RM6187 Framework Schedule 6 (Order Form and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	715065453
THE BUYER:	Strategic Command (Defence Digital) - Ministry of Defence
BUYER ADDRESS	Defence Digital, Building 405, Spur F1, MoD Corsham, Westwells Road, Corsham, SN13 9NR
THE SUPPLIER:	KPMG LLP
SUPPLIER ADDRESS:	15 Canada Square, London, E14 5GL
REGISTRATION NUMBER:	OC301540
DUNS NUMBER:	00-166-7906

Applicable framework contract
This Order Form is for the provision of the Call-Off Deliverables and dated 10/06/2025.
It's issued under the Framework Contract with the reference number RM6187 – Management Consultancy Framework 3 (MCF3) for the provision of a Secure MOD Single Sign On (SSO) Capability Team.

CALL-OFF LOT(S):
Not applicable

Call-off incorporated terms
The following documents are incorporated into this Call-Off Contract.
Where schedules are missing, those schedules are not part of the agreement and can not be used. If the documents conflict, the following order of precedence applies:

1. This Order Form includes the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation) RM6187 3. The following Schedules in equal order of precedence:

Joint Schedules for RM6187 Management Consultancy Framework Three

- Joint Schedule 1 (Definitions)
- Joint Schedule 2 (Variation Form)
- Joint Schedule 3 (Insurance Requirements)

- Joint Schedule 4 (Commercially Sensitive Information)
- Joint Schedule 10 (Rectification Plan)
- Joint Schedule 11 (Processing Data)

Call-Off Schedules

- Call-Off Schedule 1 (Transparency Reports)
- Call-Off Schedule 7 (Key Supplier Staff)
- Call-Off Schedule 8 (Business Continuity and Disaster Recovery) – Supplier Operational Statement of Resilience provided as agreed with the Buyer. See file: DCPP Supplier Assurance Questionnaire (SAQ) RAR 250527A02
- Call-Off Schedule 9 (Security)
- Call-Off Schedule 10 (Exit Management) – As amended by this Order Form which sets out the agreed scope of the exit services and charges applicable
- Call-Off Schedule 13 (Implementation Plan and Testing) – As amended by this Order Form which sets out implementation and testing plans for delivery
- Call-Off Schedule 14 (Service Levels)
- Call-Off Schedule 15 (Call-Off Contract Management)
- Call-Off Schedule 16 (Benchmarking)
- Call-Off Schedule 17 (MOD Terms)
- Call-Off Schedule 20 (Call-Off Specification)

4. CCS Core Terms
5. Joint Schedule 5 (Corporate Social Responsibility) - Mandatory

Supplier terms are not part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

Call-off Special Terms

The following Special Terms are incorporated into this Call-Off Contract:

Special Term 1 - The Buyer is only liable to reimburse the Supplier for any expense or any disbursement which is:

(i) specified in this Contract or
(ii) which the Buyer has Approved prior to the Supplier incurring that expense or that disbursement. The Supplier may not invoice the Buyer for any other expenses or any other disbursements.

Special Term 2 - Primary Quality Assurance Standard Requirements – No specific Quality Management System requirements are defined. This does not relieve the Supplier of providing conforming products under this contract. Certificate of Conformity shall be provided in accordance with DEFCON 627.

Special Term 3 - Quality Plans – No Deliverable Quality Plan is required, reference

DEFCON 602B Edn. 12/06.

Special Term 4 - Concessions – Concessions shall be managed in accordance with Def Stan. 05-061 Part 1, Issue 7 – Quality Assurance Procedural Requirements – Concessions.

Special Term 5 - Contractor Working Parties – Any contractor working parties shall be provided in accordance with Def Stan. 05-061 Part 4, Issue 4 – Quality Assurance Procedural Requirements – Contractor Working Parties.

Special Term 6 - Security - The Supplier confirms that Supplier Staff working on Buyer Sites and on Buyer Systems and Deliverables hold a valid SC Security Clearance at the start of this contract.

Special Term 7 - Working Arrangements - A hybrid arrangement will be in place consisting of both onsite and remote working. Supplier staff will be expected to attend meetings within standard office hours. Supplier staff will be expected to attend site as and when required, dependent on business need.

