**27th June 2022**

**Intelligent Business Process Management (iBPM) Platform – Early Market Engagement**

This Request for Information (RFI) notice invites interested technology product vendors to read and provide feedback on the details shared below concerning the Intelligent Business Process Management (iBPM) platform requirement.

Responding to this announcement is voluntary and does not start an official procurement process for iBPM. The department will not be funding any work undertaken by vendors in responding to this RFI. This RFI activity is for the Authority to gather information only and to aid the team in shaping the iBPM requirement for any future competitive procurement that may follow.

**Background and context**

The [Digital Strategy for Defence](https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data) sets out the strategic role of automation and the need for coherence supported by clear “rules of the road”. It also describes the role of the Digital Foundry which is a critical part of Defence Digital’s strategy to exploit digital, data and technology across Defence.

Defence needs the ability to automate a range of complex processes and to enable continuous, data-driven process improvement. Automation is already delivering a range of benefits, including:

* Financial benefits;
* Reductions in the elapsed time of processes (including reduced error rates);
* Improvements in security, safety, environmental and legal compliance and assurance;
* Improvements in employee satisfaction and digital betterment;
* Improved management information and actionable insight.

Defence processes can be complex in the following different ways:

* They support complex activities and high volume decisions underpinned by individual expertise and complex business rules often spanning multiple systems;
* They are currently supported by a varied range of applications and infrastructure both internal and external to the Department;
* They support different business areas with similar objectives and with process variants;
* Improvement will increasingly require access to more intelligent services and decision-making, provided through artificial intelligence (AI) techniques as well as access to other services.

The Automation Centre of Expertise (ACOE) is the part of the Digital Foundry focusing on support for process automation and low code automation technologies. The aim of the ACOE is to cohere low code automation technologies across Defence by:

* Setting and governing common standards and tooling for automation;
* Enabling reuse and sharing;
* Enabling accredited technology on MOD platforms.

The intelligent Business Process Management (iBPM) programme is part of the ACOE’s strategy for implementing low code automation technologies that can support continuous, data-driven process improvement. These technologies include:

* General purpose low code automation platforms – the Microsoft Power Platform and Oracle APEX are in use in Ministry of Defence;
* Robotic Process Automation (RPA) – Blue Prism is in use in Ministry of Defence;
* Intelligent Business Process Management (iBPM) – as described in this document.

The aim is to implement iBPM platforms coherently. A coherent approach combines a number of different dimensions. These include:

* Clear rules of the road including standards and policies;
* The reuse and sharing of components and good practice;
* The need for a critical mass of Defence staff with key skills to reduce the reliance on contractors and retain corporate knowledge;
* Support for the federated Foundry delivery model.

**Problem statement**

The federated Foundry model is designed to enable application teams to deliver at pace. But the rules of the road for iBPM are not yet agreed and there is a risk that technologies will proliferate and that the implementation of individual technologies will not be coherent. This will:

* Reduce the likelihood that a critical mass of skills can be developed for each technology;
* Increase the policy, technical governance and support overhead;
* Increase the integration and accreditation overhead;
* Reduce the ability to reuse and share components and good practice.

Without clarity about the position of iBPM technologies in the architecture and associated roadmaps, there is a risk that integration with the Authority (“Ministry of Defence”) infrastructure and the necessary accreditation will be slow.

**Desired outcome**

iBPM platforms, integrated into the Authority infrastructure, need to support the Foundry federated delivery model in which a range of different delivery teams can operate independently aligned to a common architecture, principles and standards. The platforms also need to support different security classifications up to Secret.

The service provided to delivery teams needs to be coherent. This means that it needs the following characteristics:

* Clear rules of the road for iBPM, including:
  + A defined set of low code iBPM technologies on governed and supported Defence-wide platforms.
  + Clear policies, standards and technical governance.
  + Governance of citizen development in which citizen development is limited to those activities for which professional delivery expertise is not required.
* Components and good practice widely shared and reused, including:
  + A governed reference architecture for each technology.
  + Efficient reuse mechanisms.
  + Promotion of good practice.
* A critical mass of Defence staff with key iBPM skills, based on:
  + iBPM skills included in the Defence skills framework.
  + Clarity about required roles (including for citizen development) supported by training.
  + Maintenance of key skills through staff retention and skills replenishment policies and processes.
* A clear organisational model for iBPM aligned to the Foundry model, enabling clarity about services provided by the Foundry core (including the ACOE) to enable application teams to deliver products at pace, reuse effectively and support coherence.

