Appendix 1: Services

1. GENERAL

This Appendix 1 (Services) sets out the scope of the Services that the Supplier is required to make available under the Framework Agreement and which may be purchased by Customers under Call-Off Contracts.

2. GENERAL DEFINITIONS OF THE CLOUD SERVICES PROVIDED

Under this Framework Agreement the Supplier shall deliver and provide services as described in this Appendix through the public internet and/or other government and DFØ approved network and without requiring any further ICT infrastructure than a customer of the products and services would reasonably be expected to already have access to; and deliver products and services that will comply to the NIST Definition of Cloud Computing set out below[1].

Below, we refer to the Platform as the digital solution used to deliver the Services. With Services, we refer to all elements off the requested scope, which includes the Platform.

3. DELIVERY MODELS UNDER THE FRAMEWORK AGREEMENT

The Supplier shall have the ability to simultaneously deliver the Services via Software as a Service (SaaS) service model as described in the NIST definition below:

> "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

[1] https://csrc.nist.gov/pubs/sp/800/145/final

4. SCOPE UNDER THE FRAMEWORK AGREEMENT

The scope under this Framework Agreement encompasses services for general training and awareness in information security and data protection, which aim to enhance knowledge and readiness among employees. These services include a variety of training and awareness platforms, which may be referred to as “security awareness computer-based training” by Gartner and “security awareness and training solutions” by Forrester. Leveraging diverse content and tools—such as e-learning modules, interactive simulations, role-based training, and phishing campaigns—these services are intended to support Norwegian public entities by strengthening employees' understanding of security best practices, improving overall preparedness, and fostering a proactive security culture across the organization.

5. THE PURPOSE OF THE FRAMEWORK AGREEMENT

Information security is critically important to the Norwegian government and public sector. The purpose of this Framework Agreement is to provide public sector entities with effective tools and services for general security training and awareness, aimed at strengthening organizational security culture and reducing human-related security risks.

This includes implementing a cloud-based SaaS solution for information security and data protection training and awareness that offers flexible access and scalability without the need for extensive infrastructure investments, with the capability to:

a) Deliver information security and data protection training and awareness programs covering a wide range of topics, such as fundamental security principles, phishing prevention, and handling sensitive data, tailored to all employee levels.

b) Provide analytics and reporting to give a comprehensive overview of the organization’s security culture and areas needing improvement.

c) Generate actionable insights, visualizations, and reports to help stakeholders understand the importance of security awareness, identify vulnerabilities, and assess potential risks.

d) Support strategic oversight through executive-level reporting, customizable dashboards, and assessments that assist leadership in making informed decisions about resource allocation and prioritization of security initiatives.

e) Facilitate operational follow-up by offering monitoring, tracking, and reporting on training progress and security metrics to evaluate the effectiveness of training programs, measure compliance, and identify areas for improvement.

6. REQUIREMENTS

Explanation to the requirements in the table below:

All requirements specified in 6.1 Functional requirements and 6.2 Technical requirements are subject to evaluation under the award criteria quality. The requirements shall be answered with **yes, partially** or **no**. Regardless of the response, suppliers are expected to provide short description (max 100 words and up to two screenshots per answer) in the right column to explain how the requirement is met, or, if the response is **"partially"** or **"no"**, which aspects are not fulfilled and why.

The description should be concise and, where relevant, include examples, screenshots or references to support documentation to demonstrate compliance. The evaluation will be based on the written answer (maximum 100 words and up to two screenshots per answer). The parts of the descriptions that exceed 100 words will not be read. Provided References/ Reports shall only be provided as documentation of compliance and descriptions therein will not be evaluated. Any deviations to requirements must be provided as part of the written answer (maximum 100 word). Deviations in references/attachments/reports etc. will not be considered agreed.

6.1 Functional requirements

ID	Requirement text	Please confirm Yes/No or Partially	Short description (Max 100 words)
F1	**Course Content** The Platform should cover basic topics in information security and data protection, such as phishing, social engineering, password security, GDPR, and compliance. These modules should provide a solid foundation in general information security and data protection awareness for employees.	Answer	