Special Term 8 - Security Aspects Letter – The Supplier has confirmed compliance with the Security Aspects Letter for this Contract.

Special Term 8: Cyber Security – In compliance with DEFCON 658, the Risk Profile for this contract has been assessed as “N/A”. The Risk Assessment Reference is: RAR - 250527A02.

Special Term 9: Maximum Liability – For the purposes of determining the Supplier’s Limitation of Liability under Clause 11.2 of the Core Terms this Framework Order Form this Special Term 9 shall amend the Supplier’s Liability Maximum to £2,220,000.00 for the term of the contract.

Special Term 10: Assumptions and Dependencies – the Supplier's performance is dependent upon the Buyer meeting the following obligations, any failure to meet these obligations would result in an authority cause (in line with core term 5). See Appendix A for a list of the Assumptions and Dependencies.

Special Term 11: Risks Associated with Delivery – this delivery introduces further additional risk as detailed in Appendix B. Risk will be managed through RAID review sessions (workstream and programme), documenting, reporting and tracking. If any of the dependencies lead to a risk to the delivery or the timelines for delivery, or there is a material change requested to the Plan and/or assumptions, the Supplier will: highlight any significant risks to the Buyer project sponsor; seek to mitigate the risk and, if necessary, propose a mitigation plan to the Buyer for approval. Where the Supplier cannot mitigate the risk, the Supplier will detail the impact of the risk and seek approval of the assessment and any associated mitigations that may include amendments to this contract.

Special Term 12 – Off-Payroll Working – The Supplier has confirmed that all resources delivering to this Contract are PAYE. Should this change, the Supplier shall notify the Authority, who may be required to review the IR35 status of the Contract. The Authority shall inform the Supplier of any changes and necessary steps required.

Call-off start date: 9th June 2025

Call-off expiry date: 6th March 2026

Call-off initial period: 9 Months

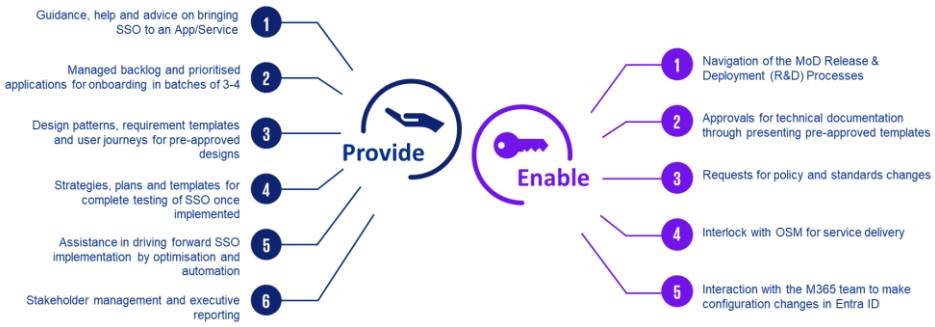
Call-Off Optional Extension Period:
BREAK POINTS
The Authority reserves the right to invoke a contract break point on 8th December 2025. This break point shall come into effect unless notified otherwise by the Authority's Commercial Representative no later than 30 calendar days before the break point date. The break points are linked to the Authority's funding position; therefore, the Authority does not commit to any spend under this contract following the break point without formal instruction to the Supplier. The Authority will not be liable for any cost incurred by the Supplier following the break point unless formal instruction from the Authority's Commercial representative has been received confirming that funding for the period following each break point has been approved.

