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 the Call-Off Contract.

2. GENERAL DEFINITIONS OF THE CLOUD SERVICES PROVIDED

Under this Framework Agreement the Supplier shall deliver and provide services as described in the public internet and/or other government 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[1].

3. DELIVERY MODELS UNDER THE FRAMEWORK AGREEMENT

The Supplier shall have the ability to simultaneously deliver the products and services via Software as a Service (SaaS) service model as described in the NIST definition as 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."

4. SCOPE UNDER THE FRAMEWORK AGREEMENT

The scope under this Framework Agreement is Cyber risk score services, also referred to as "security rating services" by Gartner and "cyber security risk ratings platform" by Forrester, that leverage data from diverse sources, including the Internet, vulnerability scans, threat intelligence, open-source intelligence, and the dark web, to provide Norwegian public entities with comprehensive situational awareness, strategic oversight, and operational follow-up of its cybersecurity exposure on the internet.

5. THE PURPOSE OF THE FRAMEWORK AGREEMENT

Information security is of critical importance to the Norwegian government and public sector. The purpose of this Framework Agreement is to enable the Norwegian government and public sector entities to objectively measure their security risk on the internet in order to strengthen their security posture.

Implement a cloud-based SaaS solution for a cyber risk service that offers on-demand access and scalability without requiring extensive infrastructure investments with the possibility to:

a) Gather and securely analyse data from various sources on the internet, including vulnerability scans, publicly available information, and the dark web, to monitor and

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

assess potential threats that may impact Customer's' digital assets and/or sensitive information.

b) Provide analytics and present a comprehensive view of Customers' cyber risk landscape.

c) Generate actionable insights, visualisations, and reports to empower stakeholders in understanding emerging threats, vulnerabilities, and potential impacts on critical systems and networks.

d) Enable strategic oversight through executive-level reporting, customizable dashboards, and risk assessment capabilities to assist senior leaders in making informed decisions regarding resource allocation, prioritization of security initiatives, and proactive risk reduction.

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

6. REQUIREMENTS

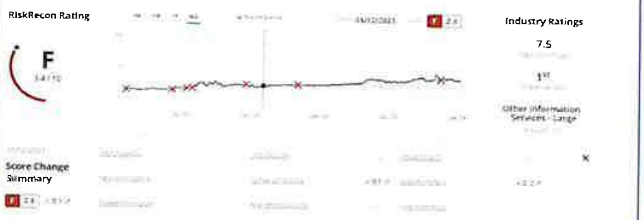
6.1 Functional requirements

ID	Requirement text	Please confirm Yes/No or Partially	Short description (Max 50 words)
F1	**General:** The platform should provide dashboards for Cyber risk score for different needs such as operational reporting, executive reporting, strategic oversight and trend analysis.	Yes	We use proprietary techniques to self-discover the company's IT profile, including all systems they register/manage themselves and the many outsourced. We capture the network, geolocation, host information. RiskRecon applies 1000's of proprietary algorithms to build a security profile. The profile is broad and deep, with 36 unique security criteria.
F2	**Data aggregation and sources:** The platform should support automated collection and processing from diverse sources, covering all the customers domain	Partially	RiskRecon sources 95% of its own data through proprietary systems that perform deep asset discovery of an organisation's internet facing systems and the passively collect data from those systems. The threat intelligence feed data comes from 100 reliable open source threat intelligence feeds along with large commercial feeds including darknet. As per tender offering, the scan does not include dark web as a source.

