATION NAME FOR 3rd PARTY” information security responsibilities allocated and documented? |  |  | *Have information security responsibilities been documented and communicated to all staff? If so, how?* |
| **A.6.1.5** | **Confidentiality Agreements** - Does the “ORGANISATION NAME FOR 3rd PARTY” have any confidentiality or non-disclosure agreements in place for staff, contracted bodies and other 3rd parties? |  |  | *Do confidentiality agreements state your requirements for security? Provide a copy of your agreement with this statement if possible.* |
| **A.6.1.8** | **Independent Review of Information Security** - Is the “ORGANISATION NAME FOR 3rd PARTY” subject to external audit? Do any of these audits look at security issues? |  |  | *The approach to managing information security and how it is implemented should be reviewed regularly, i.e. processes, procedures, policies, etc. When was the last one conducted, by whom and how regularly is it normally reviewed. If the system is included in the scope of a certified Information Security Management System, details should be provided.* |
| **A.6.2** | **External Parties** |  |  |  |
| **A.6.2.1** | **Identification of Risks relating to External Parties** - Has the “ORGANISATION NAME FOR 3rd PARTY” conducted any form of risk assessment related to their IT systems and the data held on them? Has the outcome of the risk assessment (e.g. risk treatment plan) been implemented? |  |  | *How do you assess risk to your organisation caused by the provision of access to a 3rd party? Does it also take into account physical & logical access controls, etc* |
| **A.6.2.2** | **Addressing Security when dealing with Customers** - Has the “ORGANISATION NAME FOR 3rd PARTY” identified security requirements which need to be adhered by other entities or organisations connecting into “NAME of 3rd PARTY ICT SYSTEM” before they are given access? |  |  | *Need to provide detail of any security requirements?* |
| **A.6.2.3** | **Addressing security in 3rd Party Agreements** - Does the “ORGANISATION NAME FOR 3rd PARTY” include security requirements in contracts with third parties that involve accessing, processing, communicating or managing the organisation's information or information processing facilities? |  |  | *Do the 3rd party agreements include terms that assist meet the identified security requirements? Examples of these terms or a copy of the 3rd party agreement should be provided.* |
| **A.7** | **Asset Classification and Control** |  |  |  |
| **A.7.1** | **Responsibility for Assets** |  |  |  |
| **A.7.1.3** | **Acceptable use of Assets** - Does the “ORGANISATION NAME FOR 3rd PARTY” have any documented policies on the acceptable use of information and assets associated with information processing, i.e. personal use, use of email, Internet access etc? |  |  | \*Are there rules for the use of assets within the organisation, e.g. Acceptable use policies or “Do and Don't” lists for Email & Internet, mobile devices, etc. If so, details should be provided. |
| **A.7.2** | **Information Classification** |  |  |  |
| **A.7.2.1** | **Classification Guidelines** - Does the “ORGANISATION NAME FOR 3rd PARTY” use a data classification scheme (e.g. the Government Protective Marking Scheme) with defined protective controls for each classification or sensitive personal data? |  |  | *State the classification scheme applied and associated controls to protect personal data (if applicable). Has this been documented and communicated to all staff? Provide a copy of the guidance provided if possible.* |
| **A.8** | **Human Resources Security** |  |  |  |
| **A.8.1** | **Prior to Employment** |  |  |  |
| **A.8.1.1** | **Roles and Responsibilities** - Does the “ORGANISATION NAME FOR 3rd PARTY” identify security roles and responsibilities of employees, contractors and 3rd party users? Are such roles/responsibilities documented? |  |  | *Are there defined, documented and communicated security roles and responsibilities? State what these are at a high-level and provide documentation where possible to support this. E.g. role/function terms of reference.* |
| **A.8.2** | **During Employment** |  |  |  |
| **A.8.2.1** | **Management Responsibilities** - Does “ORGANISATION NAME FOR 3rd PARTY” management ensure security requirements are enforced by employees, contractors and 3rd party users? How is this achieved? |  |  | *How do management ensure that staff and contractors are aware and comply with their responsibilities for security?* |