Call-off deliverables:

Below are listed the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract:

Deliverable	1 – SSO Delivery
Outcome	Continuance of the established Single Sign On (SSO) Centre of Excellence (CoE) within Digital Identity for Defence (DIfD) including implementation of the developed SSO Onboarding Blueprint approach and enablement of the rapid onboarding of applications to Microsoft Entra ID at Official to realise enhanced security and user benefits. Target: 20* applications onboarded to Entra ID for SSO over a 6+3 month period but not limited to and exceeded where possible. Priority given to On-Prem SSO NETIQ IdAM catalogue and particularly the HR System applications within that live service catalogue, subject to assumptions and dependencies as outlined in Appendix A of this document. Further application onboarding subject to application complexity, Defence priorities and external dependencies (M365, SLA agreements etc). Identification of requirements for attributes to enable SSO that are out of current Entra ID scope are discovered. Mitigations or 'business requirements captured' from the app owners confirming the necessity of these attributes in accordance with Data Centric Security. To be fed back to the Core Prg Delivery Manager and Data workstream to enable Schema 1.3 reviews. Completion of the onboarding of the applications already selected for live (success is dependent on agreement of SLAs (between M365 and application owners) and, M365 configuration into SIT and onboarding to live).

	Address opportunities and priority onboarding to increase MFA coverage at OFFICIAL via including the HR System applications within the established conditional access policies. ** A full list of dependencies to enable a successful outcome is captured at Appendix A. To ensure all On-Prem SSO NETIQ IdAM catalogue and HR System applications are transferred to Entra ID with SSO enabled one of the following dependencies needs to be met:* • *MODNET O is transitioned to MNO thereby providing enriched identity attributes within Entra ID to meet application requirements.* • *Entra ID identity attributes are enriched directly from NetIQ prior to the MODNET O to MNO transition.* • *On-Prem SSO NETIQ IdAM catalogue and HR System applications accept transition from NetIQ to Entra ID with reduced short term attribute availability.*
Description	Provision of Project Management, Business Analysis, Architecture, Development and Testing to: a) Provide a Centre of Excellence within DIfD to enable onboarding of applications for SSO, b) Implement and refine the SSO Blueprint framework, c) Identify high security applications that would benefit from MFA coverage via the existing Conditional Access Policy for the Live SSO / MFA service.

Activities and Approach	**Activities** The CoE will facilitate the delivery of SSO to applications through a prebuilt process. As part of this, the CoE will support app owners with specialised knowledge and expertise to accelerate SSO delivery. Additionally, the CoE will manage and enable clear governance and processes to control and streamline activity, improve efficiency and ensure consistency. Activities include:  **Approach** The PM will oversee all application onboarding to Entra ID on MODNET O applying Scaled Agile Framework (SAFe) principles and methodology

to develop a comprehensive Backlog of applications and to deliver outcomes in an agile and efficient manner.

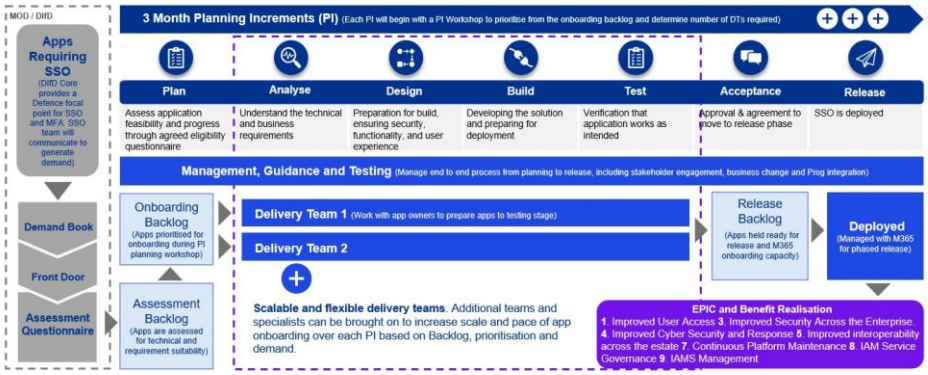
The PM will integrate with the DIfD Prog Core Delivery Manager to prioritise the transition from On-Prem IdAM Live service applications to Cloud and where possible to generate requirement through the Defence Digital Demand Book and Front Door, building an extensive Onboarding Backlog and co-ordinating a concurrent pipeline of application onboarding activity.

In line with the SSO Blueprint concept, work will be pushed application side for economies of CoE resources and to ensure VfM.