	names and IP-addresses exposed on the Internet such as network scans, vulnerability scans, threat intelligence, open-source intelligence, and the dark web.		
F3	**Risk scoring and prioritisation:** The platform should assign and categorize risk scores related to identified risks, threats and vulnerabilities affecting the customers domain names and IP-addresses. Such risks may for example be based on patching levels, exposed vulnerabilities (referring to CVE scores), DNS and network configuration, application security, and indicators of data breaches from open sources.	Yes	Risk-prioritised action plans with evidence necessary to mitigate risk and collaborate with suppliers. Our automated solution relies on advanced models and security analytics to prioritise actions based on each system's issue severity, and asset value. Based on CVE's, DNS, software-patching level, other vulnerabilities, open ports, bot, phising. And other mechanics.
F4	**Notifications and alerts:** The platform should provide functionality for defining notifications / alerts.	Yes	Unique to RiskRecon is the ability to create two sets of alerts. You can set alerts based on score changes for overall rating and/or any individual security criteria. You can receive alert when score drops by a certain amount or if it drops below a certain overall threshold.
F5	**Operational follow-up:** The service should provide functionality for extracting detailed technical reports and for managing follow-up of actions based on issues identified by the service.	Yes	One of the fundamental tenets of RiskRecon is that risk remediation and collaboration depends on your ability to share information internally and with your suppliers/vendors related to the risks observed. These risk policies are used to generate action plans focusing on the issues that are most important.
F6	**Executive reporting:** The platform should generate executive-level reports, and visualisations that give a comprehensive view	Yes	The portal has the capability to generate various types of reports, including exclusive reports and risk position reports for all the companies listed within the portal. These reports serve different purposes and provide valuable insights.

	of the organisation's cyber risk posture.		
F7	**Scanning frequency:** The platform should provide the entities with timely insights and actionable information, conducting regular and up-to-date scans of vulnerabilities, threat intelligence sources, open sources, and dark web forums.	Partially	Every 14 days we build an entire new company report. We have further the possibility via "Refresh Assessment" that DxO can run a new report build on demand. For the security domains/criteria we use around 120 open source intelligence tools that run 24/7 multiple times per day. This will be displayed in the section "Largest Score Drop" – means near to real time data. The nine security domains assessed by RiskRecon are Software Patching, Application Security, Network Filtering, Web Encryption, System reputation, Data Breach Events, DNS Security, Email Security and System Hosting. As per tender offering, the scan does not include dark web as a source.
F8	**Third-party risk management:** The platform should include features for assessing and monitoring the cyber risk posture of third-party vendors and partners, facilitating risk assessments, monitoring of vendor security performance, and reporting functionalities to support effective third-party risk management.	Yes	RiskRecon is the world's leading platform for easily understanding and acting on third-party cyber risk. All functionality, incl. shareable risk, prioritising action plans, that are available for building a cyber risk score of own entity is also available for assessing third-party vendors and partners.
F9	**Data export formats:** Reports and data should be able to be exported in various formats, as minimum PDF and CSV	Yes	The portal's versatile reporting capabilities allow users to generate reports and data that can be conveniently exported in multiple formats. These formats include PDF for professional presentation and CSV for easy data manipulation and analysis.
F10	**General:** The platform should have role-based access control	Yes	The platform features role-based access control with varying levels of control, including segmentation for vendors. Users can define and assign roles within the platform.

F11	**Strategic oversight:** Selected national and sector security entities should have access to the national domain portfolio, data access APIs, and dedicated access to supplier's cyber security subject matters experts at an appropriate level. The entities should get an overview across all Customers that are covered by the Framework Agreement (listed in Appendix 6), which can facilitate national oversight and control of information security challenges. Examples are (in Norwegian): Nasjonal sikkerhetsmyndighet (NSM), HelseCERT, JustisCERT etc.	Yes	Access levels are contingent upon the role you log in with. Top-level accounts have the capability to access a consolidated summary of all subdomains within the same portal hierarchy. In scenarios where multiple instances of the portal exist, the API can be employed to merge detailed findings and high-level scores. For more information about Subject Matter Experts, see Attachment 1.1.
F12	**Strategic oversight:** MPS should have access to the national domain portfolio and dedicated access to supplier's cyber security subject matters experts at an appropriate level. MPS should get an overview across all Customers that are covered by the Framework Agreement (listed in Appendix 6) The Contracting Authority's monitored data should, at a minimum, include aggregated and historical CVE (Common Vulnerabilities and Exposures) scores, starting from the implementation of the service. This data should be presented	Yes	RiskRecon's monitoring solution delivers risk prioritised findings that enable identification and elimination of your most critical security risks. Our service delivers the data-driven evidence necessary to rapidly pinpoint and remediate security weaknesses on the externally facing systems associated with the entities you wish to monitor. 

