

**GovAssure:**

**Scoping Document**

**(Worked example)**

**Department of Artificial Intelligence and Robotic Technologies (DAIRT)**

**Purpose of this document?**

The purpose of this document is to demonstrate how key discussions and decisions taken by organisations to identify and define their essential services and ’in-scope’ critical systems for GovAssure should be evidenced in the GovAssure Scoping Document.

[**Part A: Organisation background**](#bookmark=id.30j0zll)

[**Part B: Essential services**](#bookmark=id.35nkun2)

[**Part C: Critical systems**](#bookmark=id.1ksv4uv)

[**Part D: GovAssure in-scope systems**](#bookmark=id.44sinio)

**Who is this document for?**

This document is primarily for use by the relevant government organisation to refer to during Stages 1 and 2 of GovAssure, as the organisation documents how they have identified and defined their essential services and ‘in-scope’ critical systems.

**How to use this document?**

This document is a worked example of a completed Scoping Document for the purposes of GovAssure. The document should be used by government organisations going through GovAssure as a guide to completing their own Scoping Document and does not represent the return of a real government organisation.

**DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND ROBOTIC TECHNOLOGIES (DAIRT)**

|  |  |
| --- | --- |
| **Key roles and responsibilities** | |
| GovAssure Accountable Officer | James Smart, CISO |
| GovAssure Coordinator / Responsible Officer | Sue Perkin, Information Security Specialist |



**01**

**02**

**03**

**04**

**05**

**Understanding the context and overall mission of the organisation to identify essential services. These will help shape and scope the GovAssure self-assessment.**

**Identifying and prioritising the systems on which essential services rely and considering the system boundaries and determining the dependencies. Identifying the CAF profile (Baseline or Enhanced) to be assigned.**

**Completion of a self-assessment for each organisation based on the scope identified during Stages 1 & 2 against the CAF Guidance documentation.**

**Self-assessment will be reviewed by an independent assessor, providing independent and objective verification of the assessment. Assessors will meet the minimum security and assurance requirements.**

**A final report will be produced, outlining observations and recommendations and providing assessment against the target CAF profile. This will be a key mechanism to support investment and decision making.**