F2	**Delivery** Access to the Platform should be integrated with the Customers' IT workplace tools, supporting multiple communication channels, such as e-mail, Teams and SMS, to ensure maximum employee engagement.	Answer	
F3	**Engaging and Interactive Learning** The Platform should provide continuous learning programs that utilize multimedia elements such as videos, animations, quizzes, gamification and phishing simulations to make the learning process engaging, and train employees effectively.	Answer	
F4	**Content customization and Personalization** The Platform should allow for customization of training programs based on sector-specific content needs and specific organizational needs. It should also offer customizable training schedules and reminders to ensure employees can complete training at their convenience.	Answer	
F5	**Role-based training** The Platform should allow for customized training for specific user groups, such as top leadership teams, personnel managers, and IT specialists.	Answer	
F6	**Progress Tracking and Reporting** Administrators should have access to dashboards that monitor user progress and completion rates. The Platform should provide detailed analytics and performance reports to track the effectiveness of the	Answer	

	training program, identify knowledge gaps and areas for improvement. It should be possible to restrict and/or anonymise employee personal information if required.		
F7	**Strategic oversight** The Platform should provide executive dashboards and reports specifically meant for leadership to follow up on the effectiveness and impact of the service.	Answer	
F8	**National situational awareness** It should be possible to grant relevant Norwegian national authorities access to aggregated data from the platform, such as course topic completion rates, user attendance, and scoring levels, to enable assessment of the level of awareness in the public sector and identify areas for improvement.	Answer	

F9	**Data export formats** Reports and data should be able to be exported in various formats, as minimum PDF and CSV.	Answer	
F10	**Certificates of completion** The Platform should offer certificates of completion or similar form of reward to users who successfully complete the training modules.	Answer	
F11	**Multilingual Support** The Platform should offer training materials in multiple languages, including Norwegian (Bokmål and Nynorsk), Samisk and English, to cater to a diverse workforce, ensuring that all employees can benefit from the training.	Answer	
F12	**Feedback** The Platform should have mechanisms for users to provide feedback on the training content.	Answer	
F13	**Onboarding** The Supplier should provide a scalable and efficient process to ensure seamless onboarding and integration of new Customers and its' users, including any necessary and/or recommended establishment services and/or user training to enable full use of the Services.	Answer	

F14	**Framework agreement performance management** DFØ should have access to aggregated performance statistics to monitor the effectiveness and impact of the Services through use of the licenses provided under section 2 of the Framework Agreement.	Answer	
F15	**Free Trial Period** The Supplier should provide a free trial period with full access to the Services for a period, allowing Customers to evaluate the Service's capabilities before committing to a payable subscription with a seamless transition to a paid plan.	Answer	
F16	**User Support** The Services should include a user support framework to assist the Customers' end users with any questions regarding use of the Services, e.g. a contactable help desk and/or user guidance documentation	Answer	

F17	**Training** The Supplier should offer training to Customers' end users in use of the Services, e.g. training sessions or training material included as part of the Services and/or the possibility to separately procure training seminars	Answer	

6.2 Technical requirements

ID	Requirement text	Please confirm Yes/No or Partially	Short description (Max 100 words)
T1	**Scalability and Performance** The Platform should be cloud-based to support thousands of concurrent users without performance degradation. It should be optimized for scalability to handle large numbers of employees simultaneously.	Answer	
T2	**Data Encryption** The Platform should implement strong encryption according to best practices for all customer data, including personal information, at rest and in transit. Data transmitted to and from the API should be encrypted using current standards, such as TLS 1.3.	Answer	
T3	**APIs and integration** The Platform should offer well-documented and secure APIs, enabling seamless integration with other security tools, data sources, and HR/management systems to allow for enhanced data exchange, workflow automation, and the ability to leverage existing investments.	Answer	

T4	**Accessibility and Universal Design** The Platform should comply with universal design principles and must be accessible to all users, including those with disabilities, by adhering to standards such as Web Content Accessibility Guidelines (WCAG). It should feature scalable text, high color contrast, keyboard navigation, and screen reader compatibility. Content should use clear language, provide text alternatives, and include transcripts for multimedia. Interactive elements should be accessible and provide consistent navigation and feedback.	Answer	
T5	**Mobile Compatibility** The Platform should have a mobile-friendly design to support learning on various devices, including smartphones and tablets, allowing employees to access training anytime, anywhere.		
T6	**Technical support** The Services should inlcude a technical support framework to assist the Customers' IT personnel with any issues related to the Services, including any API interactions.	Answer	
T7	**Access control** The Platform should provide role-based access control to manage and restrict access to specific training modules, Platform dashboards and results.	Answer	
T8	**Authorization and Authentication** The Platform should include authorization and authentication mechanisms to ensure secure access to training materials	Answer	

	and user data. It should support Single Sign-On (SSO) to provide a seamless and secure login experience for users, integrating with enterprise identity providers such as Active Directory/EntraID, LDAP, or SAML-based services.		
T9	**Multi-factor authentication** The Platform should also include multi-factor authentication (MFA) as an additional security layer to protect against unauthorized access.	Answer	