This will be done by:

- Establishment of a CoE to provide specialist knowledge, expertise, innovation and continuous improvement. Transferring that knowledge to Crown Resource where possible.
- Enactment of the SSO Blueprint, ensuring all stakeholders understand their roles and necessary steps to accomplish successful implementation of SSO.
- Implementation of clear governance and process to control and streamline activity, improve efficiency and ensure consistency.
- Coherence of dependant teams and resources.
- Exploitation of security controls and protocols available within Entra ID.

The CoE will follow a SAFe methodology, building a backlog, prioritising delivery over 3 x 3-month Planning Increments (PI) to meet demand, technical and security prioritisation as shown in the diagram below.



- **PI 1**. Focus will be on the identification of applicable applications from across the MODNET O environment; building of a comprehensive application Onboarding Backlog; analysis and design of selected applications with prioritisation given to the OnPrem SSO NETIQ IdAM catalogue and HR applications. By end of PI 1, a target of a minimum of 5 further applications will be ready within the Release Backlog for deployment to live.

- **PI 2**. Focus will be on the Design, Build, Test and Release of applications from the onboarding backlog. Prioritisation will again be given to On-Prem SSO NETIQ IdAM catalogue and HR applications. By end of PI 2, a target of a minimum of 10 further applications will be ready within the Release Backlog for deployment to live.

- **PI 3**. (subject to extension) Focus will be on the completion of onboarding all remaining On-Prem SSO NETIQ IdAM catalogue and HR applications. By end of PI 3, a target of all remaining OnPrem SSO NETIQ IdAM catalogue applications will be ready within the Release Backlog for deployment to live.

Resource

A CoE SSO model comprised of Project Manager (PM), SSO Architect, Test resources and scalable resource or multiple Delivery Teams (DT) (each DT to consist of Business Analysist and Engineer) to Manage, Plan, Analyse, Design, Build, Test and Release applications for SSO on MODNET O. A description of roles, grades and responsibilities is shown on the table below.

Role	SFIA grade	Responsibilities
Project Manager (PM)	5	• Manage the backlog and prioritise applications for onboarding in batches of 3-4 (adjust based on team capacity and application complexity). • Manages project timeline, budget, and resources. • Facilitates RAID meetings to track and escalate issues. • Provides regular status reports and updates to stakeholders. • Oversees SSO integration deployment and post-deployment support.
SSO Architect	5	• Designs overall SSO architecture, defines technical standards/best practices. • Collaborates with PM/BA to understand application needs and map to SSO architecture. • Oversees technical implementation of SSO solutions, works with Engineer. • Reviews onboarding questionnaire, participates in user research, provides input on schedules, receives tester feedback.
Tester	4	• Develops/executes test cases, verifies functional/security requirements. • Reports and documents test results, works with Security Engineer on resolutions. • Provides feedback to SSO Architect and BA.
Business Analyst (BA)	4	• Gathers and analyses business requirements, defines user roles/access/security. • Runs the user journey definition. • Provides input on testing and validation. • Documents SSO integration process and requirements. • Works with SSO Architect on requirements.
Engineer	4	• Configures and secures SSO integration. • Works with Application owners, M365 team, and SSO Architect on technical tasks (coding, scripting, config).
Specialists	5-4	• Automation • On prem AD • NetIQ

Support

Support will include storing/uploading of key Core artefacts, including the RAID log and decision log; contributing where needed of Core ‘delivery SSO /MFA only’ artefacts for Programme Board and other governance forums; The PM will escalate key risks and issues impacting at a programme level, interfacing with the programme PMO.

Boundaries	The technical boundary is to use Entra ID via M365 (OFFICIAL) only. Noting the Supplier is unable to onboard any applications to Cloud SSO without cooperation and support from M365. Support and engagement is also needed from the application teams therefore, delivery is dependent
	upon these teams. A good working relationship is required with a collaborative mindset. Existing LLD and process templates are readily available and should be used in first instance. Technical coherence from Foundation IdAM live Service and technical leads for Foundation and Service Architecture are expected to support supplier with knowledge sharing for the Live Service transition and any de-risking work should be passed to the supplier PM within 7 days of contract award.
Dates	9 June 25 – 6 March 2026
Duration (months)	6 months, with 3 month extension subject to Authority approvals
Success Criteria	HR systems are offboarded from the on-prem IdAM live service to Entra M365 MODNET/MNO cloud environment for SSO and included in the MFA conditional access policy. 100% of applications that can be offboarded from IdAM Live service have been transitioned. Impact understood and articulated to the app owner and Service Owner for acceptance for those that do NOT wish to transition or can NOT transition due to technical debt or external resource/dependencies that can not be met. Additional* backlog of applications onboarded to Cloud SSO. *Number of applications subject to Application Team readiness, application complexity, technical compatibility, application owner compliance and M365 capacity to support delivery.