**Purpose**

The purpose of this Request for Information (RFI) is to understand better:

* How organisations comparable to the Authority have addressed and organised enterprise-scale implementations of iBPM platforms to support the automation of complex processes;
* What iBPM technology capabilities are available, how they differ from each other and how many iBPM platforms are required in Defence;
* How iBPM technologies and organisations could support the desired outcomes described above.

**Response Submission Deadline** 

Responses to this RFI must be submitted to email address [Daniel.hicks113@mod.gov.uk](mailto:Daniel.hicks113@mod.gov.uk) and [Thomas.blackall100@mod.gov.uk](mailto:Thomas.blackall100@mod.gov.uk) no later than 23:59 GMT on Wednesday 27th July 2022.

Any Clarification Questions (“CQs”) must be submitted via the Defence Sourcing Portal.

**Questions**

See page 4 below.

**Questions to Industry**

|  |  |
| --- | --- |
| Id | Request |
| A. Overview of organisation and products  The implementation of iBPM in the Authority requires technology that is proven in a large, complex, secure environment. | |
| A.1 | Please provide an overview of your technology and products relevant to the Authority's iBPM strategy. |
| A.2 | Please provide case studies where your technology has been implemented in an organisation of comparable size and complexity in a secure environment. |
| B. Support for the Authority strategy  The Authority is looking for technology and organisational support aligned to the strategy. | |
| B.1 | What is your roadmap for future services? How can the Authority use and exploit your roadmap? How would the Authority be able to influence the roadmap? |
| B.2 | What roles and governance arrangements do you provide to customers to support the achievement of benefits through the use of your technology? |
| B.3 | What is your recommended approach to the reuse and sharing of knowledge and artefacts (related to your technology)? What capabilities does your technology provide in support of these recommendations? Please provide examples. |
| B.4 | In what ways is your technology and approach differentiated from other technologies and approaches? |
| B.5 | What is your approach to low/high code development and tools? What scope do your low code approach and tools apply to? Are they provided through a single development environment or more than one? To what elements of the development process is a high code approach required? What constraints would apply to the Authority in aligning with your technology and approach? |
| B.6 | What strategic relationships do you have with other technology providers (in relation to iBPM)? How could these relationships contribute to the Authority strategy? |
| C. Complex processes  The Authority requires technology to support the automation of complex processes. | |
| C.1 | How does your technology support case management and processes with complex relationships between information, people, teams, policies and other applications? How does your approach assess the complexity of processes and the suitability of your technology to support it? |
| C.2 | How does your technology support complex decisions and rules? |
| C.3 | How does your technology support process collaboration between people and also between people and technology (including AI)? |
| C.4 | How does your technology support the management of users? |
| C.5 | How does your technology support different user technologies and channels (inside and outside of the Authority infrastructure) and the management of customer interactions? |
| C.6 | How does your technology support notifications, guidance and prompts relevant to the user journey and process context? |
| D. Process improvement  The Authority requires technology that can support continuous, data-driven process improvement. | |
| D.1 | How does your technology support process discovery? |
| D.2 | Can your technology manage process data so that users are anonymous and individual user performance cannot be analysed? |
| D.3 | How does your technology enable different types of change to be decoupled to minimise the scope of changes and to enable process changes independently of changes to channels and information sources (including legacy information sources)? |
| D.4 | What tools and standards does your technology provide to support process definition, modelling, maintenance and management? |
| D.5 | How does your technology support the provision of management information, the definition of benefits, the automation of benefits management and the definition, measurement and improvement of process performance? |
| D.6 | How does your technology support innovation and prototyping? |
| D.7 | What is your methodology to support process improvement in the following cases:   * process renewal and, where possible, standardisation in which existing processes are supported by different process variants in different business areas based on a mixed technology landscape * identifying process waste and recommending improvements * improving user experience * reducing technical debt associated with legacy service interfaces * incorporation of new services, including the incorporation of a variety of AI tools * scaling up common processes by starting in in one or more business areas and then implementing more widely, taking necessary business area differences into account? |
| D.8 | How does your technology and approach support agile implementation? Please provide examples. |
