Attachment 4.2.2. Information security requirement

For guidance on how to fill out the table, see the tab Guidance or click below:

Guidance

The supplier may provide supporting documentation where applicable, such as ISO27001:2022 certificate and SOC2 Type 2 reports.

Informatin security requirements	Reference to clause in Appendix 4.2:	Compliance (yes, partially, no)	Response from Supplier	Supplier reference to attachment, further information
Security Governance	**14**	N/A	N/A	N/A
Compliance with standards and frameworks	14.1	Yes	14.1.1 a) **KPMG** have in place an ISMS certified according to ISO 27001:2013 **Mastercard** has a comprehensive, enterprise- wide data security program that is compliant with numerous domestic and international regulations (e.g., the Federal Trade Commission's information safeguarding rules under the Gramm-Leach-Bliley Act, 16 CFR Part 314) and is regularly audited and tested by third parties, including an annual SSAE 18 Report examination. 14.1.1 b) **RiskRecon** run in AWS data centers. AWS has several international standards including ISO27001, ISO27017, SOC2, and SOC3. **Mastercard** is pursuing a **FedRAMP Moderate** authorization for the RiskRecon product. • Mastercard are currently planning to start our "FedRAMP Ready" external assessment for RiskRecon in June of 2024. Assuming our assessors deem our environment ready after the assessment is complete, our evidence will be supplied to the FedRAMP PMO for review. If our evidence is accepted, we will be considered a "FedRAMP Ready" SaaS provider with RiskRecon and will be given a status of "FedRAMP Ready" in the FedRAMP marketplace (https://marketplace.fedramp.gov/products). If all goes well, this should be complete by the end of 2024. We are still on track to achieve Ready status in Q4 2024. However, it's of course dependent on an external audit so subject to change. • The process to achieve full FedRAMP Authorization status will then take another full year to achieve. Once we are ready for that, we will require the external assessor to return and perform another audit of additional controls. That could be complete by the end of 2025 or early 2026.	Please see: Mastercard Compliance Self Attestation Statement KPMG ISO 27001 Certificate
Information security management system	14.2	Yes	14.2.1 **KPMG** ISMS is certified according to ISO 27001:2013, ISMS transition to 27001:2022 is planned for 2025 **Mastercard**, please see Mastercard Information Security Executive Summary **14.2.2** **KPMG** ISMS is certified according to ISO 27001:2013, ISMS transition to 27001:2022 is planned for 2025 **Mastercard**, please see response to requirement **14.1.1b)** above related to **FedRAMP Moderate** level	Please see: Mastercard Information Security Executive Summary KPMG ISO 27001 Certificate
Security audit and security testing obligations	14.3	Yes	14.3.1 It is the policy of **Mastercard** to outline its security program and responsibilities and provide an overview of the associated program elements, which ensures enterprise-wide coverage is met. The Corporate Security objectives are reinforced by Mastercard Corporate Security Policy and its supporting directives and standards that map to controls and control procedures. This provides a comprehensive approach across all systems, Staff, and processes within the organization. The purpose of Mastercard Corporate Security Policy is to also demonstrate Mastercard's efforts to achieve regulatory and contractual requirements. **14.3.2** **Mastercard** have in place a number of supporting directives and standards mandated by Mastercard Corporate Security Policy ensuring that any issues identfied are adressed without undue delay. The most central directives are: • **Security Incident Management Directive** provides requirements to identify, track and remediate IT events, incidents, and problems. • **Security Monitoring and Response Directive** provides requirements on monitoring information resources, preventing security controls from being circumvented and ensuring a timely response to information security incidents.	Please see: Mastercard Corporate Security Policy
Access to security documents	14.4	Yes	14.4.1 Security documents are **KPMG Confidenital** and cannot be shared with the client "as is". NDA may be reqired to be signed. KPMG will accomodate requests from client that may independent audit and request the independent review of these documents as part of audit engagement.	Please see: Mastercard Corporate Security Policy
Third party security management	14.5	Yes	**14.5.1** **KPMG** being the Supplier under this contract ensure that any third party used in providing the Services to the Customer under the Call-Off Contract meet the security requirements set out in this Framework Agreement and the Call-Off Contract **14.5.2** **KPMG** will notify the Customer in advance of any planned changes to the ownership or operation of the data centres or infrastructure used to deliver the Services.	Please see: Mastercard TPRM Executive Summary
Cooperation regarding information security	15	Yes	15.1 **KPMG** will appoint an information security responsible under the Call-Off Contract as a counterpart to the Customer 15.2 **KPMG** and DFØ may summon a meeting with 7 (seven) days' written notice	
Incident and vulnerability management	**16**	N/A	N/A	N/A