**Owner:**

**Department**

**Owner:**

**Department & GSG**

**Owner:**

**Department & GSG**

**Owner: Independent Assessor,**

**Department & GSG**

**Owner: Independent Assessor,**

**Department & GSG**

**Stage 1: Organisation Mission & Services**

**Stage 2: In-Scope Systems & Alignment to CAF**

**Stage 3: CAF Self-Assessment**

**Stage 4: Assurance Review**

**Stage 5: Final Assessment & Targeted Improvement Plan**

|  |  |
| --- | --- |
| **PART A: ORGANISATIONAL MISSION, OBJECTIVES AND PRIORITIES** | |
| *Please consider and document the following ‘about the organisation’ aspects to help inform the organisational context that is presented to the independent assurance reviewer (Stage 4).* ***Please keep all answers under 250 words.*** | |
| **Strategic Context** | *What is the organisation fundamentally trying to achieve? What are the organisation's mission, objectives and priorities, and how do they support the delivery of Government services?*  *Please think about how an ‘elevator pitch’ about the organisation would look if written in in 2-3 sentences.*  **Mission:** The Department of Artificial Intelligence and Robotic Technologies (DAIRT) was established in 2019. DAIRT is an expert policy Department following the growth of domestic and commercial Artificial Intelligence (A.I.) and robotic technologies. DAIRT works with industry and academia to make every day domestic tasks safer, more efficient, and inclusive. To do this, DAIRT aims to shape the safe and secure introduction of domestic and commercial A.I and robotics into households and service-oriented organisations leading the government’s wider Future of A.I and Robotics programme.  **Objectives:** The objectives are to:   * Set strategic direction and provide investment certainty through policy and other interventions. * Develop and implement the legislative and safety framework necessary to enable the safe domestic and commercial deployment of A.I. and Robotic Technologies (AIRT) across different areas including UK homes and the Hospitality sector. * Engage with the public to gain an insight into public opinion and increase the public’s understanding of the emergence of AIRT. * Provide joint investment with industry through to 2025 to overcome the barriers to commercial deployment, thereby attracting, de-risking, and anchoring global investment. * Creating jobs and strengthening our supply chain so that the UK is a maker of AIRT and not just a taker. * Provision of the AIRT Safety Management System. Reporting on the performance of AIRT through use, and trial outcomes, which will include incidents or issues encountered, recalls and advisories. This includes:   + Communication with the AIRT regulator, the A.I. and Robotics Authority.   + Delivery of a communication platform for Universities and Research organisations.   + Delivery of communications and messaging platforms for urgent updates and recalls to AIRT providers; and   + Data analysis for use in statutory publications or used internally and externally to feed in to legislative and safety frameworks.   Our priorities are:   * To ensure the safety of the population when engaging with domesticated and commercially deployed AIRT. * Working in collaboration with other government departments to ensure the UK is a viable and attractive destination for innovation in support of the government’s goals for our country’s economic development. * Keeping a focus on the key governmental aim of protecting our people. More specifically, the department’s long term priority to support the adoption and engagement with domestic and commercial robotic technology, to create structures to support our citizens. |
|
| **Organisationbackground** | *How is the organisation currently set up to deliver its mission/objectives and strategy?*  *How does the organisation operate? For example, does the organisation have 24/7 x 365 services that are delivered online, or an offline non-transactional service?*  DAIRT is located within The Globe, St James St, London, this is a restricted access building exclusively for DAIRT employees. We provide a high availability 24x7 x 365 day Safety management recording system with a public facing logging facility. We have a range of on-premise and cloud hosted systems delivered from a managed service providers and a self-managed infrastructure. The whole is set up to provide a well-integrated system to maximise the re-use of underlying structures to minimise cost and maximise repeatable architectural patterns, such as; Single Sign On through one AD for cloud and on premise services, Messaging Buses, files ingress and egress services, collaboration zones for interaction with OGDs and third parties, security monitoring, internet and boundary controls. |
|
| **Current threat landscape** | *Who is looking to attack you, why are you a target, and ‘what could go wrong’ if they were successful? If there is a multi-threat picture, please feel free to bullet point the different types. Feel free to reference threat assessments if you have them.*  It is recognised that all organisations within the AIRT sector are a target for cyber threat actors. Whilst DAIRT do not hold specific AIRT design and coding data, they are linked to organisations that do and it is recognised that they may be targeted as a conduit or launchpad to a target organisation. Organisations associated with AIRT are a constant target to steal AIRT information for malicious intent. This would include threat actors looking to ultimately take control of the technology for nefarious means. The wider introduction of AIRT would allow cyber criminals to launch a new wave of sophisticated attacks that may evade traditional security-detection and monitoring tools. In most instances, the attackers would look to gain access to information on the government’s position on robotic technology. This information could then be used for financial gain by exploiting sensitive knowledge on the subject to use as ‘inside information’.  Our main threat sources are:   * **State-sponsored threats** are likely to use capable cyber resources to perform defensive and offensive tasks to achieve political influence and gain. The most likely assessed threat from state actors is the theft of intellectual property which could be used to gain technology advantage or exploit infrastructure relating to DAIRT’s programmes. Attacks to disrupt technology could include hijacking the department’s robots, leaking sensitive and confidential documents about AIRT design, or declassifying AIRT documents and experiments. Like many government departments, the department is seeing increased attempts to cause denial of service to its systems or gain access to its data. If successful, they could cease operations or gain information directly related to the department and its emerging policy respectively. * **Insiders (or whistle-blowers)** are usually rogue or unsatisfied employees who aim to either steal AIRT confidential information, or infiltrators that help outsiders to conduct their attack remotely through abuse of privilege and who seek to discredit the Future of A.I and Robotics programme. Insiders can also cause physical damage and destruction to AIRT systems. The department is aware of a contingent of the employee base that may not agree with the direction this department, or indeed the government, is taking regarding commercial robotic technology. If these actors were successful, it can be expected that there may be a significant data leakage as it pertains to this department’s operations. * **AIRT Development Competitors**usually rivals in the robotic industry, who aim to maintain a leading edge in this domain. Many methods could be adopted, such as the reliance on inside threat actors for industrial espionage, to leak confidential documents and damage reputation. |
|
| **Cyber Risk appetite** | *Please confirm if the organisation has a Cyber Risk Appetite (or not), where it is defined, and what the level of appetite is. If this is already defined and documented feel free to copy and paste into this box.*  We have a defined Cyber Risk Appetite (CRA) for all our ‘essential services’. We have provided a copy of this as part of our response to the process. Our CRA directly links to the risk appetite of the wider department, except that we are more risk tolerant in relation to our goals given we do not possess or maintain any critical national infrastructure. |
|

