Bijlage A: Statement of Work (SoW)

Openbare Europese aanbesteding

Cyber Recovery Solution

Kadaster

Kenmerk	xxx
Opdrachtgever	Directie DGV
Versie	1.0
Versiedatum	15-2-2023

Inhoud

1 Overview

This Statement of Work (this “SoW”) describes the services, as requested by Kadaster, to be delivered by the service provider.
This Statement of Work (or “SoW”) sets forth the roles and responsibilities of both service provider and Kadaster as part of the Services.

2 Services Overview

Kadaster acquires a Cyber Recovery Solution (CRS) and related services for its most critical business processes and related systems. This CRS solution is to enable Kadaster to recover critical systems within days after a successful ransomware attack. This attack is assumed to have destroyed or encrypted a high number of systems and datasets, and the standard operational environment will not be available for restore for at least one week.
The service provider delivers:

1. A data vault and related data vault services to store Kadaster data safe from Cyber-attack and separated from the standard operational environment.
2. A recovery environment and restore services to restore critical datasets and systems from the data vault into the recovery environment.

After restore the service provider will support the critical systems to run production for an extended period, before the systems and data can be transitioned back to the standard operational environment. The service provider is responsible for the retransition of the critical datasets.

In the Data Vault and Recovery Environment the service provider will provide standard cybersecurity services to prevent, detect and where necessary clean the datasets and systems from malware infection.
The requested solution and services must be highly integrated to enable the required recovery objectives.

3 Scope of Service

This section describes and scopes the Service environment to be supported and/or with which the service provider shall comply.

3.1 Scope for Data Vault services

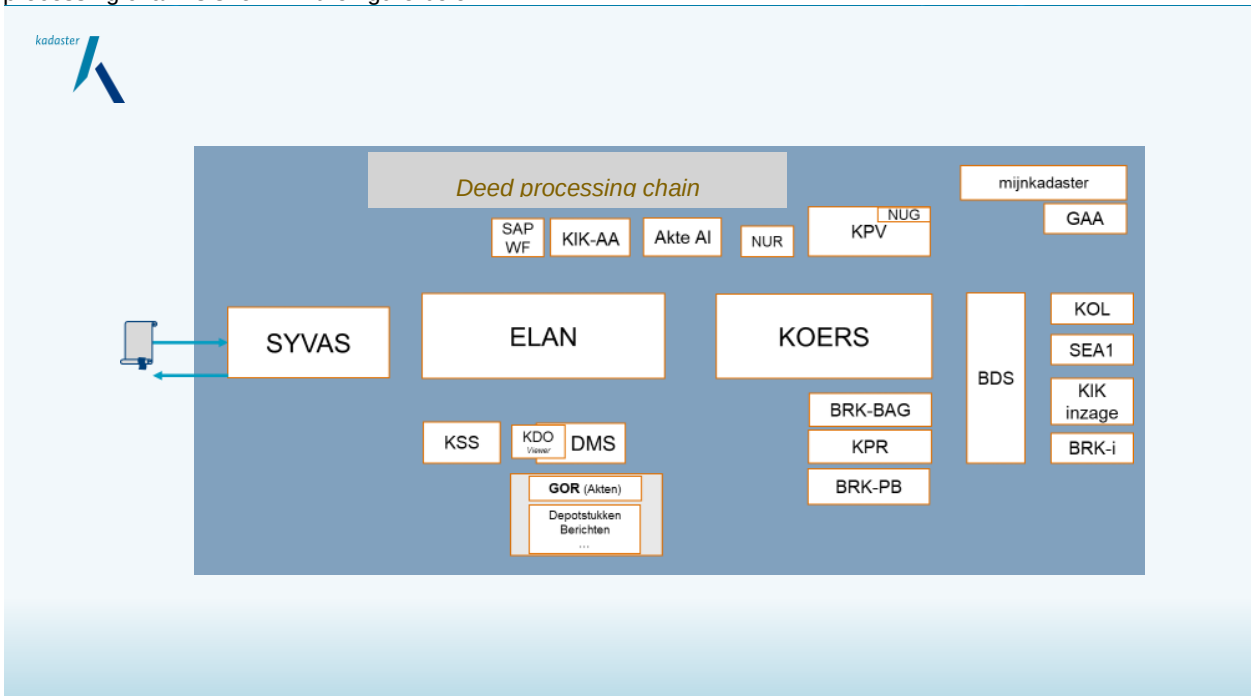
The scope for the Data Vault covers all Kadaster datasets that need protection by an offsite back-up or data copy. Only datasets which can be recreated effectively from external sources will not be protected in the Data Vault.

