CSA Consensus Assessment Initiative Questionaire (CAIQ)

April 2024

datafi

Notice

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Datafi product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from Datafi and its affiliates, suppliers or licensors. Datafi products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of Datafi to its customers are controlled by Datafi agreements, and this document is not part of, nor does it modify, any agreement between Datafi and its customers.

Abstract

The CSA Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. Datafi has completed this questionnaire with the answers below. The questionnaire has been completed using the current CSA CAIQ standard, v3.1.1 (11-15-19 Update).

Introduction

The Cloud Security Alliance (CSA) is a “not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.” For more information, see https://cloudsecurityalliance.org/about/.

CSA Consensue Assessment Initiative Questionaire

Question ID	Consensus Assessment Questions	Consensus Assessment Answers			Notes	Control Responsibility
		Yes	No	N/A		
AIS-01.1	Do you use industry standards (i.e. OWASP Software Assurance Maturity Model, ISO 27034) to build in security for your Systems/Software Development Lifecycle (SDLC)?	X			The Datafi system development lifecycle incorporates industry best practices which include formal design reviews, threat modeling and completion of a risk assessment.	Datafi
AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	X			Automated code analysis tools are run as a part of the Software Development Lifecycle	Datafi
AIS-01.3	Do you use manual source-code analysis to detect security defects in code prior to production?	X				Datafi
AIS-01.4	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		X		We use some opensource libraries, which does not follow SLDC in some cases	Datafi
AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	X			Static code analysis tools are run as a part of the standard build process. Our security risk assessment reviews begin during the design phase and the engagement lasts through launch to ongoing operations. Customers are responsible for performing vulnerability scanning of their workloads based on their internal scanning requirements.	Shared

AIS- 02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	X			Datafi and customers agree to a **Service Agreement** outlining the terms of service and responsibilities of both parties prior to service delivery.	Shared
AIS- 02.2	Are all requirements and trust levels for customers' access defined and documented?	X			Datafi and customers agree to a **Service Agreement** outlining the terms of service and responsibilities of both parties prior to service delivery.	Shared
AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?			X		N/A
AIS-03.2	Are data input and output integrity routines (i.e. MD5/SHA checksums) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?			X		N/A
AIS-04.1	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	X			Datafi has developed and implemented a security control environment designed to protect the confidentiality, integrity, and availability of customers' systems and content.	Datafi
AAC-01.1	Do you develop and maintain an agreed upon audit plan (e.g., scope, objective, frequency, resources,etc.) for reviewing the efficiency and effectiveness of implemented security controls?	x			Datafi has established a formal, periodic audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness.	Datafi
AAC-01.2	Does your audit program take into account effectiveness of implementation of security operations?	X			Internal and external audits are planned and performed according to the documented audit scheduled to review the continued performance against standards-based criteria and to identify general improvement opportunities.	Datafi
AAC-02.1	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?			X	Datafi does not have SOC2 certification	N/A
AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	X			Datafi performs regular network security assements of our cloud services infrastructure	Datafi

AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	X			Datafi performs regular network security assesments of our cloud services infrastructure	Datafi
AAC-02.4	Do you conduct internal audits at least annually?	X			Internal audits are performed at a regular basis to cover different products and services using a standards-based approach.	Datafi
AAC-02.5	Do you conduct independent audits at least annually?		X		Datafi has not established a formal external independant audit progam at this time	N/A
AAC-02.6	Are the results of the penetration tests available to tenants at their request?	X			Although Datafi regularly performs recurring penetration testing, we will share the results directly with customers when appropriate.	N/A
AAC-02.7	Are the results of internal and external audits available to tenants at their request?		X		Although Datafi regularly performs internal and external testing, we do not share the results directly with customers.	N/A
AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	X			Datafi maintains relationships with internal and external parties to monitor legal, regulatory, and contractual requirements.	Datafi
BCR-01.1	Does your organization have a plan or framework for business continuity management or disaster recovery management?	X			The Datafi business continuity plan ensures the efficient and timely recovery of core systems.	Datafi
BCR-01.2	Do you have more than one provider for each service you depend on?		X		Datafi operates on AWS geographically distributed infrastructure. Currently use AWS exclusively for core services	Datafi
BCR-01.3	Do you provide a disaster recovery capability?	X			Datafi provides customers the flexibility to host Edge Servers on multiple geographic regions on thier prefered cloud service providers.	Customer
BCR-01.4	Do you monitor service continuity with upstream providers in the event of provider failure?	X			Datafi monitors and reports on infrastructure services provided by our cloud partners	Datafi
BCR-01.5	Do you provide access to operational redundancy reports, including the services you rely on?	X			Datafi provides real-time status reports on dependant service for customers	Datafi
BCR-01.6	Do you provide a tenant-triggered failover option?		X		Datafi does not provide customers with tenant-triggered failover options	N/A
BCR-01.7	Do you share your business continuity and redundancy plans with your tenants?		X		Datafi does not share business continuty and reduncance plans with tenants	N/A

BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	X			Datafi Continuity Policies and Plans have been developed and tested at least annually in alignment with industry standards.	Datafi
BCR-03.1	Does your organization adhere to any international or industry standards when it comes to securing, monitoring, maintaining and testing of datacenter utilities services and environmental conditions?	X			AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 11 and link below for Data center controls overview: https://aws.amazon.com/compliance/data-center/controls/	AWS
BCR-03.2	Has your organization implemented environmental controls, fail-over mechanisms or other redundancies to secure utility services and mitigate environmental conditions?	X			AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC reports provide additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. Please refer to link below for Data center controls overview: https://aws.amazon.	AWS
BCR-04.1	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	X			Information System Documentation is made available internally to AWS personnel through the use of Amazon's Intranet site.	AWS
BCR-05.1	Is physical damage anticipated and are countermeasures included in the design of physical protections?	X			AWS data centers incorporate physical protection against environmental risks. AWS' physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices.	AWS
BCR-06.1	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?		X		Each AWS data center is evaluated to determine the controls that must be implemented to mitigate, prepare, monitor, and respond to natural disasters or malicious acts that may occur.	AWS
BCR-07.1	Do you have documented policies, procedures and supporting business processes for equipment and datacenter maintenance?	X			AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers.	AWS

BCR-07.2	Do you have an equipment and datacenter maintenance routine or plan?	X			AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers.	AWS
BCR-08.1	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	X			AWS equipment is protected from utility service outages in alignment with ISO 27001 standard.	AWS
BCR-09.1	Do you use industry standards and frameworks to determine the impact of any disruption to your organization (i.e. criticality of services and recovery priorities, disruption tolerance, RPO and RTO etc) ?	X			Policies and Procedures for continued service operations have been established	Datafi
BCR-09.2	Does your organization conduct impact analysis pertaining to possible disruptions to the cloud service?	X			Business Impact Assessment is performed to assign business criticality to supporting processes and identification of operational processes, teams and dependencies to sustain operations during a business disruption.	Datafi
BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	X			Information System Documentation is made available internally to personnel	Datafi
BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	X			Datafi maintains a retention policy in order to continue operations of our business and services. Critical system components, including audit evidence and logging records, are replicated across multiple AWS Availability Zones and backups are maintained and monitored. Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Shared

BCR-11.2	Do you have documented policies and procedures demonstrating adherence to data retention periods as per legal, statutory or regulatory compliance requirements?	X			Datafi maintains a retention policy in order to continue operations of our business and services. Critical system components, including audit evidence and logging records, are replicated across multiple AWS Availability Zones and backups are maintained and monitored. Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Shared
BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	X			Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer
BCR-11.4	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	X			Customers can create an AWS CloudWatch alarm that monitors an AWS EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure.	Customer
BCR-11.5	If using virtual infrastructure, do you provide tenants with a capability to restore a virtual machine to a previous configuration?			X		N/A
BCR-11.6	Does your cloud solution include software/provider independent restore and recovery capabilities?	x			Customers can export their AMIs and use them on premise or at another provider	Customer
BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?			X	Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer
CCC-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	X			The design of all new services or any significant changes to current services follow secure software development practices and are controlled through a project management system with multi-disciplinary participation.	Datafi
CCC-02.1	Are policies and procedures for change management, release, and testing adequately communicated to external business partners?			X		N/A

CCC-02.2	Are policies and procedures adequately enforced to ensure external business partners comply with change management requirements?			X		N/A
CCC-03.1	Do you have a defined quality change control and testing process in place based on system availability, confidentiality, and integrity?	X			Datafi maintains internal quality control and testing process based on system lifecycle developmen.	Dataif
CCC-03.2	Is documentation describing known issues with certain products/services available?	X			Datafi system availabilty and alerting notify customers of security and privacy event. Customers can subsribe to system availability and event bulletins.	Datafi
CCC-03.3	Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?	X			Datafi has a process and notifies and coordinates with the appropriate resources when conducting security-related activities within the system. Activities include, triage, remediation, vulnerability scanning, contingency testing, and incident response exercises.	Datafi
CCC-03.4	Do you have controls in place to ensure that standards of quality are being met for all software development?	X			Datfi maintains a systematic approach, to planning and developing new services to ensure the quality and security requirements are met with each release. Our strategy for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing. The design of all new services or any significant changes to current services follow secure software development practices and are controlled through a project management system with multi-disciplinary participation.	Datafi
CCC-03.5	Do you have controls in place to detect source code security defects for any outsourced software development activities?			X	Datafi does not outsource to development of core services	N/A
CCC-03.6	Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?	X			The Datafi system development lifecycle (SDLC) incorporates industry best practices.	Datafi
CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	X			The abilility to install software to production environment is restrited. Before being installed to production environments, all software goes through the standard change management process enforced by AWS, including appropriate approvals.	Datafi

CCC-05.1	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights/responsibilities within it?		X		Datafi does not provide this level of granularity to customers. We notify customers of changes to the service offering. Datafi continuously evolves and improves our existing services, and frequently adds new services.	N/A
CCC-05.2	Do you have policies and procedures established for managing risks with respect to change management in production environments?	X			Datafi applies a systematic approach to managing change to ensure that all changes to a production environment are reviewed, tested, and approved.	Datafi
CCC-05.3	Do you have technical measures in place to ensure that changes in production environments are registered, authorized and in adherence with existing SLAs?	X			The abilility to install software or change the production environment is restricted. Before being installed to production environments, all software goes through the standard change management process, including appropriate approvals.	Datafi
DSI-01.1	Do you provide a capability to identify data and virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?			X	Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	N/A
DSI-01.2	Do you provide a capability to identify data and hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?			X	Datafi does not provide hardware as part of our service	N/A
DSI-02.1	Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?	X			Datafi provides the required documentation and associated data flow diagrams for services. Customers determine the design patterns based on their usage of Datafi services and associated network and system components.	Customer
DSI-02.2	Can you ensure that data does not migrate beyond a defined geographical residency?	X			Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer
DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	X			Datafi services are available via TLS protected endpoints, which provide server authentication. Customers can use TLS for all of their interactions. Datafi provides open encryption methodologies and enables customers to encrypt and authenticate all traffic, and to enforce the latest standards and ciphers.	Datafi

DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	X			Datafi services are available via TLS protected endpoints, which provide server authentication. Customers can use TLS for all of their interactions. Datafi provides open encryption methodologies and enables customers to encrypt and authenticate all traffic, and to enforce the latest standards and ciphers.	Shared
DSI-04.1	Are policies and procedures established for data labeling and handling in order to ensure the security of data and objects that contain data?			X	Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer
DSI-04.2	Do you follow a structured data-labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?			X	Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer
DSI-04.3	Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?			X	Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer
DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?			X	Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer
DSI-06.1	Are the responsibilities regarding data stewardship defined, assigned, documented, and communicated?			X	Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer
DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?			X	Customers retain control and ownership of their data. Datafi has no insight as to what type of content the customer chooses to connect via Datafi and the customer retains complete control of how they choose to classify their content, where it is stored, used and applicable retention policies.	Customer

DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	X			Customers can terminate their use of our service and remove all metadata and event history as defined in the **Service Agreement**.	Datafi
DCS-01.1	Do you classify your assets in terms of business criticality, service-level expectations, and operational continuity requirements?	X			AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools.	AWS
DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	X			AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools.	AWS
DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	X			Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means.	AWS
DCS-03.1	Do you have a capability to use system geographic location as an authentication factor?	X			We provides the capability of conditional user access based on geographic location.	Datafi
DCS-03.2	Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?	X			AWS manages equipment identification in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.	AWS
DCS-04.1	Is authorization obtained prior to relocation or transfer of hardware, software, or data to an offsite premises?	X			Environments used for the delivery of the AWS services are managed by authorized personnel and are located in an AWS managed data centers. Media handling controls for the data centers are managed by AWS in alignment with the AWS Media Protection Policy. This policy includes procedures around access, marking, storage, transporting, and sanitation.	AWS
DCS-05.1	Can you provide tenants with your asset management policies and procedures?	X			AWS does not provide confidential AWS policies and procedures directly to the customers AWS engages with external certifying bodies and independent auditors to review and validate our compliance with policies. AWS SOC reports provide additional details on the specific asset management related policies and control activities executed by AWS	AWS

DCS-06.1	Can you provide evidence that policies, standards, and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas?	X			AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks.	AWS
DCS-06.2	Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards, and procedures?	X			In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete.	AWS
DCS-07.1	Are physical access control mechanisms (e.g. CCTV cameras, ID cards, checkpoints) in place to secure, constrain and monitor egress and ingress points?	X			Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.	AWS
DCS-08.1	Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?	X			Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.	AWS
DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	X			Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy.	AWS
EKM-01.1	Do you have key management policies binding keys to identifiable owners?	X			Datafi services create tenant specific keys uniquely bound to the compute layer within their environment	Datafi
EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	X			Datafi services create tenant specific keys uniquely bound to the compute layer within their environment	Datafi
EKM-02.2	Do you have a capability to manage encryption keys on behalf of tenants?	X			Datafi services create tenant specific keys uniquely bound to the compute layer within their environment	Datafi
EKM-02.3	Do you maintain key management procedures?	X			Internally, Datafi establishes and manages cryptographic keys for required cryptography employed within the infrastructure. Datafi produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes. A secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute credentials needed on hosts	Datafi

EKM-02.4	Do you have documented ownership for each stage of the lifecycle of encryption keys?	X			Datafi has internal documentation on services that create tenant specific keys and the lifecycle management of the keys	Datafi
EKM-02.5	Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?		X		Datafi does not utilize any third party or open source framework to manage encryption keys.	Datafi
EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	X			Datafi encrypts all customer data in transit and at rest using industry standard practices	Datafi
EKM-03.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?	X			Datafi encrypts all customer data in transit and at rest using industry standard practices	Datafi
EKM-03.3	Do you have documentation establishing and defining your encryption management policies, procedures, and guidelines?	X			Datafi maintains documentation on our processes based in industry standard practices	Datafi
EKM-04.1	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	X			Datafi encrypts all customer data in transit and at rest using industry standard practices	Datafi
EKM-04.2	Are your encryption keys maintained by the cloud consumer or a trusted key management provider?	X			Encryption keys are generated by the service and maintainted by the customer	Customer
EKM-04.3	Do you store encryption keys in the cloud?	X			Encryption keys are generated by the service and maintainted by the customer	Customer
EKM-04.4	Do you have separate key management and key usage duties?	X			Datafi maintains separation of key management and key usage duties	Datafi
GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	X			Datafi has established and monitors baseline infrastructure standards, including for network components. Many of the services are provided by AWS	Datafi
GRM-01.2	Do you have the capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?	X			Datafi has established and monitors baseline infrastructure standards, including for network components	Datafi
GRM-02.1	Does your organization's risk assessments take into account awareness of data residency, legal and statutory requirements for retention periods and data protection and classification?	X			Datafi maintains a Risk Management program to mitigate and manage risk. In addition, Customers retain control and ownership of their data and can implement data residency, security and retention requirements based on legal and regulatory requirements.	Shared