| E. Application architecture  The Authority requires technology that enables efficient reuse and sharing at an enterprise scale. | |
| E.1 | What is the application architecture of your technology and how does it support coherence, reuse and sharing in a federated IT environment? What governance arrangements do you recommend to ensure that reuse increases efficiency and does not increase technical debt? |
| F. Technical implementation | |
| F.1 | What hosting options are available for your technology and for each:   * what is the technology architecture? * what [Government Security classification](https://www.gov.uk/government/publications/government-security-classifications)s have been achieved with other customers? * has it achieved any accreditation with the Authority and if so, what has been accredited? * how does it integrate with the Authority infrastructure and services? * how does it scale in terms of volume and numbers of different applications? * how does it support service availability and resilience requirements? * in what countries is data processed? * what technical dependencies would the option require of the Authority? |
| F.2 | What capabilities does your technology provide to create human and machine-readable information about the implementation (including processes, integrations and data)? What standards are supported? |
| F.3 | What capabilities does your technology provide to integrate with other applications and information services? |
| F.4 | What capabilities does your technology provide to enable external content and data to be accessed and managed? |
| F.5 | What capabilities does your technology provide to support users internal and external to the Authority? What user devices and software (eg browsers) are supported? |
| G. Support | |
| G.1 | What support models and locations are available for the different hosting models (in the response to F.1) and to what extent are they compatible with different security classifications? |
| G.2 | How are changes to the technology (including operating system changes and security patches) managed under the different hosting options (in the response to F.1) and what is the impact on service availability? |
| G.3 | What capabilities are available to monitor the performance of the platform and applications under the different hosting options (in the response to F.1)? |
| H. Federated development  The Authority has a federated IT environment for developing applications. Any iBPM technology needs to support this environment. | |
| H.1 | How can your technology support multiple different implementations by different teams, potentially using different tools (eg testing, ALM and CI/CD tools) and under different governance? Please provide examples. |
| H.2 | What capabilities are available to support multi-functional (business and technical) teams developing and supporting applications? What approach do you recommend? |
| H.3 | How does your technology support modern web development tools and user interfaces? |
| I. Accelerators | |
| I.1 | What relevant, pre-built components are available to accelerate the development of user interfaces, integration and processes? What examples can you provide of integrating with government services (eg gov.uk.notify)? |
| I.2 | What connectors and capabilities, from your technology or strategic partner technologies (see B.6), are available to accelerate the automation and improvement of Defence processes and Defence Functions (including, for example, People, Finance, Commercial, Digital, Support)? |
| J. COE and governance  The Authority strategy is to provide coherent services. The strategy requires appropriate governance and controls suited to the Authority’s federated IT environment. | |
| J.1 | What organisational model and controls do you recommend to support and develop the technology implementation in a federated IT environment and to govern the roadmap, architecture, policies, environments, reuse and sharing? Please provide examples in organisations of the scale and complexity of the Authority. |
| J.2 | What capabilities do your technology and hosting options provide to support data governance and GDPR? |
| K. Skills  The Authority strategy is to upskill Defence staff for appropriate roles with respect to iBPM technology supplemented by skills acquired from the market. | |
| K.1 | What capabilities can you provide to upskill Defence staff in the use of your technology? What training and learning paths are available for your technology, how are they accessed and delivered? What certification is available? |
| K.2 | What skills are required to implement your technology? What is the availability in the UK of these skills? What partners do you have to provide skills in the UK? |
| L. Commercial  The Authority requires a flexible licencing and cost model aligned to a variety of different types of process. | |
| L.1 | Please provide examples of pricing models that have been used for contracts you have agreed with both private and public sector customers for similar requirements. Please include reference to the below where applicable:   1. Licensing Model (please include any metrics that you use for software licensing and for sizing implementations) 2. Core components, optional components and accelerators (see J.1) that could be licensed separately 3. Professional Services Model. 4. Please list the routes to market that would enable your organisation to meet this requirement (i.e. CCS frameworks) |