|  |  |  |  |
| --- | --- | --- | --- |
| **Part B: IDENTIFYING AND DEFINING THE ESSENTIAL SERVICES** | | | |
| **Essential service** | **Function** | **Type (OES/CNI/Other)** | **In scope?** |
| **Example:**  Essential Service 1 |  | Fundamental Organisational Output | Unconfirmed |
| AIRT Safety Management Recording and Reporting | AIRT Incident and Event Recording | Fundamental Organisational Output | Yes |
| AIRT Emergency Alerting | Fundamental Organisational Output | Yes |
| Citizen Engagement Portal | Fundamental Organisational Output | Yes |
| Policy and Standards | Development of policies and standards | Fundamental Organisational Output | No |
| Policy and standards version control | Fundamental Organisational Output | No |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PART C: IDENTIFYING AND DEFINING THE CRITICAL SYSTEMS** | | | | |
| *Having considered your prioritised essential services, please consider the critical systems that support the delivery of these essential services.* | | | | |
| *Do you have a defined methodology in place to identify and prioritise critical systems? Y/N*  *If yes, please describe at a high level the methodology followed.* | | | | |
| **Critical system** | **Essential Service / Function this supports (from Part B)** | **Core IT infrastructure underpinning the service (e.g. Network/Cloud Provider)** | **Breakdown of backend systems/applications (where applicable)** | **In scope?** |
| **Example:**  Critical system 1 |  |  | App 01 | Unconfirmed |
| IMS | **AIRT Safety Management Recording and Reporting** / AIRT Incident and Event Recording | Cloud (Microsoft Azure) | End user computing  Azure AD / Cloud Monitoring and logging  Storage table  App Services/Cloud Compute  Database components | Yes |
| AIRT SECOM | **AIRT Safety Management Recording and Reporting** / AIRT Emergency Alerting | DDCAIRT Network | End user compute  SQL database  Active Directory  Alerting API | Yes |