GRM-02.2	Do you conduct risk assessments associated with data governance requirements at least once a year?	X			Datafi maintains a Risk Management program to mitigate and manage risk.	Datafi
GRM-03.1	Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?	X			The Control environment begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies.	Datafi
GRM-04.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?		X		Datafi maintains a Risk Management program but does not share these with Customers	N/A
GRM-04.2	Do you review your Information Security Management Program (ISMP) at least once a year?	X			Datafi security policies are reviewed and approved on an annual basis by Leadership.	Datafi
GRM-05.1	Do executive and line management take formal action to support information security through clearly-documented direction and commitment, and ensure the action has been assigned?	X			Datafi management leads an information security program that identifies and establishes security goals that are relevant to business requirements.	Datafi
GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	X			Datafi maintains an information security progam and makes available to impacted employees and partners	Datafi
GRM-06.2	Are information security policies authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership?	X			Datafi management leads an information security program that identifies and establishes security goals that are relevant to business requirements.	Datafi

GRM-06.3	Do you have agreements to ensure your providers adhere to your information security and privacy policies?			X		N/A
GRM-06.4	Can you provide evidence of due diligence mapping of your controls, architecture, and processes to regulations and/or standards?		X		Datafi maintains a information security program but does not share these with Customers	Datafi
GRM-06.5	Do you disclose which controls, standards, certifications, and/or regulations you comply with?		X		Datafi maintains a information security program but does not share these with Customers	Datafi
GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Datafi management leads an information security program that identifies and establishes security goals that are relevant to business requirements. HR policies define disciplinary actions.	Datafi
GRM-07.2	Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?	X			Datafi management leads an information security program that identifies and establishes security goals that are relevant to business requirements. HR policies define disciplinary actions.	Datafi
GRM-08.1	Do risk assessment results include updates to security policies, procedures, standards, and controls to ensure they remain relevant and effective?	X			Datafi management leads an information security program that identifies and establishes security goals that are relevant to business requirements. HR policies define disciplinary actions.	Datafi
GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?		X		Datafi security and/or privacy policies are subject to change based on various inputs, including, risk assessment activities, regulatory or legal guidance, follow-up to audit reviews etc. Updates are made to the Service Agreement as needed.	Datafi
GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	X			Datafi security policies are reviewed and approved on an annual basis by Leadership.	Datafi
GRM-10.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	X			Datafi security policies are reviewed and approved and tested on an annual basis by Leadership.	Datafi
GRM-10.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories?	X				Datafi
GRM-11.1	Do you have a documented, organization-wide program in place to manage risk?	X			Datafi security policies are reviewed and approved and tested on an annual basis by Leadership.	Datafi

GRM-11.2	Do you make available documentation of your organization-wide risk management program?		X		Datafi security policies are reviewed and approved and tested on an annual basis by Leadership and not shared with Customers	N/A
HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	X			Upon termination, the responsible managers ensures that a formal checklist, which includes steps for access removal and collection of assets, is completed	Datafi
HRS-01.2	Do you have asset return procedures outlining how assets should be returned within an established period?	X			Upon termination of employee or contracts, assets in their possessions are retrieved on the date of termination.	Datafi
HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	X			Datafi conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee’s position and level of access	Datafi
HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	X			Employees complete periodic role-based training that includes Security training and requires an acknowledgement to complete	Datafi
HRS-03.2	Do you require that employment agreements are signed by newly hired or on-boarded workforce personnel prior to granting workforce personnel user access to corporate facilities, resources, and assets?	X			Personnel supporting Datafi systems and devices must sign a non-disclosure agreement prior to being granted access.	Datafi
HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	X			Leadership teams defines internal management responsibilities to be followed for termination and role change of employees and vendors.	Datafi
HRS-04.2	Do the above procedures and guidelines account for timely revocation of access and return of assets?	X			Access is automatically revoked when an employee’s record is terminated	Datafi

HRS-05.1	Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones, and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	X			Datafi has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy).	Datafi
HRS-06.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented, and reviewed at planned intervals?	X			Legal Counsel manages and periodically revises the NDA to reflect business needs.	Datafi
HRS-07.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?	X			The Datafi Service Agreement provides details on the roles and responsibilities of Datafi and those of our Customers.	Datafi
HRS-08.1	Do you have policies and procedures in place to define allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices and IT infrastructure network and systems components?	X			Datafi has implemented data handling and classification requirements that provide specifications around: • Data encryption • Content in transit and during storage • Access • Retention • Physical controls • Mobile devices • Data handling requirements Employees are required to review and sign-off on an employment contract, which acknowledges their responsibilities to overall Company standards and information security.	Datafi
HRS-08.2	Do you define allowance and conditions for BYOD devices and its applications to access corporate resources?	X			Datafi has a documented BYOD policy that outlines the procedures for employees to Bring their own device	Datafi

HRS-09.1	Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model, segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	X			Datafi employees complete periodic Information Security training which requires an acknowledgement to complete.	Datafi
HRS-09.2	Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?	X			Datafi employees complete periodic Information Security training which requires an acknowledgement to complete.	Datafi
HRS-09.3	Do you document employee acknowledgment of training they have completed?	X			Datafi employees complete periodic Information Security training which requires an acknowledgement to complete.	Datafi
HRS-09.4	Is successful and timed completion of the training program(s) considered a prerequisite for acquiring and maintaining access to sensitive systems?	X			The security awareness and training are required prior to gaining system access and are reviewed and updated at least annually, or sooner if required due to information system changes.	Datafi
HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	X			The security awareness and training are required prior to gaining system access and are reviewed and updated at least annually, or sooner if required due to information system changes. Employees complete periodic Information Security training which requries an acknowledgement to complete	Datafi
HRS-09.6	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?	X			Datafi employees complete periodic Information Security training which requires an acknowledgement to complete.	Datafi
HRS-10.1	Are personnel informed of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards, and applicable regulatory requirements?	X			Datafi has implemented various methods of internal communication to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner.	Datafi
HRS-10.2	Are personnel informed of their responsibilities for maintaining a safe and secure working environment?	X			Datafi roles and responsibilities for maintaining safe and secure working environment are reviewed and updated annually	Datafi
HRS-10.3	Are personnel informed of their responsibilities for ensuring that equipment is secured and not left unattended?	X			Datafi roles and responsibilities for maintaining safe and secure working environment are reviewed and updated annually	Datafi