3.2 Scope for Recovery Environment and Recovery Services

The scope for the Recovery Environment and Recovery Services is limited to the critical Kadaster Deed processing chain. The Deed process validates and administrates real estate transactions in the Netherlands. The critical Deed processing chain consists of around 20 applications, which maintain and disclose the “Basis Registratie Kadaster”(BRK, Kadaster Base Registry) and the “Openbaar Register” (OR, Public Registry). The key applications for the BRK are SYVAS, ELAN,GOR, KOERS, KPV, KPR and BRK-adressen and the related datasets have to be in sync at all times. Access to the BRK information is limited to specific internal and external user groups.

Three (3) SAP modules are needed for critical deed processing: SAP Workflow management, SAP PO/PI and SAP DMS. These modules operate independently from the general SAP landscape.
The Kadaster user access structure consists of mijnkadaster.nl, GAA and Azure AD. mijnkadaster.nl and GAA have to be recovered in the recovery environment. Azure AD will be recovered by Kadaster.

The scope of the Deed processing chain is quantified in infrastructural terms in chapter 5.3.2. The Deed processing chain is shown in the figure below.



4 Service Level Requirements

The services outlined in this SoW should be compliant with the minimum Service Levels required at the end of the implementation project. All times referenced are in Central European Time (CET).
All critical systems in the Deed processing chain have a technical Recovery Time Objective (RTO) of 4 calendar days. The Deed processing chain has to be restarted within 7 calendar days, where 7 days is the absolute maximum down time. 3 calendar days are reserved as contingency for unplanned events and activities.
The Recovery Point Objective (RPO) is defined in business terms as 'Once deeds have been received by Kadaster they may not be lost'. The means that the systems in the critical Deed process chain have a RPO of 15 minutes.

For retransition of the Deed processing chain to the standard operational environment the maximum window is a weekend (from Friday night 12:00pm till Monday morning 6:00am).
For the Deed processing chain a complete restore test in the recovery environment has to be performed twice a year.

5 Service Descriptions

5.1 Data Vault Services

Data Vault services are the services and activities, as detailed in this Statement of Work, required to create and preserve a copy of the Kadaster data with the desired level of protection, and make it available for cyber recovery of Kadaster IT applications and infrastructure.
The solution contains a Data Vault, where all Kadaster datasets, files and documents, needed for recovery, are stored safe from malware infection from the standard operational environment and from elsewhere. In case of a cyber-attack the restore and validation of the systems in the Recovery Environment can only rely on data from the Data Vault.

The service provider manages the incoming data streams into the data vault. It performs malware scanning and malware cleaning on the incoming data streams and stores all data on immutable storage. The service provider can identify the clean data copies and the most recent consistent return point. The service provider manages restore from the Data Vault towards both recovery environment as well as towards the standard operational environment and is able to meet all RTO-requirements also for mass restores. As current Kadaster practices do not allow for these short recovery times the service provider has to advise on and implement measures to enable short restore times of large datasets. Kadaster will be responsible for related changes in the standard operational environments. As soon as the Deed chain applications are running in the recovery environment, the service provider will start back-up and data streaming from the recovery environment to the data vault. Upon the retransition of the Deed chain applications to the standard operational environment, the service provider will stop the back-up and data streaming from the recovery environment to the Data Vault.
Regular restore tests are performed from the Data Vault into both Recovery Environment and to the standard operational environment.

5.2 Recovery Services

The service provider has to support Kadaster at different levels during the recovery process.

5.2.1 Server provisioning

As a first step the service provider provisions database- and file servers as well as the containers and virtual servers needed for application servers into the Recovery Environment (See below 5.3.2 Provisioning of infrastructure services).

5.2.2 Malware cleaning

When a cyberattack occurs the risk of malware infection in both the back-ups and software repositories is very high. During the restore and redeployment process the service provider is responsible for malware detection and malware cleaning on any item in the recovery environment. Detection and cleaning have to be done on infected back-ups and on. any other Kadaster files as present in the Data Vault.
In this stage the service provider is dependent on Kadaster to have identified the malware, used for the cyberattack, in the standard operational environment.

5.2.3 Software deployment

Kadaster is responsible for software deployment of Docker containers and software packages on application servers. Deployment is partly automated.
Deployment to the recovery environment is done using safe versions of the development repositories.