| **A.8.2.2** | **Information Security Awareness, Education and Training** - Do “ORGANISATION NAME FOR 3rd PARTY” employees and, where relevant, contractors and 3rd party users receive appropriate security awareness training and regular updates in “ORGANISATION NAME FOR 3rd PARTY” security policies and procedures, as relevant for their job function? |  |  | *Do all employees and contractors undergo security awareness training? How frequently is this awareness training conducted? What does the security awareness training cover at a high-level. How do you assess employees' understanding of that training?* |
| **A.8.3** | **Termination or Change of Employment** |  |  |  |
| **A.8.3.3** | **Removal of Access Rights** - Does the “ORGANISATION NAME FOR 3rd PARTY” remove access rights of all employees, contractors and 3rd party users to information and information processing facilities upon termination of their employment, contract or agreement? How is this done? |  |  | *Details should be provided on the process for removing access rights on termination of employment.* |
| **A.9** | **Physical and Environmental Security** |  |  |  |
| **A.9.1** | **Secure Areas** |  |  |  |
| **A.9.1.1** | **Physical Security Perimeters** - Does the “ORGANISATION NAME FOR 3rd PARTY” have a defined, effective, security perimeter to protect areas that contain information-processing facilities? |  |  | *Describe the physical security barriers, e.g. walls, alarm systems, doors/gates, fencing, etc, where applicable.* |
| **A.9.1.2** | **Physical Entry Controls** - Are there secure areas within the “ORGANISATION NAME FOR 3rd PARTY” premises, protected by appropriate entry controls to ensure that only authorised personnel are allowed access? |  |  | *Describe any designated secure areas in the building. Where will the servers/workstations/gateway used to support this connection be located? What security controls are in place to limit access to those with a need-to-know?* |
| **A.9.1.6** | **Public Access Delivery & Loading Areas** - Are access points such as delivery and loading areas and other points where unauthorised persons may enter the “ORGANISATION NAME FOR 3rd PARTY” premises controlled and, if possible, isolated from information processing facilities to avoid unauthorised access? |  |  | *Describe the controls limiting access from public access, delivery and loading areas to the areas housing the ICT services used to support this connection.* |
| **A.9.2** | **Equipment Security** |  |  |  |
| **A.10** | **Communications and Operations Management** |  |  |  |
| **A.10.1** | **Operational Procedures and Responsibilities** |  |  |  |
| **A.10.1.1** | **Document Operating Procedures** - Does the “ORGANISATION NAME FOR 3rd PARTY” have operating procedures for the system connecting to “NAME OF MoJ ICT SYSTEM”? |  |  | *Are operating procedures documented? A copy of the document or Table of Contents will suffice.* |
| **A.10.1.2** | **Change Management** - Does the “ORGANISATION NAME FOR 3rd PARTY” have a Change Management process which covers the system connecting to the “NAME OF MoJ ICT SYSTEM”? |  |  | \*Describe the change management process. |
| **A.10.2** | **3rd Party Service Delivery Management** |  |  |  |
| **A.10.2.1** | **Service Delivery** - If the “ORGANISATION NAME FOR 3rd PARTY” use a 3rd party service provider for its ICT Service , does the “ORGANISATION NAME FOR 3rd PARTY” ensure that the security controls, service definitions and delivery levels included in the 3rd party service delivery agreement are implemented, operated and maintained by that 3rd party? |  |  | *Do you use a 3rd party supplier to support ICT used in this connection? Are security requirements stated within the agreement? How do you check the effectiveness of the security controls stated in the 3rd party agreement?* |
| **A.10.3** | **System Planning & Acceptance** |  |  |  |
| **A.10.4** | **Protection against Malicious and Mobile Code** |  |  |  |
| **A.10.4.1** | **Controls against Malicious Code** - Has the “NAME of 3rd PARTY ICT SYSTEM” implemented controls to detect and protect against malicious code and that appropriate user awareness procedures is provided? What AV application is installed and how often is the AV library updated? |  |  | *What measures are in place to control against malicious software/code? Describe the process for detection and removal of malware if detected.* |
| **A.10.5** | **Backup** |  |  |  |