HRS-11.1	Are all computers and laptops configured such that there is lockout screen after a pre-defined amount of time?	X			Datafi has established baseline infrastructure standards in alignment with industry best practices.	Datafi
HRS-11.2	Are there policies and procedures to ensure that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents?	X			Datafi roles and responsibilities for maintaining safe and secure working environment are reviewed and updated annually	Datafi
IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	X			Datafi has identified auditable event categories across systems and devices within the system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements	Datafi
IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	X			Datafi has identified auditable event categories across systems and devices within the system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements	Datafi
IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	X			Access privilege reviews are triggered upon job and/or role transfers	Datafi
IAM-02.2	Do you have policies, procedures and technical measures in place to ensure appropriate data/assets access management in adherence to legal, statutory or regulatory compliance requirements?	X			Datafi has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy).	Datafi
IAM-02.3	Do you have procedures and technical measures in place for user account entitlement de-/provisioning based on the rule of least privilege?	X			Datafi has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy).	Datafi
IAM-02.4	Do you have procedures and technical measures in place for data access segmentation in multi-tenant system architectures?	X			Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them.	Datafi
IAM-02.5	Do you enforce data access permissions based on the rules of Authentication, Authorization and Accountability (AAA)?	X			Datafi controls access to systems through authentication that requires a unique user ID and password. Datafi systems do not allow actions to be performed on the information system without identification or authentication.	Datafi

IAM-02.6	Do your policies and procedures incorporate security controls for establishing higher levels of assurance for critical business case considerations, supported by multifactor authentication?	X			Datafi personnel with a business need to access the sensitive resources are required to first use multi-factor authentication to gain access	Datafi
IAM-02.7	Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?		X		Datafi tracks metrics for internal process measurements and improvements, but this level of detail is not shared with Customers	Datafi
IAM-03.1	Is user access to diagnostic and configuration ports restricted to authorized individuals and applications?	X			Datafi has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy).	Datafi
IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	X			Datafi personnel with a business need to access the sensitive resources are required to first use multi-factor authentication to gain access. The MFA system stores details on users with access	Datafi
IAM-04.2	Do you manage and store the user identity of all personnel who have network access, including their level of access?	X			Datafi personnel with a business need to access the sensitive resources are required to first use multi-factor authentication to gain access	Datafi
IAM-05.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?		X			Datafi
IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Datafi has established formal policies, procedures to delineate the minimum standards for logical access to system and network resources.	Datafi
IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	X			Datafi has established formal policies, procedures to delineate the minimum standards for logical access to system and network resources.	Datafi
IAM-07.1	Does your organization conduct third-party unauthorized access risk assessments?			X	Datafi does not utilize third parties to provide services to customers.	N/A
IAM-07.2	Are preventive, detective corrective compensating controls in place to mitigate impacts of unauthorized or inappropriate access?	X			Datafi has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy).	Datafi

IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/customer credentials following the rules of least privilege?	X			Datafi has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy).	Datafi
IAM-08.2	Based on the rules of least privilege, do you have policies and procedures established for permissible storage and access of identities used for authentication?	X			Datafi provides customers with the abilty to define rules of least privlaged access.	Datafi
IAM-08.3	Do you limit identities' replication only to users explicitly defined as business necessary?	X			Access to Datafi systems are allocated based on least privilege, approved by an authorized individual prior to access provisioning, and assigned a different user ID than used for normal business use.	Datafi
IAM-09.1	Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners, and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems, and network components?	X			Unique user identifiers are created as part of the onboarding workflow process. The device provisioning process helps ensure unique identifiers for devices.	Datafi
IAM-09.2	Do you provide upon the request of users with legitimate interest access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?	X			Datafi maintains detailed records on internal systems, and provides this level of detail to Customers with applicable need to know requirements	Datafi
IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	X			All access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked.	Datafi
IAM-10.2	Do you collect evidence to demonstrate that the policy (see question IAM-10.1) has been enforced?	X			All access grants are reviewed on a periodic basis; explicit re-approval is required or access to the resource is automatically revoked.	Datafi

IAM-10.3	Do you ensure that remediation actions for access violations follow user access policies?	X				Datafi
IAM-10.4	Will you share user entitlement and remediation reports with your tenants, if inappropriate access may have been allowed to tenant data?	X			Datafi Customers retain control and ownership of their data. Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored.	Datafi
IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	X			Access is automatically revoked when an employee's record is terminated	Datafi
IAM-11.2	Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?	X			Access is automatically revoked when an employee's record is terminated	Datafi
IAM-12.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	X			The Datafi authentication service provides identity federation to the Datafi Console. Multi-factor authentication is an optional feature that a customer can utilize.	Datafi
IAM-12.2	Do you use open standards to delegate authentication capabilities to your tenants?	X			The Datafi authentication service provides identity federation to the Datafi Console. SSO authentication is an optional feature that a customer can utilize.	Datafi
IAM-12.3	Do you support identity federation standards (e.g., SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?	X			Datafi offers multiple options for federating your identities. With federation, you can use single sign-on (SSO) to access your Datafi accounts using credentials from your corporate directory.	Datafi
IAM-12.4	Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?	X			Customers can configure policy capability using their existing Identity Providers and established fine grained policies to manage permissions to their data resources.	Datafi
IAM-12.5	Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?	X			Customers can configure policy capability using their existing Identity Providers and established fine grained policies to manage permissions to their data resources.	Datafi