5.2.4 Restore datasets

Before restore the service provider has to determine the last usable and consistent version of back-ups and other secured data.
The service provider is responsible for the restore of all the databases, data files and network storage. To create consistency over the different datasets in the processing chain, it is necessary to restore a number of databases point-in-time to the same moment before the start of the data encryption. Specific object stores have to be restored to a moment defined as “up to the last successfully received input document”. Other databases and file stores can be restored from the most recent consistent daily back-up.
In addition the service provider may have to restore a few application servers from snapshot backups.
After successful restore the datasets will be handed over to the Kadaster.

5.2.5 Dataset realignment & rework

Once all datasets have been restored, Kadaster will start and verify the systems. Kadaster is responsible for proper restart of the application chains and alignment of applications.
Kadaster is responsible for the consistency between datasets and remediation of remaining inconsistencies. Kadaster has the procedures to align all datasets to the same moment in time by resending and executing specific messages. When all datasets are aligned, rework is started to re-process all deeds from the point of recovery up to the last received deed.

5.2.6 Production in Recovery environment

During the operational phase users and clients will access the environment from the internet. User and client access is managed using the Kadaster Azure AD (Kadaster is responsible for recovery) and Kadaster web portal mijnkadaster.nl(to be recovered in the Recovery environment).
When the non-critical Kadaster systems have been restored in the standard operational environment by Kadaster, they need interfacing with the critical applications in the recovery environment over a secure connection.
As soon as user and client access have been restored in the standard operational environment access services will be redirected to the original entry point in the standard operational environment and the web connection in the recovery environment will be closed.

5.2.7 Retransition

When the Deed processing chain can be restored to the standard operational environment, the service provider is responsible for the transfer of all data back into the standard operational environment. Kadaster is responsible for the application servers and verification of the Deed processing chain.
After successful retransition the service provider will hand over the datasets to Kadaster. Kadaster will restart the systems in the standard operational environment and will restart the back-ups and data streaming to the data vault.

5.3 Recovery Environment and Operational Services

The Cyber Recovery Solution contains a recovery environment separated from the standard operational environment, where these critical systems will be restored and validated. After restore the critical workloads have to run production in the recovery environment for probably more than a month, until the systems can be transferred back to the standard operational environment.

5.3.1 Datacenter

The recovery environment is specified by requirements see attachment requirements. Critical datasets have to be redundant and have to be replicated within the recovery environment.

5.3.2 Provisioning of infrastructure services

The recovery environment must provision the virtual servers as defined in Table 1. These servers host the applications and datasets for the critical systems. The service provider delivers DBaaS service for Oracle and PostgreSQL, including point-in-time restore capabilities for a selection of databases. Provisioning is needed of Linux containers, VM's, shared storage and immutable storage. The connections between the systems are name based. In the standard operational environment system names are entered in the provisioning portal and DNS entries are generated automatically.

When the restored Deed processing chain is running production in the recovery environment data protection towards Data Vault has to be analogous to the back-up and data streaming towards the Data Vault in the standard operational environment.

	Type	***Operating system***	***Category***	***Quantity***	***Total (v)CPU cores***	***Disk Storage – persistent***	
						Total	***To be protected in Data Vault?***
Compute & Storage resources	***Virtual machines on VMware***	*Linux*	*File servers (Access: NFS, Webdav, S3)*	*30*	*150*	*10TB*	*Yes – all*
		Linux	*PostgreSQL DB*	*15*	*150*	*5TB and growing*	*Yes – all*
		Oracle Linux with Unbreakable Enterprise Kernel (UEK)	*Oracle DB*	*10*	*50*	*16TB and growing*	*Yes – all*
		Windows		*4*	*16*	*100GB*	*Partially - specific servers*
		Oracle Linux with Unbreakable Enterprise Kernel (UEK)	*Tuxedo*	*8*	*16*	*128GB*	*no*
	Docker containers	*Linux – based*		*100*	*1400*	*26 TB total (including mirroring and redundancy)*	*no*
		Windows - based		*6*	*120*		*Partially - specific servers*

Other storage	***DELL Isilon storage***	-	*Online Archives & other immutable storage*	*6*		*80TB*	*Yes – all*
Special applications	***SAP modules***	*SAP Workflow Management, SAP PO/PI (enterprise bus)*	*packages*	*1+1*			*no data to be recovered*
		SAP DMS / SAP/HANA DB	*Package as metadata for Online Archives*	*1*		*<1TB*	*Yes*

Table 1 – servers overview

5.3.3 Standard infrastructure services

In the recovery environment the service provider has to provide standard infrastructure services.
The Kadaster Azure AD is delivered by Kadaster, but it is only used for client and user access to the Kadaster Applications, while running production in the recovery environment.