Security
Part A (Short Form Security Requirements).

Short form security requirements apply and the Supplier shall adhere to the SAL specified by the programme.

Maximum liability
The limitation of liability for this Order Contract is stated in Clause 11.2 of the Core Terms as amended by the Order Form Special Term 9.

Call-off Charges

1092 days will be utilised on this Contract and are split as shown in the table below.

Item	Minimum Days	Onboarded individuals
Management and Governance	42	2
Project Management	118	1
Architecture Support	81	0.5
Delivery Teams	567	3.5
Testing Support	264	2
Specialist Support	20	1

The agreed blended day rate in relation to the days set out above is [redacted] and (assuming there are no variations or delays related to dependencies) the total contract value is £1,150.000 Ex VAT (Firm Price).

Charge Breakdown

Deliverable	Charge
Project Management	[redacted]
Architecture Support	[redacted]
Delivery Teams	[redacted]
Testing Support	[redacted]

Management, governance and technical support costs as a fixed element have been factored into the above charges pro-rate.

Payment Milestones

Total contract value will be charged equally over 9 payment milestones at £127,777.78. A breakdown of each payment milestone is shown in the table below.

Deliverable	Charge per month
Project Management	[redacted]
Architecture Support	[redacted]
Delivery Teams	[redacted]
Testing Support	[redacted]

<u>Special Discount</u>
The rate and contract value set out above has been significantly discounted to the MCF3 rate card and does not represent an undertaking to apply the provided prices to any variation notes or future contracts. Variations shall be charged at standard MCF3 rates unless otherwise mutually agreed.

All changes to the Charges must use procedures that are equivalent to those in Paragraphs 4, 5 and 6 (if used) in Framework Schedule 3 (Framework Prices).

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of:

- Specific Change in Law
- Benchmarking using Call-Off Schedule 16 (Benchmarking)

Reimbursable expenses
All expenses for locations outside of Corsham must be pre-agreed between the Contractor supplier and Authority Project and Commercial Representative and must comply with the Authority's Travel and Subsistence (T&S) Policy. For the avoidance of doubt attendance and meetings at Corsham will not be reimbursable.

Payment method
The MOD electronic purchasing system CP&F will be used.
Buyer's invoice address
Invoices must be issued via CP&F

FINANCIAL TRANSPARENCY OBJECTIVES
The Financial Transparency Objectives do not apply to this Call-Off Contract.

Buyer's authorised representative

[redacted]

Buyer's security policy
Appended at Appendix 1 to this Schedule 6 Order Form

Supplier's authorised representative

[redacted]

Supplier's contract manager

[redacted]

Supplier's Data Protection Officer

[redacted]

Progress report frequency

Report	Frequency	Contents	Format
Programme Status and progress report	Weekly	As agreed between the Parties (within 30 days of Contract award)	Electronic readable format (Word or PDF)
KPI Performance Re-port	Monthly	As agreed between the Parties (within 30 days of Contract award)	Electronic readable format (Word or PDF)

Progress meeting frequency

Meeting	Frequency	Lead	Location
Phase Checkpoint Review	As agreed between the Parties but no later than two weeks prior to phase delivery	Supplier	Corsham (or via Teams)
Delivery and Performance Review Meetings (DRMs)/ Operational Board	Monthly	Authority	Corsham (or via Teams)
Change Advisory Board (CAB)	Monthly (or Ad Hoc as required)	Authority	Corsham (or via Teams)
Contract Performance Review	Monthly (or Ad Hoc as required)	Authority	Corsham (or via Teams)

Key staff

[redacted]

Key subcontractor(s)
No Sub-contractors have been identified for the delivery of this SOW.