	through a dashboard user interface, which also includes prioritised information. Monitoring should also track the historical change in security scores over time. This tracking should include a sorted list by entities and their speed of adoption of necessary remediations. The monitored data provided to the Contracting Authority should support the entity's security management and organisational management in their strategic development of security policies. The data should include appropriate Key Performance Indicators (KPIs) to address these needs.		Historical changes are also monitored: 
F13	**Additional functionality and services** The Supplier should offer additional Cyber Risk Score functionality and services delivered through the platform, e.g. real time access, raw data access, access to additional modules/services, access to test and development modules, etc.	Yes	We provide, via API, access to all the data that we are collecting and maintaining in our 9 Domains and 39 Security criteria's. e.g. Host list, Domain Records, registered Netblocks, System reputation data, Software patching, E-mail security and more out of the box. Additional module supply chain risk module: The Supply chain feature was inspired by recent hacks and breach events that left many companies scrambling to understand the usage of vulnerable technologies within their supply chain. Cybersecurity risk managers have historically struggled to capably track the arms-length relationship of supply chain connections due to many reasons: e.g.: organisations may know who their third parties are, but rarely know the full scope of their fourth parties. RiskRecon is helping to address these challenges with the new supply chain module. To enable this increased level of 3rd and 4th party visibility.

6.2 Technical requirements

ID	Requirement text	Please confirm Yes/No or Partially	Short description (Max 50 words)

T1	**APIs and integration:** The platform should offer well-documented and secure APIs, enabling seamless integration with other security tools, data sources, and management systems to allow for enhanced data exchange, workflow automation, and the ability to leverage existing investments.	Yes	The API, built using Swagger, provides developers with a framework for designing, building, documenting, and consuming RESTful web services. Clients can pull data from the API with the same information available in RiskRecon risk assessment reports. Updates occur on the same schedule as the portal.
T2	**Machine learning/artificial intelligence:** The platform should leverage machine learning / artificial intelligence capabilities, enabling more effective and proactive insights into emerging threats and vulnerabilities.	Yes	The first time RiskRecon produces a report for an organisation, one not currently monitored by RiskRecon, analyst assisted/Driven automation is used to train the machine learning model that is used to perform subsequent analysis of the target organisation in question. Once the initial assessment is performed, subsequent analyses are fully automated and performed on a regular basis. With that said, quality assurance thresholds are in place to trigger analyst review when changes from one analysis to the next deviate from acceptable thresholds. We use our own proprietary mechanisms on AI.
T3	**Support for IPv6:** The platform should support IPv6. This support should extend to data gathering, analysis, reporting, and any other relevant platform functionalities.	No	It has been our experience that the vast majority of relevant public/internet facing assets are discoverable via IPv4 either natively (dual stack IPv4/IPv6) or through IPv4/IPv6 Network Address Translation (NAT). As such, we have had no issues supporting customers with IPv6 implementations.