Security incident management and threat intelligence	16.1	Yes	16.1.1 **Mastercard** has a comprehensive and multi-tiered approach to identify, prevent and respond to incidents, vulnerabilities or security related events that may occur. 16.1.2 **KPMG** will, in case of a serious security incident, report in writing to the Customer in line with the timeframes set forth in requirement 16.1.2 16.1.3 **KPMG** will, in case of a serious security incident, cooperate with relevant vendors of the Customer to ensure the operational information security of the Customer's systems. 16.1.4 **KPMG** and **Mastercard** maintain a security log of all incidents concerning Customer Data, including log data and relevant indicators of compromise, for Customer incident analysis and digital forensic purposes. 16.1.5 **KPMG** and **Mastercard** perform threat intelligence regularly and update indicators of compromise (IoCs) and malware definitions. 16.1.6 **KPMG** and **Mastercard** ensure that all software and storage media used in the performance of the Service(s) is free of any malicious software.	Please see: Mastercard Incident Response Executive Summary Mastercard Corporate Security Policy
Vulnerability management	16.2	Yes	16.2.1 **KPMG** and **Mastercard** have in place processes for managing vulnerabilities in the Services. 16.2.2 **KPMG** and **Mastercard** have in place processes monitoring third-party vulnerability notifications and other relevant security vulnerability advisories 16.2.3 **Mastercard** assignes a unique Common Vulnerability and Exposures ("CVE") identifier and a Common Vulnerability Scoring System ("CVSS") score to vulnerabilities identified in the Service. Identified vulnerabilities are recorded. 16.2.4 **KPMG** will notify the Customer without undue delay of any vulnerabilities identified in the Services with a CVSS score of 9.0 to 10.0 (Critical) or 7.0 to 8.9 (High).	Please see: Mastercard Vulnerability Management Executive Summary
Suspension of service due to security incidents or vulnerability	16.3	Yes	16.3.1 **KPMG** will In the event of a serious security incident or vulnerability in the Services, assist the Customer with suspending the Services upon request.	Please see: Mastercard Enterprise Resilience Executive Summary
Penetration testing rights	16.4	Yes	16.4.1 **KPMG** will, subject to prior notification, facilitate Customers under the Call-Off Contract, their right to perform penetration testing of the Services according to agreed routines, to identify and analyse any potential security vulnerabilities and risks.	Please see: Mastercard Penetration Testing Executive Summary and RiskRecon Penetration Testing Statement - Jan 2024
Access control and Customer Data	**17**	**N/A**	**N/A**	**N/A**
Security access management	17.1	Yes	17.1.1 **Mastercard** have in place strict access control policies and procedures to ensure that only identified and authorised personnel have access to the Service(s) and their management system. Access to customer data and logs is only provided on an as needed basis and follows best practices of separation of duties. Some examples of this are: • Support staff requires access to customer accounts to assist with troubleshooting issues. Due to this business need, they are allowed this access. Other staff such as marketing has no need for customer account access so they will not have this type of access. • Our security operations staff have access to logging for monitoring of relevant logs including: web, application, network, etc. Due to this business need, they are allowed access to logs. Other staff such as the RiskRecon product team do not have need of this access and do not have permissions to the logging data. 17.1.2 **KPMG** and **Mastercard** are conducting regular access review to ensure compliance with the established access control policies and procedures.	Please see: Mastercard Corporate Security Policy
Flexible and fine-grained identity and access management	17.2	Yes	17.2.1 **Mastercard** RiskRecon supports and provides Customer swith flexible and fine-grained mechanisms for identity and access management including SSO-capabilities. RiskRecon provides multiple methods for authentication to meet the needs of our customers including MFA and SSO. We support SAML authentication integration with multiple products which allows our customers to have full visibility into authentication events due to SSO tracking using an Identify provider at the customer organization. 17.2.2 **Mastercard** RiskRecon supports cross-domain identity management.	Please see: Mastercard Corporate Security Policy, MFA_Multi-Factor Verification Release Notes, and RiskRecon MFA Update Release Note
Secure remote access	17.3	Yes	17.3.1 **Mastercard** RiskRecon supports strong encryption and authentication measures in accordance with best industry practices, and that security gateways (enabling security policy enforcement, security monitoring, etc.) are used to control access to the RiskRecon Service(s) over Internet.	Please see: Mastercard Corporate Security Policy