| **A.10.6** | **Network Management** |  |  |  |
| **A.10.6.1** | **Network Controls** - Is the system connected to the “NAME of 3rd PARTY ICT SYSTEM” segregated from other “ORGANISATION NAME FOR 3rd PARTY” systems? Note: It is understood that this may not be possible in all cases. |  |  | *How is the connecting system protected against network intrusions? Describe any segregation of other networks and provide a high-level logical network diagram if possible.* |
| **A.10.7** | **Media Handling and Security** |  |  |  |
| **A.10.7.3** | **Information Handling Procedures** - What procedures are in place for the handling and storage of MoJ information in order to protect such information from unauthorised disclosure or misuse? |  |  | \*Describe your information handling procedures. How does this map to A.7.2.1 above (Information Classification). |
| **A.10.7.4** | **Security of System Documentation** - What security procedures are in place to secure the system documentation concerning this connection so it is protected from unauthorised access? |  |  | *How is the system documentation prevented from unauthorised access?* |
| **A.10.8** | **Exchange of Information** |  |  |  |
| **A.10.8.5** | **Business Information Systems** - Are there any policies and procedures to protect information shared over this connection? |  |  | *Please provide any policies or an Information Sharing Agreement.* |
| **A.10.9** | **Electronic Commerce Services** |  |  |  |
| **A.10.10** | **Monitoring** |  |  |  |
| **A.11** | **Access Control** |  |  |  |
| **A.11.1** | **Business requirement for Access Control** |  |  |  |
| **A.11.2** | **User Access Management** |  |  |  |
| **A.11.2.1** | **User Registration** - Does the “NAME of 3rd PARTY ICT SYSTEM” have a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services? |  |  | *Describe the registration and deregistration process. Are the user registration procedures documented?* |
| **A.11.2.2** | **Privilege Management** - Does the “NAME of 3rd PARTY ICT SYSTEM” restrict the allocation and use of privileges? |  |  | *Who has (or will be given) privileged access to the MoJ ICT System – roles will suffice? How will this access be restricted to just those named roles?* |
| **A.11.2.3** | **User Password Management** - What process is in place to allocate passwords to users? Is a password policy enforced and what technical controls are in place to support that enforcement? |  |  | *Describe the process for allocating new passwords, the password policy and any control used to enforce it?* |
| **A.11.2.4** | **Review of User Access Rights** - Is there a review process that covers users' access rights on the “NAME of 3rd PARTY ICT SYSTEM”? |  |  | *Describe the process for regularly reviewing access rights* |
| **A.11.3** | **User responsibilities** |  |  |  |
| **A.11.3.1** | **Password Use** - Do users follow good security practices in the selection and use of passwords? |  |  | \*State the password policy. What controls are in place to prevent users from selecting weak passwords? |
| **A.11.3.2** | **Unattended User Equipment** - Is there a user timeout set on the “NAME of 3rd PARTY ICT SYSTEM”? |  |  | *What is the timeout process?* |
| **A.11.4** | **Network Access Control** |  |  |  |
| **A.11.4.1** | **Policy on use of Network Services** - How does “NAME of 3rd PARTY ICT SYSTEM” ensure that users only have direct access to the services that they have been specifically authorised to use? |  |  | *Describe how users are limited to those services that they are only authorised to use. Is there a policy covering access to network services?* |
| **A.11.4.2** | **User Authentication for External Connections** - Does “NAME of 3rd PARTY ICT SYSTEM” ensure any remote access is subject to authentication of the same standard as for normal users? See Control A.11.2.3 above. |  |  | *What security safeguards are in place to control access by remote users?* |
| **A.11.5** | **Operating System Access Control** |  |  |  |
| **A.11.5.1** | **Secure Log-on Procedures** - Is access to the “NAME of 3rd PARTY ICT SYSTEM” only attainable via a secure log-on process? |  |  | *Provide an overview of the secure log-on process.* |
| **A.11.5.2** | **User Identification and Authentication** - Do all users of the “NAME of 3rd PARTY ICT SYSTEM” have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual? |  |  | *State clearly whether users have a unique User ID associated with their use of the ICT system and additionally that this unique identifier can be used uniquely/unequivocally to identify the activities of that user.* |