Commercially sensitive information
Contract Pricing and preceding Commercial email correspondence relating to the contract.

Service credits
Please refer to Call-Off Schedule 14 (Service Levels)

Additional insurances Not applicable

Guarantee
Not applicable

Buyer's environmental and social value policy
Appended at APPENDIX 2 to this Schedule 6 Order Form.
Social value (SV) commitment
The Supplier agrees, in providing the Deliverables and performing its obligations under the Call-Off Contract, that it will comply with the social value commitments in Joint Schedule 5 (Corporate Social Responsibility). The proposed activities are described below. The Supplier will work with the Buyer's SV lead to ensure that these activities align with the Buyer's objectives and if necessary mutually agree alternative approaches.

Social Value #1 – Fighting climate change MAC4.2. - Mitigating climate change: working towards Net Zero: SV1: Total CO_2e generated from travel / offset

On this contract, we will implement a Sustainable Travel Policy reducing un-necessary travel and, where travel is required, using public transport or car-pooling to reduce CO2e. We will measure and report quarterly on CO2e generated by our travel using our Carbon Traveller Dashboard and use these metrics to improve our performance. We will offset CO2e from travel in a UK based carbon reduction programme. This will influence our staff and suppliers' staff behaviours by demonstrating how significant positive impacts can be achieved with minimal inconvenience.

Social Value #2 – Influencing support for health and wellbeing – MAC 7.2: SV2: Monthly wellbeing check-ins with project team and participating team members from the Buyer

During the period of the contract we will share our approach to health and wellbeing with the joint team (including MOD), supporting their welfare and equipping them with approaches and techniques to take onto other projects. Together we will use our bespoke 'Wellbeing EDGE' tool to create a wellbeing baseline and a project charter outlining individual working styles, priorities, caring responsibilities, and other considerations (e.g. neurodiversity). Where there are gaps, we will provide your team with access to the resources available to KPMG team members.

Formation of call off contract
By signing and returning this Call-Off Order Form the Supplier agrees to enter a Call-Off Contract with the Buyer to provide the Services in accordance with the Call-Off Order Form and the Call-Off Terms.

The Parties hereby acknowledge and agree that they have read the Call-Off Order Form and the Call-Off Terms and by signing below agree to be bound by this Call-Off Contract.

For and on behalf of the Supplier:

Signature:
[redacted]

Name:
[redacted]

Role:
[redacted]

Date: 9 June 2025

For and on behalf of the Buyer:

Signature:

[redacted]

Name:

[redacted]

Role:

[redacted]

Date: 10 June 2025

Appendix A: Assumptions and Dependencies

In accordance with Call Off Special Terms 10, see below the list of assumptions and dependencies. In addition to these listed, the existing RAID log will also be used.

- The supplier is dependent on the DIfD Programme and the Foundation project providing the necessary attributes from NETIQ to Entra ID to enable On-Prem SSO NETIQ IdAM catalogue and HR applications onboarding to Entra ID.
- The delivery of onboarding on-prem applications to Entra ID is dependent on the MNO go-live to facilitate the necessary attributes being available. If this is not met, then the project won't be able to onboard all On-Prem SSO NETIQ IdAM catalogue and HR applications.
- The supplier is dependent on the On-Prem SSO NETIQ IdAM catalogue and HR applications accepting going live without the full attribute set if the MNO migration has not completed before the end of this contract.
- The supplier is dependent on application teams supporting being onboarded to SSO complying and adhering to all deadlines throughout the onboarding process. The supplier is not responsible for any delays caused by application teams not meeting any given deadlines.
- The supplier is dependent upon the M365 team to facilitate the application onboarding process to SSO. In particular, the supplier is dependent on M365 enabling applications to progress to SIT (to facilitate testing) and then progressing to live once testing is completed. The supplier will not be held accountable for any delays caused by the M365 team.
- The Supplier is dependent upon the Buyer providing proposed and currently engaged staff with timely access to the Buyer's tools and systems (through allocation of accounts, hardware i.e. laptops and access of appropriate resources (e.g. Jira and Confluence) and that all relevant Supplier software required for delivery carries appropriate licencing for the purpose of such delivery.
- The Supplier is dependent upon timely decision making by the Buyer and its decision makers. If this is not met, then progress may be significantly delayed/hindered through lack of decision making.
- The Supplier is dependent on a suitable Programme Manager remaining in post for the duration of the delivery. This Programme Manager must be suitably familiar with the programme and ways of working. If this is not met, then the Supplier will need to onboard a Programme Manager resource to fill this gap. This would be at an additional cost to the Buyer.