|  |  |
| --- | --- |
| **PART D: IDENTIFYING THE IN-SCOPE CRITICAL SYSTEMS FOR GOVASSURE**  Now you have identified the critical systems that support your organisation's essential services, please consider which critical systems will be assessed as part of GovAssure | |
| **IN-SCOPE SYSTEM 1 DESCRIPTION** | |
| **System name:** | **IMS** |
| **Essential service and function this supports** | **Service:** AIRT Safety Management Recording and Reporting  **Function:** Incident and event recording |
| **Description – what does the system do and why do you consider it in scope for GovAssure:** | IMS is DDCAIRT’s primary system for capturing and recording AIRT incidents and events. It should be included in scope as without this system, it is not possible to record and communicate important events to the AIRT regulator and providers, the impact of this would be that we would be unable to issue urgent advisories and recall notices. |
| **Breakdown of components (if appropriate)** | |
| IMS consists of the following components:   * **SIEM** – The Security Information and Event Management (SIEM) component collects AIRT event log data from other components, which can then be analysed in real time to identify potential threats and vulnerabilities. * **SIEM Log Forwarder** – The Log Forwarding component is point of contact between the SIEM and other components. It forwards the logs containing AIRT events and incidents to and from the SIEM for analysis. * **Azure AD** – Azure Active Directory (AD) is a cloud-based identity and access management service that allows external devices to authenticate and access to external system resources. The Azure AD service also keeps a cloud monitoring service and a logging functionality. * **Logging** – Azure AD keeps a logging service which includes audit logs of every relevant event in Azure AD. These can include changes to applications, groups or users, such as sign ins or groups provisioning. * **Storage Table** – The Azure Table Storage is a service that stores non-relational structured data in the cloud in a cost-effective manner, associated with an Azure Subscription. It can store AIRT-related events and incident logs which can then be fed to the system App Services. * **App Services** – The App Services allows the creation and deployment of web and mobile apps to various platforms. In particular, many AIRT apps with focus on presenting event and incident results, conclusions and next steps can be deployed based on the data collected from other components. * **Blob Storage** – A Blob Storage structure allows users to store large amounts of unstructured data, which include AIRT event logs. * **Databricks** – Databricks creates a collaborative environment for data processing and analysis of large datasets of AIRT event and incident logs * **ML Studio** – ML Studio allows a deep analysis of AIRT event logs and incidents by using AI to build models for in-depth insights, which can then be fed into the App Services * **Data factory** – Data Factory is essential to receive data (including event and incident logs) from various sources and transform it according to the system rules, which then can be transferred to other components. | |
| **Key dependencies** | |
| *What are the key dependencies that enable delivery of the system and service?*   * **Cloud Compute –** There is a core dependency on the cloud compute function. This enables the apps in the Azure infrastructure to scale based on demand. Without the functionality of Cloud Compute, there would be additional server costs and scalability issues. * **Azure Active Directory –** AAD is used to identify and authenticate users. The AIRT Incident and event recording system has a dependency on Azure Active Directory as it is used to identify usernames who appear in the log format. As a result, queries in the monitoring system can easily be linked to a specific user. * **Azure Subscription –** An Azure Subscription is a requirement for users to interact with Azure resources, represented in the graph below. It creates a logical grouping of the resources a user has access to. * **Cloud Monitoring –** Monitoring is a core dependency as it alerts for possible issues with Azure components, presents possible solutions to solve these issues, and can respond in real-time to solve these issues. | |
| **System boundary (Top-level)** | |
| Map out interdependencies on other systems/suppliers/government organisations   |  |  | | --- | --- | | **System Name** | **Interdependencies** | | **SIEM Log Forwarder** | The SIEM Log Forwarder has an interdependency on log sources being forwarded to it. Logs include a range of AIRT systems integrations including firewall and data loss prevention systems. | | **Cloud Monitoring** | The Cloud Monitoring component has an interdependency on the AIRT Security Operations Team. It is the AIRT Security Operations Teams role to actively monitor logs and produce reports based on detections. | | **Azure Subscription** | There is an interdependencyon the procurement team to manage the Azure environment to ensure that relevant products and components are procured and implemented into the AIRT Incident and event recording system. | | **Please state the rationale for each boundary** | |   The boundary for this system incorporates the Cloud system which includes all components included in the system diagram below. The Devices have not been included in the boundary as they are external systems that are used by the end user to interact with the system. | |
| **In Scope Systems Diagrams** | |
| Please include diagrammatic representations of your In Scope systems, clearly indicating the following:   * The critical components and/or assets (grouped if needed); * the security boundary around the critical components and/or assets (system boundary); * other, non-critical, components and assets which are within the system boundary and related interconnectivity (direct wired and wireless); and * entry and exit points within the system boundary including data ingress and egress points (ie. end user devices).     **Essential database components** | |
| **IN-SCOPE SYSTEM 2 DESCRIPTION** | |
| **System name:** | **AIRT SECOM** |
| **Essential service and function this supports** | **Service:** AIRT Safety Management Recording and Reporting  **Function:** AIRT Emergency Alerting |
| **Description – what does the system do and why do you consider it in scope for GovAssure:** | AIRT SECOM is DAIRT’s Emergency Alerting system supporting the function of providing emergency alerts to AIRT holders and communicate recall/software update actions following confirmed recordings of adverse events involving AIRT supporting our key priority of protecting the public whilst supporting the adoption and engagement with domestic and commercial robotic technologies. |
| **Breakdown of components (if appropriate)** | |
| * **Live Alert Sources –** The live alert sources component is used to aggregate alert sources that have been pre-configured in the system. Pre-configured alerts include a network compromise due to malware, ransomware compromise, internet outage and natural disaster alerts. * **Manual Alert Sources –** The manual alert sources components are used for a user to send create an alert manually. For example, in the event of an unusual incident a bespoke alert can be tailored. * **Alert Transformation –** Thealert transformation function is to transform the alert from CSV form into a formatted alert that is ready to be delivered**.** * **Alert Delivery –** The alert delivery function is the final stage before the alert is delivered. The main feature of this component is to ensure that the alert is in the correct file format and has the correct delivery instructions before it is sent to the alert gateway. * **Webserver –** The webserver provides internet access for the alerting API to communicate with. The alerting API is required to make many connections during an incident and therefore, a dedicated web server is required to ensure that the connections can be made. | |
| **Key dependencies** | |
| *What are the key dependencies that enable delivery of the system and service?*   * **Active Directory –** Utilised to identify which end user alerts need to be sent to. * **Alerting API –** Used to query the web user storage to collect alert information**.** * **SQL Database –** Used to store alert information. * **Web User Storage –** Used to store specific alert information tied to a user. | |
| **System boundary (Top-level)** | |
| Map out interdependencies on other systems/suppliers/organisations   |  |  | | --- | --- | | **System Name** | **Interdependencies** | | **Alert Delivery** | The Alert Delivery system has an interdependency on the alert gateway system. The alert gateway is the endpoint system before the alert is sent to the end user. The alert gateway manages all data that is directed internally or externally from the network. | | **Alerting API** | The Alerting API has aninterdependency on the web server. The web servers’ purpose is to receive user information from active directory and communicate with the altering API to manage monitors and alerts. | | **Manual Alert Sources** | The manual alert source’s function has an interdependency on the alert team. The alert team’s role is to create bespoke alerts for emergencies. It is their role to feed alerts to the SQL database, so they are ready to be sent to end users. | | **Please state the rationale for each boundary** | |   The boundary for this system incorporates the AIRT Emergency Alerting system which includes all components included in the system diagram below. The Alert Gateway and Web Server have not been included in the boundary as they are external systems that are managed internally – their main purpose is to manage the communication of alerts to the end user. | |
| **In Scope Systems Diagrams** | |
| Please include diagrammatic representations of your In Scope systems, clearly indicating the following:   * The critical components and/or assets (grouped if needed); * the security boundary around the critical components and/or assets (system boundary); * other, non-critical, components and assets which are within the system boundary and related interconnectivity (direct wired and wireless); * entry and exit points within the system boundary including data ingress and egress points (ie. end user devices).     **AIRT SECOM System** | |