| **A.11.5.4** | **Use of System Utilities** - A confirmation is required that the use of system utility programs on the “NAME of 3rd PARTY ICT SYSTEM” is restricted and tightly controlled? |  |  | *What procedures do you have in place to restrict access to system utility programs?* |
| **A.11.6** | **Application Access Control** |  |  |  |
| **A.11.7** | **Mobile computing and Teleworking** |  |  |  |
| **A12** | **Information Systems Acquisition, Development and Maintenance** |  |  |  |
| **A12.1** | **Security Requirements of Information Systems** |  |  |  |
| **A.12.2** | **Correct Processing in Applications** |  |  |  |
| **A.12.3** | **Cryptographic controls** |  |  |  |
| **A.12.3.1** | **Policy on the Use of Cryptographic Controls** |  |  | *Check with the MoJ system Accreditor on whether any cryptographic controls are required in this connection.* |
| **A.12.4** | **Security of System Files** |  |  |  |
| **A.12.4.1** | **Control of Operational Software** - Is there a process to control the implementation of software on the “NAME of 3rd PARTY ICT SYSTEM”? |  |  | *Provide details on the controls put in place on the implementation of operational software.* |
| **12.5** | **Security in development and support processes** |  |  |  |
| **A.12.5.1** | **Change Control Procedures** - All changes to the “NAME of 3rd PARTY ICT SYSTEM” should be examined and any major changes reported to MoJ system Accreditor. |  |  | *Is there a documented Change Control procedure? Details should be provided.* |
| **A.12.5.4** | **Information Leakage** - Are there controls in place to reduce the likelihood of information leakage (compromise of MoJ)? |  |  | *What controls are in place to detect, deter or prevent information leakage?* |
| **A.12.6** | **Technical Vulnerability Management** |  |  |  |
| **A.13** | **Information Security Incident Management** |  |  |  |
| **A.13.1** | **Reporting Information Security Events and Weaknesses** |  |  |  |
| **A.13.1.1** | **Reporting Information Security Events** - Is there a documented process to ensure information security events affecting the “NAME of 3rd PARTY ICT SYSTEM” are reported to MoJ ITSO and system Accreditor as soon as possible? |  |  | *Describe the Incident Management process applicable to the connecting system or supply documentation to support this. It must include reporting of security incidents to the MoJ.* |
| **A.13.2** | **Management of Information Security Incidents & Improvements** |  |  |  |
| **A.13.2.1** | **Responsibilities & Procedures** - Have assigned responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents been implemented? This needs to include the requirement to report incidents associated with the “NAME of 3rd PARTY ICT SYSTEM” to MoJ. |  |  | *All IT Security incidents should be reported to MoJ Operational Security Team.* |
| **A.14** | **Business Continuity Management** |  |  |  |
| **A.14.1** | **Aspects of business continuity management** |  |  |  |
| **A.15** | **Compliance** |  |  |  |
| **A.15.1** | **Compliance with legal requirements** |  |  |  |
| **A.15.1.4** | **Data Protection and Privacy of Personal Information** - Does the “ORGANISATION NAME FOR 3rd PARTY” have documented procedures covering data protection and privacy of personal information? |  |  | *Reference relevant documentation that details the procedures for adhering to privacy and protection of personal information. Provide documentation to support this if available.* |
| **A.15.2** | **Reviews of Security Policy and Technical compliance** |  |  |  |
| **A.15.2.1** | **Compliance with Security Policies & Standards** - Does the “ORGANISATION NAME FOR 3rd PARTY” conduct compliance audits to achieve compliance with security policies and standards, including the CoCo for this connection? |  |  | *What is the process to conduct a compliance audit against the processes and procedures employed to support this connection? When was the last one conducted? Were any gaps identified, if so is there a remediation plan in place?* |
| **A.15.2.2** | **Technical Compliance Checking** |  |  | *Is the connecting system subject to a technical assessment (penetration test / ITHC? When was the last one done? Were any vulnerabilities identified and if so have these been addressed/fixed?* |
| **A.15.3** | **System Audit Consideration** |  |  |  |