**UKRI Identity & Access Management (IAM) Project – Summary of the Requirement**

**Introduction and Background**

Launched in April 2018, UK Research and Innovation (UKRI) is a non-departmental public body sponsored by the Department for Business, Energy and Industrial Strategy (BEIS). UKRI brings together the nine councils, working together in innovative ways to deliver an ambitious agenda, drawing on our great depth and breadth of expertise and the enormous diversity of our portfolio.

Through our councils we maintain and champion the creativity and vibrancy of disciplines and sector-specific priorities and communities. Our councils shape and deliver both sectoral and domain-specific support.

We work with our stakeholders to understand the opportunities and requirements of all the different parts of the research and innovation landscape, maintaining the health, breadth, and depth of the system. The UKRI Digital, Data and Technology (DDaT) strategy has a vision to deliver services that maximise user productivity and empower effective decision making by unlocking UKRI business data and information.

**Flexible and Secure** isone of the strategic themes of the DDaT strategy to provide the enterprise grade Security that ensures that our assets are protected, and our legal obligations are met.

**Identity Access Management (IAM)** is the strategic initiative under Flexible and Secure theme of the DDaT strategy.

**Objectives**

The objective of UKRI IAM Project is to deliver the strategic Identity Access Management (IAM) capabilities. To avoid ambiguity, the industry standard terminology is used to describe Identity Governance and Administration (IGA) and Access Management (AM) capabilities. The low-level requirements can be found in the “**IAM Technical Compliance Requirements**”:

|  |  |
| --- | --- |
| **Identity Governance and Administration (IGA)** | * Identity Policy management
* Identity life cycle management
* Roles and Entitlements management
* Access requests and Workflow management
* Provisioning and Fulfilment
* Access certification
* Identity Governance and Auditing
* Identity analytics and reporting
 |
| **Access Management (AM)** | * Support internal and external identities
* Directory and identity synchronization, including identity repository services
* User self-service capabilities, including registration, password management, profile management and delegated administration
* User authentication methods, multifactor authentication (MFA) and single sign-on (SSO)
* Support advanced user authentication methods, such as Fast IDentity Online (FIDO) and Passwordless authentication
* Authorization and adaptive access
* Access orchestration for decision tree support of external authentication and authorization methods
* Support for UK AMF and modern identity protocols, such as Security Assertion Markup Language (SAML), OAuth, System for Cross-Domain Identity Management (SCIM) and OpenID Connect (OIDC).
* Access enforcement for standard and nonstandard target applications
* Proxy services, agents, or other mechanisms for nonstandard application enablement
* Session management
* Event logging, access analytics and reporting
* BYOI integration
* Developer self-service for application integrations and administration
 |

## IAM Project Implementation Approach

As part of UKRI’s ‘Reforming Our Business’ programme, a new environment has been created to deliver a single shared infrastructure for delivery of centralised unified IT services for the whole of UKRI. This environment is often referred to as ‘Greenfield’ and currently contains Active Directory, Azure AD, Microsoft 365, and other services.

The ‘Business IT Unification’ programme is migrating each of the councils from their legacy environments into the new ‘Greenfield’ environment.

The IAM project adopts a simplified implementation approach, which benefits other strategic UKRI programmes/projects.

The project is able to use internal UKRI resources to help the suppliers throughout the implementation phases.

The following table illustrates a phased approach for Financial Year 1 (2022-23), which is flexible. Bidders are encouraged to provide alternate implementation path that satisfies “IAM Technical Compliance Requirements”.

|  |  |  |  |
| --- | --- | --- | --- |
| Implementation Area | Phase 1(July 2022) | Phase 2(October 2022) | Phase 3(February 2023) |
| Greenfield / Non-Greenfield | Greenfield | Greenfield | Greenfield and Non-Greenfield |
| User Population | * 3000 internal users
* 5000 external users
 | * Additional 3500 internal users
* Additional 10000 external users
 | * Additional 3500 internal users (total 10,000 users)
* Additional 15000 external users (total 30,000 users)
 |
| Identity Governance and Administration (IGA) | * Build IGA Foundational capabilities
* Build a central identity vault
* Authoritative sources integration for identities having HR record (Oracle HR and Workday)
* Authoritative sources integration for identities NOT having HR record (AD, Azure AD)
* Automatic provisioning of accounts to Greenfield AD and Azure AD
* Lifecycle management of users (New Joiners and Leavers)
* Support integration of identity vault with UKRI Staff Directory service
 | * Authoritative sources integration for identities from various sources requiring manual data feed (Supplier will configure 1 source per data feed pattern)
* Guest Users management
* Roles and entitlements management of Greenfield apps (supplier will configure 2 apps per pattern)
* Access Catalogue, Access requests, workflows and automatic provisioning/deprovisioning of access (supplier will configure 2 apps per pattern)
* Automatic provisioning of accounts to council-specific AD domains (maximum 2) and council-specific Azure AD tenants (maximum 2)
* ServiceNow CMDB integration
 | * Lifecycle management of users (Movers)
* Access recertification
* Roles and entitlements management of Non-Greenfield apps (supplier will configure 2 apps per integration pattern)
* Automatic provisioning of accounts to council-specific AD domains (maximum 2) and council-specific Cloud tenants (maximum 2)
* ServiceNow Ticketing integration
* Segregation of Duties and Toxic combinations
 |
| Access Management (AM) | * Build Access Management Foundational capabilities
* Integration of selected pilot apps (maximum 5) with Access Management foundational capabilities
 | * Integration of selected Greenfield apps (Supplier will configure 2 apps per integration pattern) with Access Management foundational capabilities
 | * Integration of selected Non-Greenfield apps (Supplier will configure 2 apps per integration pattern) with Access Management foundational capabilities
 |