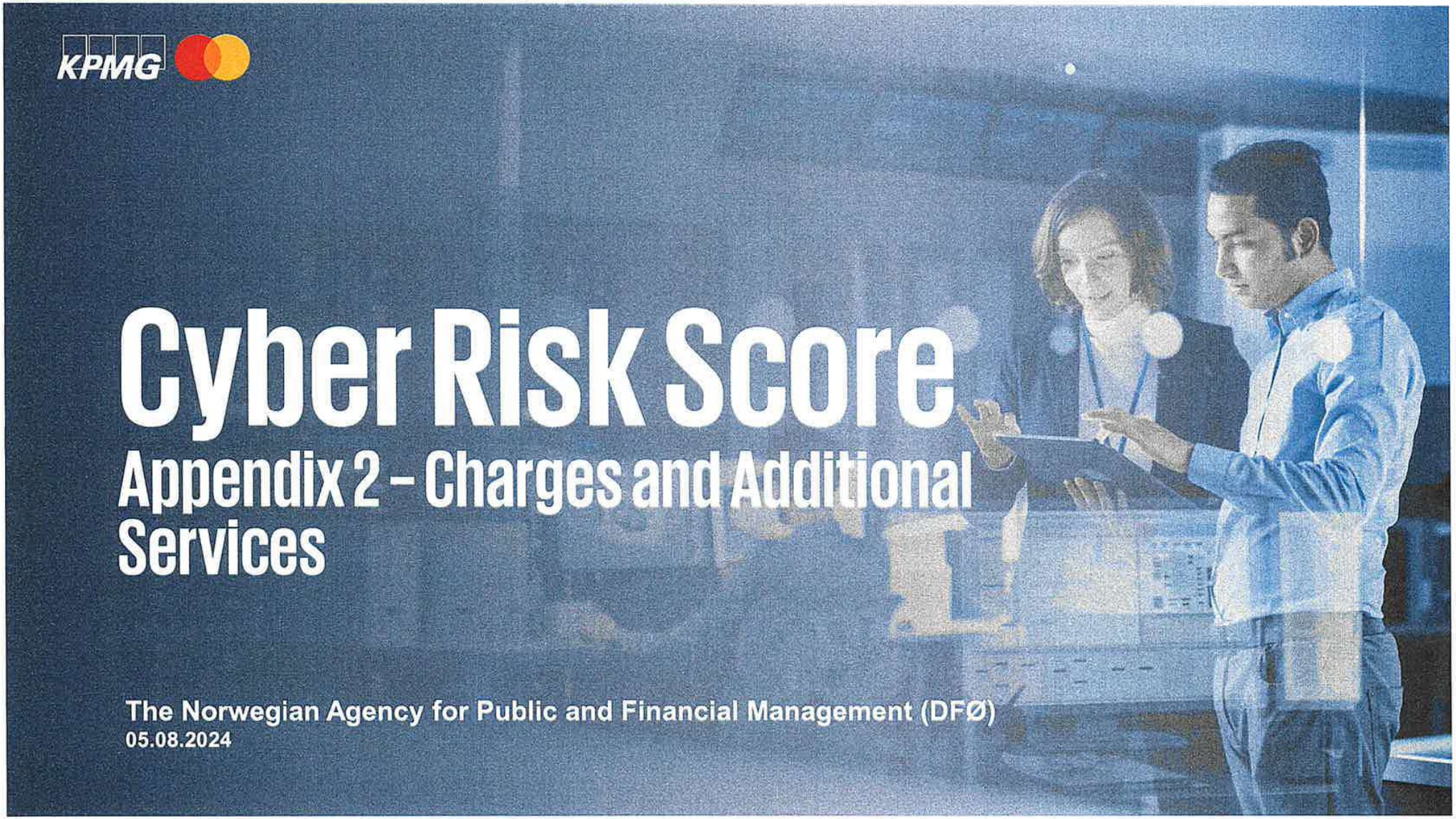
T4	**User-friendly interface:** The platform should provide a user-friendly interface that accommodates both technical and non-technical users, enabling easy navigation, data interpretation, generation of reports, and interaction with the platform's functionalities. Intuitive visualisations and interactive controls should enhance the user experience. The evaluation, includes: • Help functions: Easy access to help functionality to educate and guide users of the platform. • Responsive design: The layout and elements of a website or application automatically adjust and adapt to different screen sizes and devices. • Browser support: The service fully supports all commonly used web browsers.	Yes	RiskRecon has an industry-leading average rating of 4.6 stars on Gartner Peer Insights. The platform provides the information relevant to your role and can be used by different functions. Extensive integrated library including videos and FAQs with online support.
T5	**Cloud infrastructure:** The platform should be built on a secure and reliable cloud infrastructure that ensures availability, scalability, performance, and data redundancy, providing a robust foundation for delivering the SaaS solution.	Yes	The platform is built on AWS's industry leading cloud platform with full redundancy to be resilient, scalable, and secure, ensuring availability, performance, and data redundancy.
T6	**Multi-factor authentication (MFA):** The platform should provide MFA capabilities to strengthen user authentication and access controls.	Yes	RiskRecon is using SAML standard