IAM-12.6	Do you provide tenants with strong (multifactor) authentication options (e.g., digital certs, tokens, biometrics, etc.) for user access?	X			Datafi authentication services enable you to configure multi-factor authentication (MFA) to your workspace.	Datafi
IAM-12.7	Do you allow tenants to use third-party identity assurance services?	X			Customers can enable users to bring their own identities from social identity providers, such as Google or use their existing corporate identities through SAML.	Datafi
IAM-12.8	Do you support password (e.g., minimum length, age, history, complexity) and account lockout (e.g., lockout threshold, lockout duration) policy enforcement?	X			The Datafi authentication service enable customers to securely control access to their workspace and resources for their users.	Datafi
IAM-12.9	Do you allow tenants/customers to define password and account lockout policies for their accounts?	X			Customers can configure password policies and associated configurations for their accounts.	Shared
IAM-12.10	Do you support the ability to force password changes upon first logon?	X			Customers can configure password policies and associated configurations for their accounts.	Datafi
IAM-12.11	Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?	X			Customers can configure password policies and associated configurations for their accounts.	Shared
IAM-13.1	Are access to utility programs used to manage virtualized partitions (e.g. shutdown, clone, etc) appropriately restricted and monitored?	X			Customers can configure password policies and associated configurations for their accounts.	Datafi
IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	X			AWS Security performs regular vulnerability scans on the underlying infrastructure, web application, and databases in the AWS environment using a variety of tools.	AWS
IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	X			Audit logs are appropriately restricted and monitored.	Datafi
IVS-01.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been performed?		X		Datafi maintains detailed records on internal systems, but this level of detail is not shared with Customers	Datafi
IVS-01.4	Are audit logs centrally stored and retained?	X			Authentication logging aggregates sensitive logs stores them on internal databases. Access and privileged command auditing logs record every automated and interactive login to the systems as well as every privileged command executed.	Datafi

IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	X			Datafi maintains detailed records on internal systems and reviews them on a regular basis	Datafi
IVS-02.1	Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?	X			Virtual Machines are assigned to customers as a part of the service. Customers retain control over what resources are being used and where resources reside. Changes to Datafi Virtual Machines are logged and investigated by the security team.	Shared
IVS-02.2	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?			X	Virtual Machines are assigned to customers as a part of the service. Customers retain control over what resources are being used and where resources reside.	Customer
IVS-02.3	Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.g., portals or alerts)?			X	Virtual Machines are assigned to customers as a part of the service. Customers retain control over what resources are being used and where resources reside.	Customer
IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	X			AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol).	AWS
IVS-04.1	Do you provide documentation regarding what levels of system (e.g., network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?		X		Datafi maintains detailed records on internal systems, but this level of detail is not shared with Customers	N/A
IVS-04.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?		X		Virtual Machines are assigned to customers as a part of the service. Customers retain control over what resources are being used and where resources reside.	N/A
IVS-04.3	Does your system's capacity requirements take into account current, projected, and anticipated capacity needs for all systems used to provide services to the tenants?	X			Datafi maintains a capacity planning model to assess usage and demands at least monthly, and usually more frequently (e.g., weekly).	Datafi
IVS-04.4	Is system performance monitored and tuned in order to continuously meet regulatory, contractual, and business requirements for all the systems used to provide services to the tenants?	X			Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.	Datafi

IVS-05.1	Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?			X	Virtual Machines are assigned to customers as a part of the service. Customers retain control over what resources are being used and where resources reside.	N/A
IVS-06.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?			X		N/A
IVS-06.2	Do you regularly update network architecture diagrams that include data flows between security domains/zones?	X			Customers maintain information related to their data flow and individual application architectures of their implementations.	Shared
IVS-06.3	Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?			X	AWS access control lists and rule sets are reviewed and approved, and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date.	Shared
IVS-06.4	Are all firewall access control lists documented with business justification?			X	AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose.	Shared
IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	X			Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment	Datafi
IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	X			Datafi provides tenants on paid plans with separate environments for production. Free plans share compute and storage services	Datafi
IVS-08.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?			X	Datafi does not provides infrastructure services	N/A
IVS-08.3	Do you logically and physically segregate production and non-production environments?	X			Datafi provides logically separation of compute and storage services between production and test envronments	Datafi
IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	X			Datafi provides both system and network level protection by virtual firewalls to ensure business and customer security	Datafi

IVS-09.2	Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legal, regulatory and contractual requirements?	X			Datafi provides both system and network level protection by virtual firewalls to ensure business and customer security	Datafi
IVS-09.3	Have you implemented the necessary measures for the appropriate isolation and segmentation of tenants' access to infrastructure system and network components, in adherence to established policies, legal, statutory, and regulatory compliance obligations?	X			Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data.	Shared
IVS-09.4	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	X			Customer environments are logically segregated to prevent users and customers from accessing resources not assigned to them. Customers maintain full control over who has access to their data.	Shared
IVS-09.5	Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?	X			Datafi provides both system and network level protection by virtual firewalls to ensure business and customer security	Datafi
IVS-10.1	Are secured and encrypted communication channels used when migrating physical servers, applications, or data to virtual servers?	X			Datafi provides both system and network level protection encryption to ensure business and customer security	Datafi
IVS-10.2	Do you use a network segregated from production-level networks when migrating physical servers, applications, or data to virtual servers?	X			Datafi provides both system and network level segregation to ensure business and customer security	Datafi
IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	X			Datafi employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.	Datafi

IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?			X		N/A
IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?			X		N/A
IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?			X		N/A
IVS-13.1	Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?	X			Datafi Customers retain responsibility to manage their own network segmentation in adherence with their defined requirements.	Shared
IVS-13.2	Do you implement technical measures and apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks?	X			AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances).	AWS
IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	X			Datafi publishes a list of customer enabled APIs	Datafi
IPY-02.1	Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?	X			Datafi customers can export log files in any industry standard format	Customer

IPY-03.1	Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third-party applications?		X		Datafi does not publish private APIs for interoperability between our service and third-party applications	Datafi
IPY-03.2	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	X			Datafi provides customers with a container image for Edge Server deployments	Datafi
IPY-03.3	Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?	X			Customer retain control and ownership of their content. Customers can choose how they migrate applications and content	Datafi
IPY-04.1	Is data import, data export, and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?	X			Datafi APIs and the Console are available via TLS protected endpoints.	Datafi
IPY-04.2	Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?		X		Datafi does not publish private APIs for interoperability between our services	Datafi
IPY-05.1	Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?	X			Datafi uses industry standard containerization technology to ensure interoperability	Datafi
IPY-05.2	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	X			Datafi provides customers with a container image for Edge Server deployments	Datafi
IPY-05.3	Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?		X		Datafi does not make customization to any hypervisor or solution-specific virtualization	Datafi
MOS-01.1	Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?			X		N/A

MOS-02.1	Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?			X		N/A
MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?			X		N/A
MOS-04.1	Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?			X		N/A
MOS-05.1	Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?			X		N/A
MOS-06.1	Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?			X		N/A
MOS-07.1	Do you have a documented application validation process for testing device, operating system, and application compatibility issues?			X		N/A
MOS-08.1	Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?			X		N/A
MOS-09.1	Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (e.g., operating system and patch levels, lost or decommissioned, device assignee)?			X		N/A
MOS-10.1	Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?			X		N/A

MOS-11.1	Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?			X		N/A
MOS-12.1	Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?			X		N/A
MOS-12.2	Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?			X		N/A
MOS-13.1	Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e-discovery, and legal holds?			X		N/A
MOS-13.2	Does the BYOD policy clearly state the expectations over the loss of non-company data in case a wipe of the device is required?			X		N/A
MOS-14.1	Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?			X		N/A
MOS-15.1	Do you manage all changes to mobile device operating systems, patch levels, and applications via your company's change management processes?			X		N/A
MOS-16.1	Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?			X		N/A
MOS-16.2	Are your password policies enforced through technical controls (i.e. MDM)?			X		N/A
MOS-16.3	Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?			X		N/A
MOS-17.1	Do you have a policy that requires BYOD users to perform backups of specified corporate data?			X		N/A

MOS-17.2	Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?			X		N/A
MOS-17.3	Do you have a policy that requires BYOD users to use anti-malware software (where supported)?			X		N/A
MOS-18.1	Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?			X		N/A
MOS-18.2	Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?			X		N/A
MOS-19.1	Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?			X		N/A
MOS-19.2	Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?			X		N/A
MOS-20.1	Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?			X		N/A
MOS-20.2	Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?			X		N/A
SEF-01.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?			X	Datafi does not maintain liasons and point of contact with local authorities	N/A
SEF-02.1	Do you have a documented security incident response plan?	X			Datafi security policies are reviewed and approved and tested on an annual basis by Leadership.	Datafi
SEF-02.2	Do you integrate customized tenant requirements into your security incident response plans?		X			Datafi
SEF-02.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?		X		Datafi security policies are reviewed and approved and tested on an annual basis by Leadership but does not publish to Customers. Customer roles are described in the **Service Agreement**	Datafi
SEF-02.4	Have you tested your security incident response plans in the last year?			X	AWS incident response plans are tested on at least an annual basis.	Datafi

SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	X			Datafi employees are trained on how to recognize suspected security incidents and where to report them.	Datafi
SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	X			Datafi maintain an incident response communication channel with customers	Datafi
SEF-04.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?	X			Datafi contingency plans and incident response playbooks have defined and tested tools and processes to detect, mitigate, investigate, and report a security incident.	Datafi
SEF-04.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?	X			Datafi contingency plans and incident response playbooks have defined and tested tools and processes to detect, mitigate, investigate, and report a security incident.	Datafi
SEF-04.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?	X			Customers retain control over their content on the platform, including the ability to preserve logs, snapshots, and other evidence.	Customer
SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	X			Datafi does not disclose customer information unless we're required to do so to comply with a legally valid and binding order.	Datafi
SEF-05.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	X			Datafi security team monitors and reports on all information security incidents	Datafi
SEF-05.2	Will you share statistical information for security incident data with your tenants upon request?		X		Datafi security team monitors and reports on all information security incidents, but does not publish to Customers	Datafi
STA-01.1	Do you inspect and account for data quality errors and associated risks, and work with your cloud supply-chain partners to correct them?		X		Customers retain control over their content on the platform, including the ability to preserve logs, snapshots, and other evidence	Customer
STA-01.2	Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privileged access for all personnel within your supply chain?	X			Datafi has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy).	Datafi

STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	X			Datafi makes available details of security incidents to all affected customers	Datafi
STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	X			Datafi collects capacity planning details for all relevant components for purposed of strategic planning	Datafi
STA-03.2	Do you provide tenants with capacity planning and use reports?		X		Datafi collects capacity planning details for all relevant components for purposed of strategic planning, but does not publish to Customers	Datafi
STA-04.1	Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?	X			Datafi has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy).	Datafi
STA-05.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored, and transmitted?	X			Datafi assesses and continuously monitors suppliers to ensure that they are conforming to specific requirements and contractual obligations.	Datafi
STA-05.2	Do you select and monitor outsourced providers to ensure that they are in compliance with applicable legislation?	X			Datafi assesses and continuously monitors suppliers to ensure that they are conforming to specific requirements and contractual obligations.	Datafi
STA-05.3	Does legal counsel review all third-party agreements?	X			Datafi legal counsel reviews all third-party agreements	Datafi
STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	X			Contracts with third-party suppliers cover, at a minimum, the following: • Legal and regulatory requirements • User awareness of information security responsibilities and issues • Arrangements for reporting, notification, and investigation of information security incidents and security breaches • Target and unacceptable levels of service (for example, SLA, OLA) • Service continuity requirements (e.g., recovery time objectives - RTO) • Protection of Intellectual Property Rights (IPR) • Conditions for renegotiation/termination of the agreement	Datafi
STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	X			Datafi has existing back and recovery of internal systems	Datafi

STA-05.6	Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	X			Datafi will assign compute and storage based on geographic requirements	Datafi
STA-05.7	Can you provide the physical location/geography of storage of a tenant’s data upon request?	X			Datafi will provide physcial location of storage of tenant data upon request	Datafi
STA-05.8	Can you provide the physical location/geography of storage of a tenant's data in advance?	X			Datafi will provide physcial location of storage of tenant data upon request	Datafi
STA-05.9	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?		X		Datafi does not allow tenants to define acceptable geographic locations for data routing	N/A
STA-05.10	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?			X		N/A
STA-05.11	Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?		X		Datafi tenants cannot opt out of mandatory metadata inspection.	N/A
STA-05.12	Do you provide the client with a list and copies of all subprocessing agreements and keep this updated?	X			Datafi provides Customers with a list of all subprocessing agreements and keeps this updated.	Datafi
STA-06.1	Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?		X		Datafi maintains a formal risk management policy and procedures which includes management and assessment of risks posed by subcontractors.	Datafi
STA-07.1	Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate, and relevant agreements (e.g., SLAs) between providers and customers (tenants)?		X		Through the use of established assessment procedures, AWS assesses and continuously monitors suppliers to ensure that they are conforming to specific AWS requirements.	AWS
STA-07.2	Do you have the ability to measure and address non-conformance of provisions and/or terms across the entire supply chain (upstream/downstream)?			X		N/A
STA-07.3	Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?			X		N/A

STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	X			Datafi publishes current SLAs and system performance statistics that can be found here: https://status.datafi.us/	Datafi
STA-07.5	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	X			Datafi publishes current SLAs and system performance statistics that can be found here: https://status.datafi.us/	Datafi
STA-07.6	Do you provide customers with ongoing visibility and reporting of your SLA performance?	X			Datafi publishes current SLAs and system performance statistics that can be found here: https://status.datafi.us/	Datafi
STA-07.7	Do your data management policies and procedures address tenant and service level conflicts of interests?			X		N/A
STA-07.8	Do you review all service level agreements at least annually?	X			SLAs are reviewed periodically	Datafi
STA-08.1	Do you assure reasonable information security across your information supply chain by performing an annual review?			X		N/A
STA-08.2	Does your annual review include all partners/third-party providers upon which your information supply chain depends?			X		N/A
STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?		X		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. AWS maintains standard contract review and signature processes that include legal reviews with consideration of protecting AWS resources.	AWS
STA-09.2	Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?	X			AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. AWS maintains standard contract review and signature processes that include legal reviews with consideration of protecting AWS resources.	AWS
TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?		X			Datafi
TVM-01.2	Do you ensure that security threat detection systems using signatures, lists, or behavioral patterns are updated across all infrastructure components as prescribed by industry best practices?	X				Datafi

TVM-02.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	X			Datafi Security teams performs regular vulnerability scans on the host operating system, web application, and databases in the environment using a variety of tools.	Datafi
TVM-02.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?	X			Datafi Security teams performs regular vulnerability scans on the host operating system, web application, and databases in the environment using a variety of tools.	Datafi
TVM-02.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?	X			Datafi Security teams performs regular vulnerability scans on the host operating system, web application, and databases in the environment using a variety of tools.	Datafi
TVM-02.4	Will you make the results of vulnerability scans available to tenants at their request?		X		Datafi Security teams performs regular vulnerability scans on the host operating system, web application, and databases in the environment using a variety of tools, but do not publish to Customers	Datafi
TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	X			Datafi security teams patch systems on a regular basis	Datafi
TVM-02.6	Do you inform customers (tenant) of policies and procedures and identified weaknesses if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control?	X				Datafi
TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	X				Datafi
TVM-03.2	Is all unauthorized mobile code prevented from executing?	X				Datafi

Document Revisions

Date	Description
January 2022	First Publication
May 2022	Update Publication
January 2023	Update Publication
April 2024	Update Publication