5.3.4 Service management

The service provider will manage the recovery environment.

5.3.5 External connections

During restore phase the Recovery environment requires access to safe versions of devops repositories Gitea, Jenkins and Artifactory. Gitea is deployed in Azure. Jenkins and Artifactory run in the standard operational environment (datacenter).

During the operational phase users and clients will access the recovery environment over a secure web connection which is to be secured by firewall, and best practice cybersecurity measures. User and client access is managed using the Kadaster Azure AD.

As soon as user and client access is restored in the standard operational environment, user and client access will be redirected to the original entry point in the standard operational environment. The web connection in the recovery environment will be closed. From that moment the recovery environment needs interfacing over a secure connection with the standard operational environment to connect the Deed processing chain with other Kadaster systems, which are restored and restarted in the standard operational environment.

5.4 Cyber Security Services

All the services require best practice cybersecurity protection services and security events have to be fed into the Kadaster SIEM.
Apart from the standard security services the Data Vault and Recovery Environment need additional security services to detect and clean malware from both incoming and already stored back-ups, log data and restored systems and datasets.

6 Service Outcomes and Deliverables

Supplier shall deliver the following key high-level Service outcomes:

6.1 Service delivery

Unless otherwise specified explicitly in this schedule,service provider shall provide all services and perform all roles, responsibilities and activities outlined in this schedule, in accordance with Kadaster performance requirements.

6.2 First implementation: minimal recovery solution

Kadaster expects a two phase delivery towards the defined target situation for the requested services. As a first deliverable the service provider will implement a temporary solution, which enables recovery of the Deed processing chain into the Recovery environment, which is separated completely from the current operational environment. For this first implementation the current restore playbooks and offsite Commvault back-up can be used. This first implementation will enable recovery of the deed processing chain in the recovery environment, but it does not need to comply with the required RTO and RPO targets.

6.3 Implementation target situation: SLA based recovery for Deed processing chain

In the target situation the service provider has complete control over all service elements within her responsibility. The service provider delivers the contracted services (Data vaulting, Recovery services, Recovery environment & operational services and cybersecurity services) to the mutually agreed SLA.
These services enable Kadaster to recover the Deed processing chain with a RTO of 4 calendar days and data loss (RPO) < 15 minutes. The RTO and RPO are being assured by design and by repeating recovery tests.

6.4 Continuous improvement

The service provider will improve its services continuously during the contract, so it will be able to withstand the continuous renewal of cyberthreats. The service provider will advise and implement innovations to stay best in class in its field.

7 Service Roles and Responsibilities

The following tables identifies the roles and responsibilities associated with the Cyber Recovery Solution.

7.1 Data Vault

Service Roles and Responsibilities	Supplier	Kadaster
Data Vault and Reporting		
Specify the data sources and destinations to be covered by the Service		X
Specify application and dataset dependencies		X
Specify back-up or data streaming requirements on data sources, which have to be protected in the Data Vault	X	
Implement data back-up or data streaming from data sources in the Kadaster datacenters to the Data Vault according to specification of the service provider	X	X
Integrate / remove data sources and destinations from the scope of the Services upon Kadaster request	X	
Perform back-up of Kadaster data into the Data Vault	X	
Monitor the backup process in order to detect anomalies, such as back-up failures, abnormal volume of data	X	
Inspect data received from Kadaster system in order to detect anomalies related to ransomware and other cyber attacks	X	
Perform periodic checking of the integrity of the backup data and metadata stored in the Data Vault and detect anomalies	X	
Rescan past backups to detect newly identified malware	X	
Investigate detected anomalies and take corrective actions under the service provider's responsibility	X	
Inform Kadaster on the detected anomalies, corrective actions taken and their outcome	X	
Retain Kadaster data in the Data Vault as per the policies agreed with Kadaster	X	
Destroy Kadaster data stored in the Data Vault as per the policies agreed with Kadaster	X	
Manage the capacity of the Data Vault to always be able to store the Kadaster data as per the policies and volumes agreed with Kadaster	X	
Advise and implement measures to assure timely recovery of datasets to the recovery environment within RTO and RPO objectives	X	
Request restore of Kadaster data (as part of real recovery or tests)		X
Restore Kadaster data to the supported environments upon Kadaster request	X	
Monitor the restore process to detect anomalies	X	
Validate restore of Kadaster data		X
Integrate and manage logging of the anomalies and other alerts to the Kadaster security monitoring system	X	
Support testing anomaly and security threat detection and response features of the Data Vault by the service provider, as required		X