6.3 Free trial and onboarding

ID	Requirement text	Please confirm Yes/No or Partially	Short description (Max 50 words)
FT1	**Free Trial:** When receiving a Call-off from a Customer, the Supplier should offer a free trial for a minimum period of three months. The free trail should meet the same requirements as per the Framework Agreement. During the free trial period the Customer should be able to exit/terminate free of charge and without any obligations. The first-year contract period will therefore be 3 + 12 months.	Yes	All potential customers can be pre-registered in platform and immediately get access to all functionality for own entity. Entities also gain access to onboarding materials. Customers may cancel anytime during the trial.
FT2	**Onboarding** The Supplier should offer an onboarding process to the Customer. This should be included in the agreed fee. The Supplier may choose to organise their onboarding process as a staged onboarding.	Yes	The onboarding program is designed by KPMG and Mastercard to make customers gain benefits from the use of RiskRecon as quickly as possible and build internal skills and knowledge.

7. TRAINING AND SUBJECT MATTERS EXPERT

7.1 The supplier offers different training courses and access to Subject Matter Experts. Information about the content of the training courses and subject matter experts are set out in Attachment 1.1.



Cyber Risk Score

Appendix 2 – Charges and Additional Services

The Norwegian Agency for Public and Financial Management (DFØ)

05.08.2024

01

Training Courses

Appendix 2 - Additional Services

Training Courses

RiskRecon is a powerful tool providing organizations with valuable insight to the organization's Cyber Risk exposure. In order to ensure customers taking advantage of the insight provided by RiskRecon, KPMG in cooperation with Mastercard RiskRecon have developed a range of customized courses designed to fit Norwegian organizations. These courses provides attendees with valuable insight into the use of and configuration of the service, interpretation of the risk reports and how to transform and make use of the risk reports in the organization's risk and security management processes.

All courses offered are related to RiskRecon as a tool and are particularly suitable for personnel who will use the product or use reports from the product. However, the courses can also provide valuable insights and value for personnel working with security and risk management who do not have direct access to the RiskRecon Service.

Delivery Format

We offer businesses two options: (1) participation in group training sessions or (2) company-specific training.

Group Training Sessions

Group training sessions are open to the public and held for participants from multiple companies at once.

- These are standardized and designed to fit the breadth of businesses that have acquired or considering to acquire RiskRecon.
- They will be suitable for businesses that only want to send 1-3 employees to the course, or for businesses that are curious about various aspects of RiskRecon but have not yet acquired the product.

Company-specific course

The company-specific courses are limited to the individual company that orders the course.

- KPMG and RiskRecon will then design a program that is only offered to the company's employees, and the company can decide how many employees it wants to participate in the course. (Minimum 5 participants.)
- This will be suitable for businesses that want to train 5 or more employees and who wants a course exclusively for their own employees facilitating transparency in discussions and discussion of company-specific issues.

Courses are held at KPMG's office in Oslo or via MS Teams if desired. Course material will be distributed digitally.

Training Courses

Our course package is carefully designed to cover various needs that businesses may have. The goal is to offer courses that strengthen participants' understanding of Service while providing knowledge on how the business can get the most out of the Service through tuning, integrations, and interpretation of results.

Offered Courses Related to RiskRecon

Introduction to RiskRecon
Strategic and Technical Course

See slide 5 for more info.

Enhance your Security with RiskRecon
Strategic Course

See slide 6 for more info.

Understand Your Cyber Risk
Strategic Course

See slide 7 for more info.

Advanced Features for Advanced Users
Technical Course

See slide 8 for more info.

Understand and Act on Third-Party Risk with RiskRecon
Strategic Course

See slide 9 for more info.