**Annex A: Essential services and critical systems through five lenses**

Key:

In-scope

**Organisation: Department of Artificial Intelligence and Robotic Technologies (DAIRT)**



**Essential Service**

**Functions**

**Systems**

**Sites/Locations**

**Essential Service 1:**

**AIRT Safety Management, Recording and Reporting**

**Lens 1: Essential Service**

Looking top down, this describes the essential service that support the Departments mission at a high-level and who is being served and why it’s important. This provides important context to subsequent scoping approaches. We would recommend identifying the top three essential services key to delivering the Department’s mission and presenting these in a similar way to this worked example.

**Lens 2: Department Function**

Provide a breakdown of the Departments essential service into the various functions or sub-components that enable its delivery. This should identify the high-level functions, and any relationships between these functions, to provide an overview of the approach an organisation takes to delivering their essential service.

Incident and Event Recording

Emergency Alerting

Citizen Engagement Portal

d

**Lens 3: Core Underlying Infrastructure:**

Identify the relevant underlying infrastructure such as the network or cloud hosting arrangement required to deliver the functions above that underpin the essential service.

This viewpoint should clearly identify the groups of network on which essential services rely, or which are used for the provision of essential services.

**Lens 3: Systems**

Identify the relevant and prioritised critical systems sitting on the underlying infrastructure that are required to deliver the functions above that underpin the essential service. This helps to provide a view of system architecture.

**Lens 5: Sites/Locations**

This layer identifies all the relevant sites that are related to the delivery of the essential service. Consideration should be given to the interconnected nature of locations and/or dependencies of sites, supplemented with other information sources that describe the criticality of sites when considering risks to the provision of essential services.

Priority 1: AIRT SECOM

Priority 2: INC App 02

Priority 3: EV 03

Priority 1: IMS

**Core underlying Infrastructure**

AWS

Priority 2: ALT App 02

On premise data centre co-located 01

Off-site data centre co-located 02

Active Directory/Azure (Single sign-on integration with Apps)

DDCAIRT Network

Desktop/End user computing

Amazon Web Services (AWS)

Priority 1: PTL App 01

Serves:

Suppliers

*is enabled by:*

*are enabled by:*

*are located at:*

**Dependencies**

(what are the dependencies required to enable provision of the service)

Regulator

Higher Education

General Public

Suppliers

**Document Control**

|  |  |
| --- | --- |
| **Status** | Baselined |

**Change Log:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Comments** | **Author** |
| 0.1 | 27/07/22 | Document Created | D.Cowan |
| 0.2 | 24/08/22 | Additional narrative | D.Cowan & L.Dobson |
| 0.3 | 21/09/22 | Change to layout and additional narrative | D.Cowan |
| 0.4 | 30/09/22 | Additional narrative and name change | D.Cowan |
| 0.5 | 30/03/23 | Various naming convention changes | T.Fear |

**Version Author and Approver**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author Name and Role** | **Approver Name and Role** | **Date** |
| 0.1 | Daniel Cowan – GSG |  | 27/07/22 |
| 0.3 | Daniel Cowan - GSG |  | 21/09/22 |
| 0.4 | Daniel Cowan - GSG |  | 30/09/22 |
| 0.5 | Tim Fear – GSG |  | 30/03/23 |