Service Roles and Responsibilities	Supplier	Kadaster
Provide reporting on: - backup operations and actual return point of data stored in the Data Vault - restore operations - data destruction - service requests - all access to the Service - data sources and destinations covered - data backup and retention policies implemented - service availability - service usage - testing of the Data Vault features - incidents	X	
Provide to Kadaster recommendations for improvements	X	

7.2 Recovery services

Service Roles and Responsibilities	Supplier	Kadaster
Recovery services – Recovery capability preparation and maintenance		
Specify the systems and data to be covered by the Service.		X
On- and off-board the systems and data as per Kadaster specifications.	X	
Specify system and data dependencies.		X
Create and maintain end-to-end recovery and retransition processes for Kadaster applications.		X
Advise on the creation and maintenance of the end-to-end recovery and retransition processes for Kadaster applications.	X	
For the server images to be restored from Kadaster backups in the Data Vault, maintain safe copies of the required software and the build procedures to be used for server rebuild as a last resort recovery method.	X	
Create and maintain procedures & playbooks for activities under responsibility of the service provider.	X	
Periodically test end-to-end recovery and retransition processes.		X
Participate to the tests of the end-to-end recovery and retransition processes as per the scope of theservice provider's responsibility in the processes.	X	
Provide reporting on: - service requests, - service coverage, - incidents.	X	
Recovery services – Recovery and Retransition execution		
Initiate recovery and retransition		X
Determine last usable copy of datasets.	X	
Determine last usable synchronous, consistent moment for BRK databases	X	
Restore data and relevant servers into recovery environment within RTO from their backups in the Data Vault	X	
Manage access and authorization to the recovery environment	X	

Service Roles and Responsibilities	Supplier	Kadaster
Rebuild relevant server images from safe copies of software	X	
Restore consistent set of BRK databases to same moment in time	X	
Check leftover inconsistencies in BRK databases		X
Fix inconsistencies in BRK databases		X
Assess and approve data consistency		X
Provision containers and virtual servers as required	X	
Deploy Kadaster application software and tools		X
Restart Deed applications and processing chain		X
Rework deeds from restore moment to the last received		X
Monitor the restore process to detect anomalies	X	
Inspect restored data from Data Vault in order to detect anomalies	X	
Inspect deployed servers and containers for malware and anomalies related to ransomware and other cyber attacks	X	
Respond to detected malware and anomalies related to ransomware and other cyber-attacks, in a way agreed with Kadaster	X	
Implement data back-up and streaming from data sources in the recovery environment to Data Vault	X	
Retransition the operational datasets from recovery environment to the standard operational environment	X	
Retransition Deed applications and processing chain to the standard operational environment		X
Decommission systems and destroy datasets after use, in the recovery environment	X	
Provide reporting on: - restore operations, RTO and RPO results - data destruction after usage - incidents, service requests - all access to the Service - Service usage - Security monitoring (audit trail)	X	

7.3 Recovery Environment & operational services

Service Roles and Responsibilities	Supplier	Kadaster
Recovery Environment & operational services		
Specify the recovery environment and infrastructure services needed, with their characteristics (outside of the needs of the Recovery services described previously).		X
Provide the recovery environment and infrastructure services needed.	X	
Validate the suitability of the provided recovery environment and infrastructure service for hosting Kadaster applications.		X
Provide infrastructure requirement changes (outside of the needs of the Recovery services described previously).		X
Manage change of infrastructure requirements	X	
Provide changes on dataset and database structures		X
Implement changes on datasets and databases into Data Vault and restore procedures	X	
Provide a web portal and API for provisioning/deprovisioning the infrastructure components (e.g. containers, virtual servers, databases) in the recovery environment.	X	
Perform back-up of Kadaster data into the Data Vault.	X	
Perform operational service monitoring and systems management for recovery environment.	X	
Perform Infrastructure monitoring.	X	
Perform Kadaster applications monitoring.		X
Monitor back-ups and data streams.	X	
Manage external network connections.	X	
Manage the capacity of the recovery environment (following capacity requirements for Deed processing chain in the standard operational environment)	X	
Perform Identity and Access management for the recovery environment and infrastructure services	X	
Perform Identity and Access management for the users of the Deed processing applications		X
Inform Kadaster on the detected anomalies, corrective actions taken and their outcome	X	
Integrate and manage logging of the anomalies and other alerts to the Kadaster security monitoring system	X	
Provide reporting on: Service availability Service usage Performance Incidents Service requests All user access to the Recovery environment Back-up and data streaming operations Security incidents	X	

7.4 Cross functional

The roles and responsibilities below are generic and apply to all the service elements.