System Integration
Technical Course

See slide 10 for more info.

Training Courses

Introduction to RiskRecon

The course provides a fundamental introduction to the RiskRecon tool, enabling participants to understand the objectives of the tool, how it works, the existing features, and how to navigate through it.

Anyone who intends to use RiskRecon should be familiar with the content covered in this course to ensure effective use of the tool. When acquiring RiskRecon, management should encourage all relevant employes to attend the introduction course to ensure sufficient understanding about the Service is provided and associated features.

Content:

- RiskRecon Overview and Tour
- How to use RiskRecon
- Differentiation
- Security Ratings Data Accuracy
- Pitfalls, Tips and Tricks

Target Audience

Managers and employees in public and private organizations who are responsible for or will be using RiskRecon, or who will be handling RiskRecon results and reports as part of decision-making and risk and/or security work.

Length: 4 hours

Training Courses

The results from RiskRecon can help management to obtain a more thorough understanding of the current risk exposure, recommended priorities, and act accordingly. This course is designed to help businesses strategically utilize the RiskRecon Service to strengthen their cyber resilience.

Participants will learn how to leverage RiskRecon's capabilities to enhance their organization's security posture, integrate the tool into existing business processes, and maximize the benefits of the Service.

Content:

- The current threat picture
- What to expect from RiskRecon?
- Business Integration use cases
- How to Succeed with RiskRecon?

Target Audience

This course is tailored for managers, executives, and decision-makers in public and private organizations who are responsible for cybersecurity strategy and risk management. It is also ideal for those looking to integrate RiskRecon into their existing security frameworks to address the evolving threat landscape effectively.

Length: 7 hours

Training Courses

Understand Your Cyber Risk

Ensuring a robust security posture and preparedness for emerging threats is not an easy task. However, a comprehensive understanding of past events and current methodologies is imperative to be able to effectively assess and manage cyber risks within an organization.

This course will provide an in-depth understanding of cyber risk, drawing on insights from a decade of breach event monitoring. Furthermore, participants will acquire valuable knowledge about the RiskRecon Risk Rating Model and explore future trends in cyber risk management to help organizations to be more prepared.

Content:

- Risk Management Insights from 10 years of breach event monitoring
- The RiskRecon Risk Rating Model
- The future of cyber risk management

Target Audience

This course is designed for cybersecurity professionals, risk managers, and decision-makers in public and private organizations who are responsible for assessing and managing cyber risk. It is also suitable for anyone interested in gaining a deeper understanding of cyber risk management and the tools available to support this critical function.

Length: 7 hours

Training Courses

Advanced Features for Advanced Users

This course is tailored for experienced RiskRecon users looking to deepen their expertise and leverage advanced features of the Service. Participants will explore sophisticated tools and functionalities that can enhance their cyber risk management strategies.

By mastering these advanced features, users will be able to customize their use of RiskRecon to meet specific organizational needs and address complex security challenges more effectively.

Content:

- In-Depth Customization
- Advanced Reporting and Analytics
- Integration with Other Security Tools
- Automating Risk Management Processes
- Expert Tips and Tricks

Target Audience

This course is designed for RiskRecon users, including cybersecurity professionals, risk managers, and IT specialists who are already familiar with the basics of the Service and are looking to enhance their skill set by utilizing its advanced capabilities.

Length: 7 hours

Training Courses

Understand and Act on Third-Party Risk with RiskRecon

Third-party risks are getting more and more intricate, and to be able the handle these complexities organization have become dependent on using the right tools to fortify their security defenses. This course focuses on understanding and managing third-party risk using the RiskRecon Service.

This course empowers to effectively manage third-party risks and enhance their organization's security posture. Moreover, participants will learn why third-party risk can be criticall and explore current trends in risk management. Also, they will discover how to implement continuous controls monitoring of their value chain. Additionally, the course covers integrating Third-Party Risk Management (TPRM) with NIST standards and the emerging field of third-party security operations (SecOps).