Separation of Customer Data	17.4	Yes	**17.4.1** **Mastercard** RiskRecon ensure effective customer separation through the implementation of multiple security controls including: • Application controls that enforce strict individual request authorization using JWT tokens. These tokens enable our product to verify every request to the application to ensure that customer data is kept private and not visible to any other parties. • User authorization controls ensure that different user levels such as customer Admins and Analysts are only allowed to see relevant data within the customer account. • We also provide very granular access to individual companies through company groupings using foldering. For example, if you have 2 sets of analysts with different roles, it can be setup so that each analyst group can only see the companies within their permitted folder. • Regular security testing of the application to ensure that any possible techniques used to view unauthorized data are identified and resolved including: application logic issues, security misconfigurations, vulnerability patching, error reporting/handling, encryption, authentication, authorization methods, session takeover, SQL injection, etc	
Encryption of Customer Data	17.5	Yes	**17.5.1** **Mastercard** RiskRecon ensures protection of Customer Data in transit and at rest, both internally within the Service(s) and for inbound/outbound traffic utilizing encryption. **17.5.2** **Mastercard** RiskRecon implement state of the art encryption with adequate algorithms and key-lengths for data in transit, at rest and provide support for strong authentication (MFA). **17.5.3** **KPMG** and Mastercard monitors closely developments in the encryption field and adopts new algorithms and key-lengths as recommended by regulatory authorities (NIST, NSM)	
Logging of access to Customer Data	17.6	Yes	**17.6.1** **Mastercard** RiskRecon maintains logs of all product usage. Product usage is tracked through authentication logging of each individual customer log-on event to the RiskRecon portal. **17.6.2** **KPMG** and **Mastercard** confirms that applicable logs will be maintained and available as stipulated in applicable Laws and regulations, taking into consideration any recommendations from Norwegian national security and information security authorities	
Notification of relocation of Customer Data	17.7	Yes	**17.7.1** **KPMG** will notify the Customer in writing in advance of any planned relocation or transfer of Customer Data, including backups, to a new data centre or any other location. RiskRecon has architected all its critical systems to withstand a disaster. All critical systems are hosted in Amazon Web Services (AWS). All critical systems are deployed to multiple AWS data centers by using AWS' availability zones. RiskRecon does not maintain a traditional on-prem datacenter. Three sites render relocation unnecessary.	Currently, all RiskRecon AWS datacenters are US locations. Starting summer 2024, all EU customers will be migrated to EU based AWS datacenters. We will have new customers in the EU provisioned in the Ireland AWS datacenter no later than the end of July 2024.
Change Management and security by design	**18**	N/A	N/A	N/A
Change management	18.1	Yes	**18.1.1** **KPMG** and **Mastercard** have in place strict procedures for technology change management and deviation handling in the Service(s). **18.1.2** **KPMG** will provide advance notice to Customers of changes to the Service(s) that may negatively impact information security	Please see: Mastercard Corporate Security Policy
Security by design	18.2	Yes	**18.2.1** **Mastercard** have in place processes and routines ensuring that security by design principles in the provision of the Service(s) are adhered to and ensure that software hardening best practices are implemented with secure configuration set as default. **18.2.2** **Mastercard** conducts regular testing to ensure that the Service(s) maintain a high level of integrity and quality, with no backdoors or known vulnerabilities. **18.2.3** **Mastercard** follows relevant industry standards and best practices to ensure security by design.	Please see: Mastercard Information Security Executive Summary
Business continuity	**19**	N/A	N/A	N/A
Business continuity and disaster recovery	19.1	Yes	**19.1.1** **KPMG** and **Mastercard** have in place business continuity and disaster recovery plans that adhere to best industry standards. The plans include measures to prevent or mitigate the impact of various types of disasters or disruptions. Business continuity and disaster recovery plans are regularly test and reviewed to ensure their effectiveness in the event of a disaster or disruption. All critical systems are deployed to multiple AWS data centers by using AWS' availability zones. RiskRecon does not maintain a traditional on-prem datacenter. Three sites provides a resilient solution. **19.1.2** **Mastercard** RiskRecon are deployed to multiple AWS data centers by using AWS' availability zones. RiskRecon does not maintain a traditional on-prem datacenter. Three sites provides a resilient solution providing efficient capacity management measures ensuring stable operations in both normal and disaster recovery situations.	Please see: Mastercard Enterprise Resilience Executive Summary

Backup and restore of the Supplier's system	19.2	Yes	19.2.1 Mastercard RiskRecon are utilizing AWS services for hosting and data storage. RiskRecon has architected all its critical systems to withstand a disaster. All critical systems are hosted in Amazon Web Services (AWS). All critical systems are deployed to multiple AWS data centers by using AWS' availability zones thus providing resilience as well as high availability, efficient data-replication thus reducing need for traditional backup. . RiskRecon does not maintain a traditional on-prem datacenter.	
Physical and personell security	**20**	N/A	N/A	N/A
Physical security	20.1	Yes	20.1.1 Mastercard RiskRecon systems are hosted in AWS datacenters ensuring appropriate physical security measures for the Services. 20.1.2 Mastercard Internal Audit independently evaluate the design and operating effectiveness of the Corporate Security Program, in accordance with Internal Audit's risk assessment methodology. This includes evaluating compliance with corporate policies; procedures; and applicable laws, regulations, and governance standards; and the effectiveness of processes and systems to monitor/validate compliance.	Please see: Mastercard Corporate Security Policy
Personell security	20.2	Yes	20.2.1 KPMG ensure that all personnel involved in the delivery of the Service(s), including personnel of any Subcontractors and third parties, have committed themselves to confidentiality, receive appropriate training and maintain necessary expertise on all applicable security matters. 20.2.2 KPMG have in place procedures for personnel security, including screening and background checks in accordance with best industry practice and any applicable laws. 20.2.3 KPMG have established auditing practices performing audits on established personnel security procedure evaluating compliance with applicable standards and policies.	Please see: Mastercard Corporate Security Policy