Service Roles and Responsibilities	Supplier	Kadaster
Network		
Provide network connectivity between Kadaster andservice provider Data Centers, other than public Internet connectivity	X	X
Provide network connectivity between Kadaster and public Internet		X
Provide network connectivity betweenservice provider and public Internet	X	
Service Delivery		
Report performance against Service Levels.	X	
Coordinate Data Vault Service delivery with Kadaster support groups within all involved service areas in coordination with Kadaster, Kadasterservice providers, and all appropriate third parties as necessary.	X	
Continuously improve the Services.	X	
Provide to Kadaster recommendations for improvements	X	
Keep Kadaster up to date on new developments and related services in the field of Disaster Recovery and Cybersecurity	X	
Inform Kadaster immediately if the service provider becomes aware of any vulnerability or weakness in the services or any security breach and recommend a possible solution or mitigation.	X	
Staffing - Related		
Provide qualified, appropriately skilled personnel with applicable certifications appropriate to meet the roles and responsibilities and Service Levels set forth in this SoW.	X	
Provide timely notification of separation of all service provider personnel with access to Kadaster data / infrastructure / applications. Access to Kadaster data / infrastructure / applications should be terminated in accordance with Kadaster policies and procedures.	X	
Educate and train service provider personnel in the use of the security tools and processes specific to Kadaster.	X	
Educate and train Kadaster personnel on the use of tools and processes required by for the delivery of the services.	X	
Attend education and training sessions provided byservice provider in a mutually agreed manner.		X
Keep security capabilities best in class.	X	
Supporting		
Provide planning, solution design/architecture, and project management as needed.	X	
License, provide, deploy, install, implement, securely configure, maintain, support and administer Kadaster-approved hardware and software required to be deployed in the Kadaster environment for the delivery of the Services, in accordance with Kadaster Change Management Policy and process.	To be specified by the Tenderer	
Ensure that service provider tools and services integrate with Kadaster Configuration, Change, Problem and Incident Management System.	X	

Service Roles and Responsibilities	Supplier	Kadaster
Provide the status of planned and inflight maintenance activities for the services and provide guidance on their impact to Kadaster.	X	
Engage with Kadaster Product Owners and provide continuous improvement recommendations.	X	
Security, Compliance and Audit Support		
Confirm that theservice provider's information security controls meet Kadaster information security requirements documented as part of the Agreement.		X
Adhere to Kadaster defined data security classification policy.	X	
Provide personnel Security and physical Security forservice provider locations. Control and manage access rights forservice provider personnel and third parties.	X	
Implement and administrate logical access controls of the Services.	X	
Implement and administrate all other logical security for the Services.	X	
Perform cybersecurity threat identification, protection, detection, response, and recovery of the Service and Kadaster data (solution perimeter, client and user access and solution internal)	X	
Respond to exception or change requests from Kadaster and determine if such requests result in additional or modified information security roles and responsibilities.	X	
Validate theservice provider's compliance to Kadaster information security requirements documented as part of the Agreement.		X
Provide to Kadaster, on a quarterly basis, an evaluation ofservice provider's performance, which includes results of internal security audits, independent third-party audits, self-assessments, and evaluation ofservice provider's handling of and response to Security Incidents and Security Events. Provide details onservice provider's industry certification (e.g. ISO 27001) and report on certification status.	X	
Support Kadaster third parties engaged to conduct periodic reviews, audits, security vulnerability assessments, penetration tests, and security risk assessments of Kadaster environment, processes, and practices upon request.	X	
Remediate, including taking corrective action on assessment findings that identify that the Services provided byservice provider do not comply with Kadaster information security requirements documented as part of the Agreement. Remediation ofservice provider non-compliance and deficiencies will be completed atservice provider's expense.	X	
Cooperate and assist with audit and assessment efforts conducted by Kadaster and/or Kadaster third-party auditors.	X	
Notify Kadaster of any security violations within twenty-four (24) hours of the identified violation.	X	