Content:

- Why third party risk matters
- The State of Third-Party Risk Management
- Steps to Implement Continuous Controls Monitoring for Third Parties
- TPRM and NIST integration
- The rise of Third party SecOps

Target Audience

This course is ideal for risk managers, compliance officers, cybersecurity professionals, and anyone responsible for managing third-party relationships and ensuring the security of third-party interactions. It is particularly beneficial for those looking to enhance their understanding of third-party risk and implement effective risk management strategies using RiskRecon.

Length: 7 hours

Training Courses

System Integration

This course provides a comprehensive guide to integrating RiskRecon with other systems and tools within your organization. By the end of the course, attendees will be prepared to seamlessly integrate RiskRecon into their LSOsting IT infrastructure, enhancing their overall cyber risk management strategy.

Participants will gain an understanding of RiskRecon's integration capabilities, learn how to effectively use APIs, and explore common integration scenarios. The course will also cover troubleshooting techniques and support options, as well as common use cases for system integration.

Content:

- Overview of Integration Capabilities
- API Usage and Integration Techniques
- Common Integration Scenarios
- Troubleshooting and Support
- Common use cases

Target Audience

This course is designed for IT professionals, system integrators, and cybersecurity specialists who are responsible for implementing and managing system integrations. It is also suitable for anyone looking to enhance their technical knowledge of RiskRecon and ensure smooth integration with other tools and platforms.

Length: 4 hours

02

KPMG RiskRecon Subject Matter Expert Services

Appendix 2 - Additional Services

KPMG RiskRecon Subject Matter Expert Services

KPMG offer SME services to ensure optimal utilization of RiskRecon, while also adding an extra layer of expertise and strategic planning, ultimately supporting a strengthened, individualized, and effective cybersecurity framework for your organization.

Offered SME Services Related to RiskRecon

01 Cyber Security Roadmap

- It might be difficult to see the RiskRecon results in context with the rest of the security work and prioritize the findings against other identified gaps.
- Our Subject Matter Experts can assist the business in designing a roadmap based on the findings in RiskRecon and in light of the rest of the security work, and help the customer prioritize efforts where it has the most impact.

02 Service Optimalization

- The trust in the results presented in RiskRecon is closely linked to the confidence that the Service is configured correctly.
- KPMG offer a review of setup and configuration together with the customer so that the customer can be sure that they have understood the Service correctly and can rely on the results presented.

03 Third Party Security (3PS)

- Considering the interconnected nature of today's businesses, a weak link in the supply chain could expose all the entities to cyber threats.
- KPMG helps strengthen customers' third-party security (3PS) by identifying improvements and integrating RiskRecon as a key component.

04 Business Integration

- The real value of a tool comes when the tool is well integrated into the business and contributes to decision support and efficiency effects.
- KPMG can help identify integration opportunities and ensure that relevant business processes have access and competence to exploit the potential of RiskRecon.

05 System Integration

- RiskRecon has good support for integrations with other systems. Several tools can benefit from automatically extracting data from RiskRecon or integrating it as a data source to RiskRecon.
- KPMG can help the customer identify use cases and perform technical implementation of these integrations.

RiskRecon Subject Matter Expert Services 2/2

KPMG offer SME services to ensure optimal utilization of RiskRecon, while also adding an extra layer of expertise and strategic planning, ultimately supporting a strengthened, individualized, and effective cybersecurity framework for your organization.

Offered SME Services Related to RiskRecon

06

Strategic Overview

- RiskRecon provides an overview of risk across all organizations, which can facilitate material governance and control of unpaired information security challenges.
- An overview may require dialogue/advice with several CERTs and the National Security Authority (NSM) to ensure the desired segregation of data in governments with national strategies.

03

Pricing

Appendix 2 - Charges

04

Contacts

Appendix 2 - Additional Services

Contacts

Frank Horntvedt
M: +47 920 16 394
E: frank.horntvedt@kpmg.no

Svein Løseth
M: +47 917 70 639
E: svein.loseth@kpmg.no