- The Supplier is dependent upon support and timely cooperation of the NetIQ team to achieve any agreed outputs within the agreed timelines in order to be able to deliver any of the NetIQ-dependent work. If this dependency is not met, then the Supplier may be unable to fulfil this activity and therefore may need to issue a variation note to amend the scope.
- The supplier assumes that all in scope application teams support the move from applications being held On-Prem - NETIQ and moving to cloud based Entra ID. If this is not true, then the supplier may be unable to onboard all requested applications to Entra ID.
- It is assumed that on-prem applications will be content to go-live on cloud SSO without the full attribute set, if MNO is not delivered to time. If this is not true, then applications may be removed from the scope of this delivery contract.
- It is assumed that any surges required by third parties to accommodate the intensity of rollout are funded, facilitated and managed by the Buyer.
- There is an assumption that over the Christmas holiday period (15/12/2025 – 05/01/2026) the majority of the team would stand down for approximately three weeks.
- It is assumed that the DIfD Programme PMO will remain in place for the duration of this variation. If this is not true, additional PMO resource may need to be onboarded to perform activities that are necessary to enable the programme to continue.
- It is assumed that the Buyer will have end to end accountability for Programme Management.
- It is assumed that the Buyer will maintain responsibility for coordinating and managing any third party Service Providers.
- It is assumed that, where appropriate, the Supplier will use technology to work remotely by default and implement a Sustainable Travel Policy for our people, travelling to the Buyer’s sites (identified and agreed at the time of contracting) only where required.
- It is assumed that the Buyer will retain the responsibility for establishing and maintaining an effective internal control and governance structure.
- It is assumed that the Supplier will not perform any management functions, nor make any decisions for the Buyer, and while the Contractor may provide advice, responsibility for all related decisions and their consequences are the Buyer's responsibility. The Buyer will appoint someone of management-level with the skill, knowledge, and experience necessary to be responsible for overseeing the Services provided, evaluating their adequacy, and monitoring ongoing activities.
- It is assumed that any delay caused by lack of office facilities or technology and network unavailability at the Buyer’s sites will be the responsibility of the Buyer, which may incur additional costs that the Supplier may seek to recover.

Appendix B: Risks Associated With Delivery

Per special term 11, see below the list of risks associated with delivery. In addition to these listed, the existing RAID log will also be used.

- There is a risk that the other supporting teams (mainly M365) become overwhelmed by the pace of the SSO implementation and become unable to support the implementation. This would result in the SSO implementation either being paused, or slowing down. Rollout planning will be conducted in collaboration with the M365 team, and any adjustments in rollout pace will be approved by the Buyer’s leadership, who will be made aware of the impact of any such adjustments.

- There is a risk that the other supporting parties for implementation, such as application teams, will not provide necessary pre-requisites in time to enable the SSO implementation. Regular management and tracking of dependencies and their impact on delivery timelines will be undertaken through the weekly RAID sessions, as well as contract performance reviews and ad-hoc escalations as required.
- There is a risk that the MNO programme will be delayed or may not go live during the course of this engagement. If this risk materialises, then applications which are currently within the On-Prem SSO NETIQ IdAM will not be able to move to cloud SSO, or would have to accept going live without the full attribute set.
- There is a risk that, if the delivery is not extended past the original 6-month period, that application that are currently on-prem, will be unable to go live with the full attribute set, as the migration to MNO may not have been completed in sufficient time prior to the end of this contract. If this risk materialises, then on-prem applications must either accept going live without the full attribute set, or the project will reprioritise applications which are already on the cloud to enable application onboarding to continue.